Basic Support for IPv6 over IEEE Std 802.11 Networks Operating Outside
                  the Context of a Basic Service Set
                draft-ietf-ipwave-ipv6-over-80211ocb-52

Abstract

   This document provides methods and settings, for using IPv6 to
   communicate among nodes within range of one another over a single
   IEEE 802.11-OCB link. Support for these methods and settings require
   minimal changes to existing stacks. This document also describes
   limitations associated with using these methods. Optimizations and
   usage of IPv6 over more complex scenarios is not covered in this
   specification 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 February 10, 2020.

Copyright Notice

Table of Contents

1. Introduction

   This document provides a baseline 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 changes to existing stacks. Moreover, the
   document identifies limitations of such usage. Concretely, the
   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 is derived from IPv6
   over Ethernet [RFC2464], but operates over 802.11-OCB to provide at
   least P2P (Point to Point) connectivity using IPv6 ND and link-local
   addresses.

   The IPv6 network layer operates on 802.11-OCB in the same manner as
   operating on Ethernet with the following exceptions:

   o 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] and [RFC2464].

   o 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. Security and privacy recommendations are
      discussed in 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. Likewise, ND Extensions and
      IPWAVE optimizations for vehicular communications are not in
      scope. The expectation is that further specifications will be
      edited to cover more complex vehicular networking scenarios.

   The reader may refer to [I-D.ietf-ipwave-vehicular-networking] for an
   overview of problems related to running IPv6 over 802.11-OCB. It is
   out of scope of this document to reiterate those.

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.

   The document makes uses of the following terms: IP-OBU (Internet
   Protocol On-Board Unit): an IP-OBU denotes a computer situated in a
   vehicle such as a car, 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): is 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: refers to the mode specified in IEEE Std 802.11-2016 when the MIB attribute dot11OCBActivited is 'true'.

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 (ITS).

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, as such, 1500 octets. As noted in [RFC8200], every link on the Internet must have a minimum MTU of 1280 octets, as well as follow the other recommendations, especially with regard 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 SHOULD use a
   'priority' value of 1 (QoS with a 'Background' user priority),
   reserving higher priority values for safety-critical and time-
   sensitive traffic, including the ones listed in [ETSI-sec-archi].

   To simplify the Application Programming Interface (API) between the
   operating system and the 802.11-OCB media, device drivers MAY
   implement IPv6-over-Ethernet as per [RFC2464] 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 can be formed using an
   EUI-64 identifier, in particular during transition time, (the time
   spent before an interface starts using a different address than the
   LL one).

   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. Moreover,
   whether or not the interface identifier is derived from the EUI-64
   identifier, its length is 64 bits as is the case for Ethernet
   [RFC2464].

4.4. Stateless Autoconfiguration

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

   The RECOMMENDED method for forming stable Interface Identifiers
   (IIDs) 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. Regardless of how
to form the IID, its length is 64 bits, similarely to IPv6 over
Ethernet [RFC2464].

The bits in the IID have no specific 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 IIDs, instead of meaningful IIDs derived from a
valid and meaningful MAC address ([RFC2464], Section 4), help avoid
certain privacy risks (see the risks mentioned in Section 5.1.1). If
semantically opaque IIDs are needed, they may be generated using the
method for generating semantically opaque IIDs with IPv6 Stateless
Address Autoconfiguration given in [RFC7217]. Typically, an opaque
IID 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.

Some applications that use IPv6 packets on 802.11-OCB links (among
other link types) may benefit from IPv6 addresses whose IIDs don't
change too often. It is RECOMMENDED to use the mechanisms described
in RFC 7217 to permit the use of Stable IIDs 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 specified in Sections 6 and 7 of
   [RFC2464].

4.5.1. Address Mapping -- Unicast

   This document is scoped for Address Resolution (AR) and Duplicate
   Address Detection (DAD) per [RFC4862].

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 there 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

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

IPv6 Neighbor Discovery protocol (ND) requires reflexive properties
(bidirectional connectivity) which is generally, though not always,
the case for P2P OCB links. IPv6 ND also requires transitive
properties for DAD and AR, so an IPv6 subnet can be mapped on an OCB
network only if all nodes in the network share a single physical
broadcast domain. The extension to IPv6 ND operating on a subnet
that covers multiple OCB links and not fully overlapping (NBMA) is
not in scope. Finally, IPv6 ND requires a permanent connectivity of
all nodes in the subnet to defend their addresses, in other words
very stable network conditions.

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 vehicle
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 (i.e., a default route is absent), and the addressing peers
are equally qualified (that is, it is impossible to determine that
some vehicle owns and distributes addresses to others) the use of
link-local addresses is RECOMMENDED.

The baseline ND protocol [RFC4861] MUST be supported over 802.11-OCB
links. Transmitting ND packets may prove to have some performance
issues as mentioned in 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 a 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 does not use existing 802.11 link-layer security
mechanisms. There is no encryption applied below the network layer
running on 802.11-OCB. At the application layer, the IEEE 1609.2
document [IEEE-1609.2] provides 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). Therefore, an attacker can sniff
or inject traffic while within range of a vehicle or IP-RSU (by
setting an interface card's frequency to the proper range). Also, an
attacker may not heed to legal limits for radio power and can use a
very sensitive directional antenna; if attackers wishe to attack a
given exchange they do not necessarily need to be in close physical
proximity. Hence, such a link is less protected than commonly used
links (wired link or aforementioned 802.11 links with link-layer
security).

Therefore, any node can join a subnet, directly communicate with any
nodes on the subset to include potentially impersonating another
node. This design allows for a number of threats outlined in
Section 3 of [RFC6959]. While not widely deployed, SeND [RFC3971],
[RFC3972] is a solution that can address Spoof-Based Attack Vectors.

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 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. An example of change policy is to change the MAC
address of the OCB interface each time the system boots up. This may
help mitigate privacy risks to a certain level. Furthermore, for
privacy concerns, ([RFC8065]) recommends using an address generation
scheme rather than addresses generated from a fixed link-layer
address. However, there are some specificities related to vehicles.
Since roaming is an important characteristic of moving vehicles, the
use of the same Link-Local Address over time can indicate the
presence of the same vehicle in different places and thus leads to
location tracking. Hence, a vehicle should get hints about a change
of environment (e.g. , engine running, GPS, etc..) and renew the IID
in its LLAs.

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.

Implementations should use a policy dictating when the MAC address is
changed on the 802.11-OCB interface. 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:

o Bit "Local/Global" set to "locally administered".

o Bit "Unicast/Multicast" set to "Unicast".

o The 46 remaining bits are set to a random value, using a random number generator that meets the requirements of [RFC4086].

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

A randomized Interface ID has the same characteristics of a randomized MAC address, except the length in bits.

5.3. Pseudonymization impact on confidentiality and trust

Vehicles 'and drivers' privacy relies on pseudonymization mechanisms such as the ones described in Section 5.2. This pseudonymization means that upper-layer protocols and applications SHOULD NOT rely on layer-2 or layer-3 addresses to assume that the other participant can be trusted.

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 Mohamed Boucadair for proofreading and suggesting modifications of this document.

The authors would like to thank Eric Vyncke for reviewing 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

   [IEEE-802.11-2016]
              "IEEE Standard 802.11-2016 - IEEE Standard for Information
              Technology - Telecommunications and information exchange
              between systems Local and metropolitan area networks -
              Specific requirements - Part 11: Wireless LAN Medium
              Access Control (MAC) and Physical Layer (PHY)
              Specifications. Status - Active Standard. Description
              retrieved freely; the document itself is also freely
              available, but with some difficulty (requires
              registration); description and document retrieved on April
              8th, 2019, starting from URL
              https://standards.ieee.org/findstds/
              standard/802.11-2016.html".

   [RFC1042] Postel, J. and J. Reynolds, "Standard for the transmission
              of IP datagrams over IEEE 802 networks", STD 43, RFC 1042,
              DOI 10.17487/RFC1042, February 1988,
              <https://www.rfc-editor.org/info/rfc1042>.

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <https://www.rfc-editor.org/info/rfc2119>.

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

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

   [RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and
              More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191,
              November 2005, <https://www.rfc-editor.org/info/rfc4191>.

   [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast
              Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005,
              <https://www.rfc-editor.org/info/rfc4193>.

   [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
              Architecture", RFC 4291, DOI 10.17487/RFC4291, February
              2006, <https://www.rfc-editor.org/info/rfc4291>.

   [RFC4301] Kent, S. and K. Seo, "Security Architecture for the
              Internet Protocol", RFC 4301, DOI 10.17487/RFC4301,
              December 2005, <https://www.rfc-editor.org/info/rfc4301>.

   [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman,
              "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861,
              DOI 10.17487/RFC4861, September 2007,
              <https://www.rfc-editor.org/info/rfc4861>.

   [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless
              Address Autoconfiguration", RFC 4862,
              DOI 10.17487/RFC4862, September 2007,
              <https://www.rfc-editor.org/info/rfc4862>.

   [RFC5415] Calhoun, P., Ed., Montemurro, M., Ed., and D. Stanley,
              Ed., "Control And Provisioning of Wireless Access Points
              (CAPWAP) Protocol Specification", RFC 5415,
              DOI 10.17487/RFC5415, March 2009,
              <https://www.rfc-editor.org/info/rfc5415>.

   [RFC6059] Krishnan, S. and G. Daley, "Simple Procedures for
              Detecting Network Attachment in IPv6", RFC 6059,
              DOI 10.17487/RFC6059, November 2010,
              <https://www.rfc-editor.org/info/rfc6059>.

   [RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility
              Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July
              2011, <https://www.rfc-editor.org/info/rfc6275>.

   [RFC7042] Eastlake 3rd, D. and J. Abley, "IANA Considerations and
              IETF Protocol and Documentation Usage for IEEE 802
              Parameters", BCP 141, RFC 7042, DOI 10.17487/RFC7042,
              October 2013, <https://www.rfc-editor.org/info/rfc7042>.

   [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6
              Interface Identifiers", RFC 7136, DOI 10.17487/RFC7136,
              February 2014, <https://www.rfc-editor.org/info/rfc7136>.

   [RFC7217] Gont, F., "A Method for Generating Semantically Opaque
              Interface Identifiers with IPv6 Stateless Address
              Autoconfiguration (SLAAC)", RFC 7217,
              DOI 10.17487/RFC7217, April 2014,
              <https://www.rfc-editor.org/info/rfc7217>.

   [RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu,
              "Recommendation on Stable IPv6 Interface Identifiers",
              RFC 8064, DOI 10.17487/RFC8064, February 2017,
              <https://www.rfc-editor.org/info/rfc8064>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6
              (IPv6) Specification", STD 86, RFC 8200,
              DOI 10.17487/RFC8200, July 2017,
              <https://www.rfc-editor.org/info/rfc8200>.

9.2. Informative References

   [ETSI-sec-archi]
              "ETSI TS 102 940 V1.2.1 (2016-11), ETSI Technical
              Specification, Intelligent Transport Systems (ITS);
              Security; ITS communications security architecture and
              security management, November 2016. Downloaded on
              September 9th, 2017, freely available from ETSI website at
              URL http://www.etsi.org/deliver/
              etsi_ts/102900_102999/102940/01.02.01_60/
              ts_102940v010201p.pdf".

   [I-D.ietf-ipwave-vehicular-networking]
              Jeong, J., "IP Wireless Access in Vehicular Environments
              (IPWAVE): Problem Statement and Use Cases", draft-ietf-
              ipwave-vehicular-networking-11 (work in progress), July
              2019.

   [I-D.ietf-mboned-ieee802-mcast-problems]
              Perkins, C., McBride, M., Stanley, D., Kumari, W., and J.
              Zuniga, "Multicast Considerations over IEEE 802 Wireless
              Media", draft-ietf-mboned-ieee802-mcast-problems-07 (work
              in progress), July 2019.

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

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

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

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

   [RFC3753] Manner, J., Ed. and M. Kojo, Ed., "Mobility Related
             Terminology", RFC 3753, DOI 10.17487/RFC3753, June 2004,
             <https://www.rfc-editor.org/info/rfc3753>.

   [RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P.
             Thubert, "Network Mobility (NEMO) Basic Support Protocol",
             RFC 3963, DOI 10.17487/RFC3963, January 2005,
             <https://www.rfc-editor.org/info/rfc3963>.

   [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander,
             "SEcure Neighbor Discovery (SEND)", RFC 3971,
             DOI 10.17487/RFC3971, March 2005,
             <https://www.rfc-editor.org/info/rfc3971>.

   [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)",
             RFC 3972, DOI 10.17487/RFC3972, March 2005,
             <https://www.rfc-editor.org/info/rfc3972>.

   [RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing
             Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889,
             September 2010, <https://www.rfc-editor.org/info/rfc5889>.

   [RFC6959] McPherson, D., Baker, F., and J. Halpern, "Source Address
             Validation Improvement (SAVI) Threat Scope", RFC 6959,
             DOI 10.17487/RFC6959, May 2013,
             <https://www.rfc-editor.org/info/rfc6959>.

   [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy
              Considerations for IPv6 Address Generation Mechanisms",
              RFC 7721, DOI 10.17487/RFC7721, March 2016,
              <https://www.rfc-editor.org/info/rfc7721>.

   [RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-
              Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065,
              February 2017, <https://www.rfc-editor.org/info/rfc8065>.

   [SHA256]   "Secure Hash Standard (SHS), National Institute of
              Standards and Technology.
              https://csrc.nist.gov/CSRC/media/Publications/fips/180/2/
              archive/2002-08-01/documents/fips180-2.pdf".

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'). 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:

o The use by each node of a 'wildcard' BSSID (i.e., each bit of the
   BSSID is set to 1)

o No IEEE 802.11 Beacon frames are transmitted

o No authentication is required in order to be able to communicate

o No association is needed in order to be able to communicate

o No encryption is provided in order to be able to communicate

o Flag dot11OCBActivated is set to true

All the nodes in the radio communication range (IP-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.

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

      (i) 802.11 Infrastructure mode    (ii) 802.11-OCB mode
```
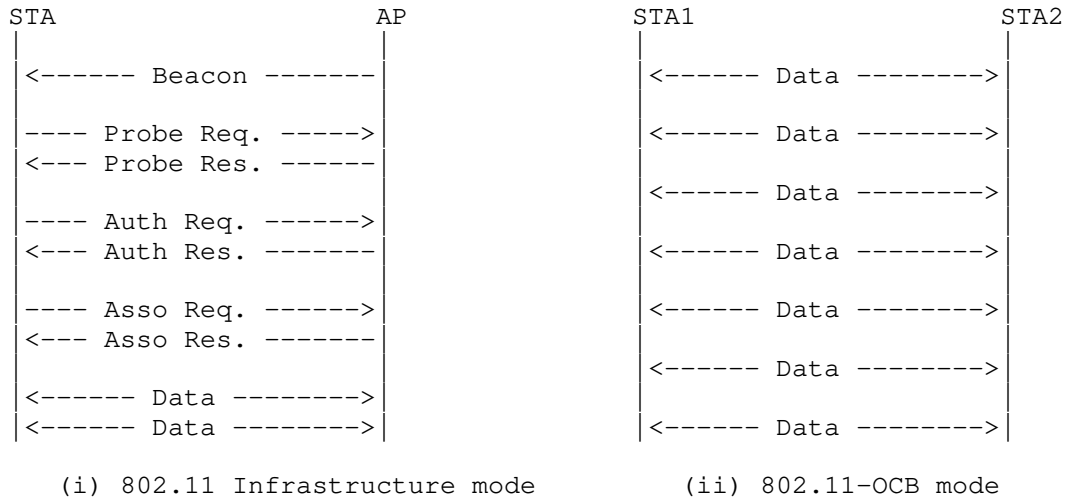
Figure 1: Difference between messages exchanged on 802.11 (left) and
                       802.11-OCB (right)

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

The most important 802.11-OCB point which influences the IPv6
functioning is the OCB characteristic; an additional, less direct
influence, is the maximum bandwidth afforded by the PHY modulation/
demodulation methods and channel access specified by 802.11-OCB. The
maximum bandwidth theoretically possible in 802.11-OCB is 54 Mbit/s

(when using, for example, the following parameters: 20 MHz channel;
modulation 64-QAM; coding rate R is 3/4); in practice of IP-over-
802.11-OCB a commonly observed figure is 12Mbit/s; this bandwidth
allows the operation of a wide range of protocols relying on IPv6.

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

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

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

Additionally, specific conditions related to congestion avoidance, jamming avoidance, and radar detection are imposed on the use of DSRC (in US) and on the use of frequencies for Intelligent Transportation Systems (in EU), compared to Wireless LAN (802.11a/b/g/n).

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

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

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

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

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

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

Changes needed on the network stack in OCB mode:

o Physical layer:

* The chip must use the Orthogonal Frequency Multiple Access
   (OFDM) encoding mode.

* The chip must be set in half-mode rate mode (the internal clock
   frequency is divided by two).

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

MAC layer:

* All management frames (beacons, join, leave, and others)
   emission and reception must be disabled except for frames of
   subtype Action and Timing Advertisement (defined below).

* No encryption key or method must be used.

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

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

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

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

Appendix 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
        +-+-+-+-+-+-{            }+-+-+-+-+-+-+-+  Boundary
        |             EPD          |      |      |
        |                          | MLME |      |
        +-+-+-{  MAC_SAP    }+-+-+-|  MLME_SAP   |
        |       MAC Sublayer       |      |        802.11-OCB
        |       and ch. coord.     |      | SME    Services
        +-+-+-{   PHY_SAP   }+-+-+-+-+-+-+-|
        |                          | PLME |      |
        |             PHY Layer    |  PLME_SAP   |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
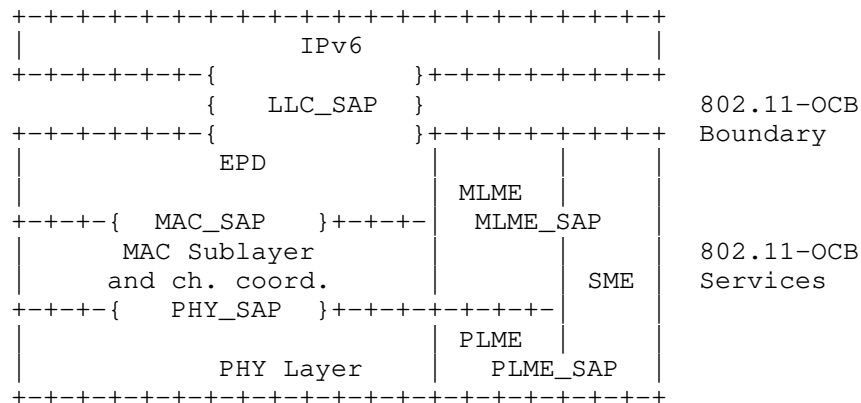
               Figure 2: EtherType Protocol Discrimination

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 transportation 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:

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

   o The STA may send control frames, except those of subtype PS-Poll,
      CF-End, and CF-End plus CFAck;

   o The STA MUST send data frames of subtype QoS Data.

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).

```
           +--------+                              +-------+
           |        |         802.11-OCB Link      |       |
       ----| Router |------------------------------| Host  |
           |        |                              |       |
           +--------+                              +-------+
```
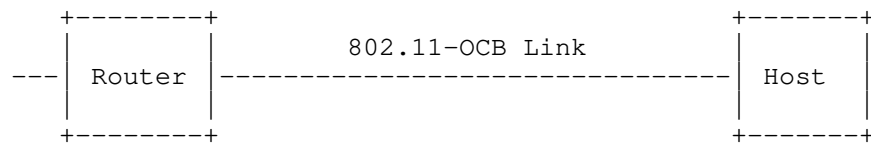
            Figure 3: Topology for capturing IP packets on 802.11-OCB

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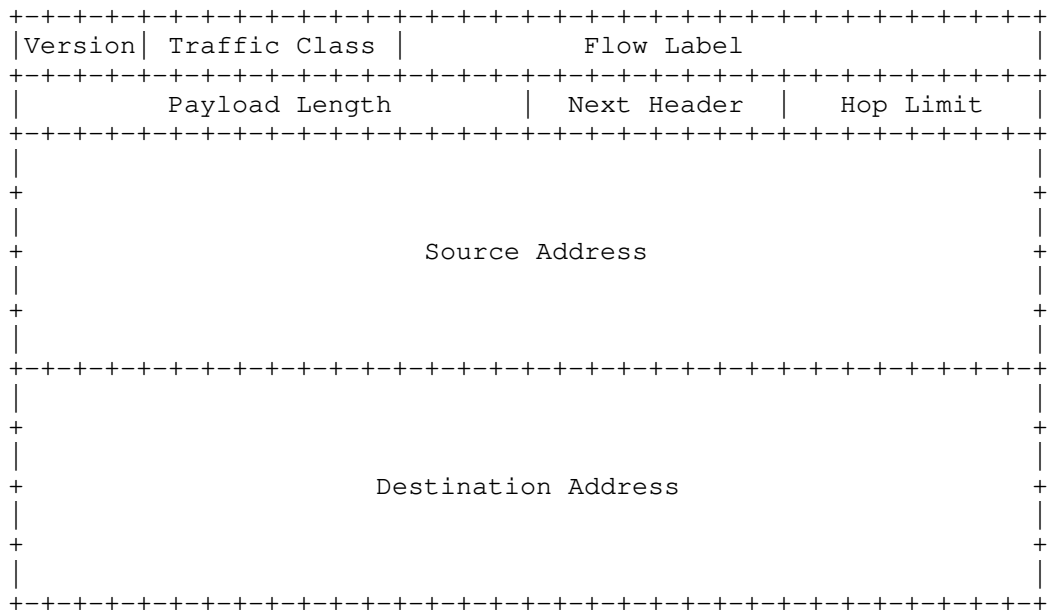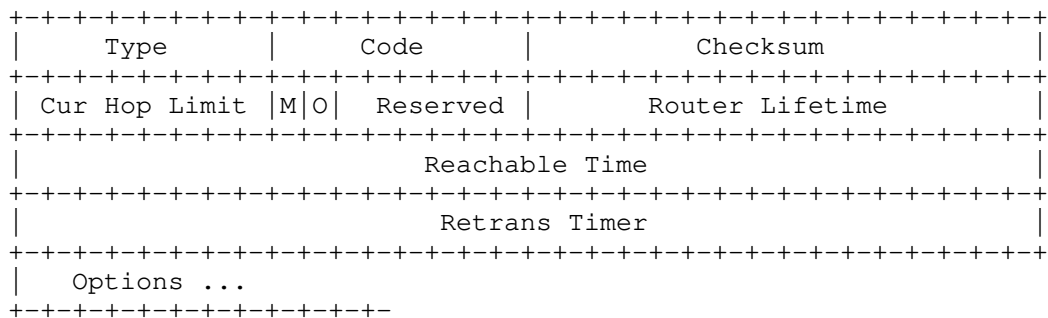
The value of the Data Rate field in the Radiotap header is set to 6
Mb/s. This indicates the rate at which this RA was received.

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.

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

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

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

One notices that the Radiotap Header, 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 2.

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

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

OBU (On-Board Unit): a term defined outside the IETF. An On-Board
Unit is a 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 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
respectgive 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. 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 [RFC4191],
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 may be implemented on OCB. OCB nodes that
support RFC 8505 SHOULD 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 of Meknes
   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 Vehicle-to-Infrastructure Networking
                draft-jeong-ipwave-v2i-problem-statement-00

Abstract

   This document specifies the problem statement for IPv6-based vehicle-
   to-infrastructure networking. Dedicated Short-Range Communications
   (DSRC) is standardized as IEEE 802.11p for the wireless media access
   in vehicular networks. This document addresses the extension of IPv6
   as the network layer protocol in vehicular networks and is focused on
   the networking issues in one-hop communication between a Road-Side
   Unit (RSU) and vehicle. The RSU is connected to the Internet and
   allows vehicles to have the Internet access if connected. The major
   issues of including IPv6 in vehicular networks are neighbor discovery
   protocol, stateless address autoconfiguration, and DNS configuration
   for the Internet connectivity over DSRC. Also, when a vehicle and an
   RSU have an internal network, respectively, the document discusses
   the issues of the internetworking between the vehicle's internal
   network and the RSU's internal network (e.g., prefix discovery,
   prefix exchange, and service discovery), and also security and
   privacy issues.

Status of This Memo

   http://www.ietf.org/shadow.html.

   This Internet-Draft will expire on September 14, 2017.

Table of Contents

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 this VANET, Dedicated
   Short-Range Communications (DSRC) [DSRC-WAVE] has been standardized
   as IEEE 802.11p [IEEE-802.11p], which is an extension of IEEE 802.11a
   [IEEE-802.11a] with a consideration of the vehicular network's
   characteristics such as a vehicle's velocity and collision avoidance.

   Now the deployment of VANET is demanded into 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) started to consider automobiles as computers instead of
   mechanical machines since many current vehicles are operating with
   many sensors and software. Also, Google made a great advancement in
   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.

   With this trend, vehicular networking has been researched to enable
   vehicles to communicate with other vehicles and infrastructure nodes
   in the Internet by using TCP/IP technologies [ID-VN-Survey], such as
   IP address autoconfiguration, routing, handover, and mobility
   management. IPv6 [RFC2460] is suitable for vehicular networks since
   the protocol has abundant address space, autoconfiguration features,
   and protocol extension ability through extension headers.

   This document specifies the problem statement of IPv6-based vehicle-
   to-infrastructure (V2I) networking, such as IPv6 addressing
   [RFC4291], neighbor discovery [RFC4861], address autoconfiguration
   [RFC4862], and DNS naming service [RFC6106][RFC3646][ID-DNSNA]. This
   document also specifies the problem statement of the internetworking
   between a vehicle's internal network and an RSU's internal network,
   such as prefix discovery, prefix exchange, and service discovery, in
   the case where the vehicle and the RSU have their own internal
   network. In addition, the document analyzes the characteristics of
   vehicular networks to consider the design of V2I 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, four new terms are defined below:

   o Road-Side Unit (RSU): A node that has a Dedicated Short-Range
      Communications (DSRC) device for wireless communications with the
      vehicles and is connected to the Internet. Every RSU is usually
      deployed at an intersection so that it can provide vehicles with
      the Internet connectivity.

   o Vehicle: A node that has the DSRC device for wireless
      communications with vehicles and RSUs. Every vehicle may also
      have a GPS-navigation system for efficient driving.

   o Traffic Control Center (TCC): A node that maintains road
      infrastructure information (e.g., RSUs and traffic signals),
      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). TCC is included in a vehicular cloud for
      vehicular networks.

4. Overview

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

   Figure 1 shows the network configuration for V2I networking in a road
   network. The two RSUs (RSU1 and RSU2) are deployed in the road
   network and are connected to the Vehicular Cloud through the
   Internet. The 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 RSU1. Vehicle1 can
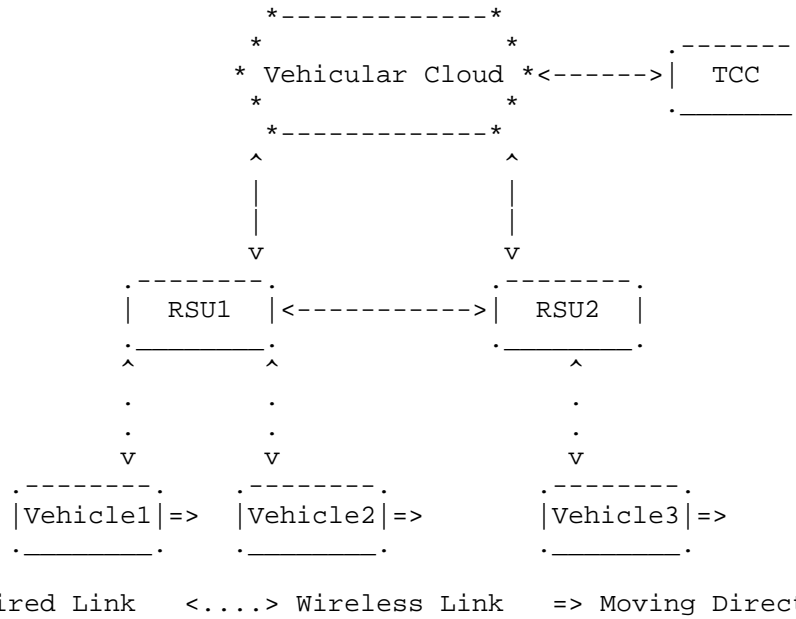   communicate with Vehicle3 via RSU1 and RSU2.

```
                      *-------------*
                     *               *        .-------.
                    * Vehicular Cloud *<------>|  TCC  |
                     *               *        ._____.
                      *-------------*
                          ^                      ^
                          |                      |
                          |                      |
                          v                      v
              .---------.                  .---------.
              |  RSU1   |<----------->|  RSU2   |
              ._____.                  ._____.
               ^       ^                     ^
               .       .                     .
               .       .                     .
               v       v                     v
          .---------. .---------.       .---------.
          |Vehicle1|=> |Vehicle2|=>     |Vehicle3|=>
          ._____. ._____.         ._____.
```

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

           Figure 1: The Network Configuration for V2I Networking

   Figure 2 shows internetworking between the vehicle's moving network
   and the RSU's fixed network. There exists an internal network
   (Moving Network1), which is located inside Vehicle1. Vehicle1 has
   the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two
   routers (Router1 and Router2). The internal network (Fixed Network1)
   is located 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
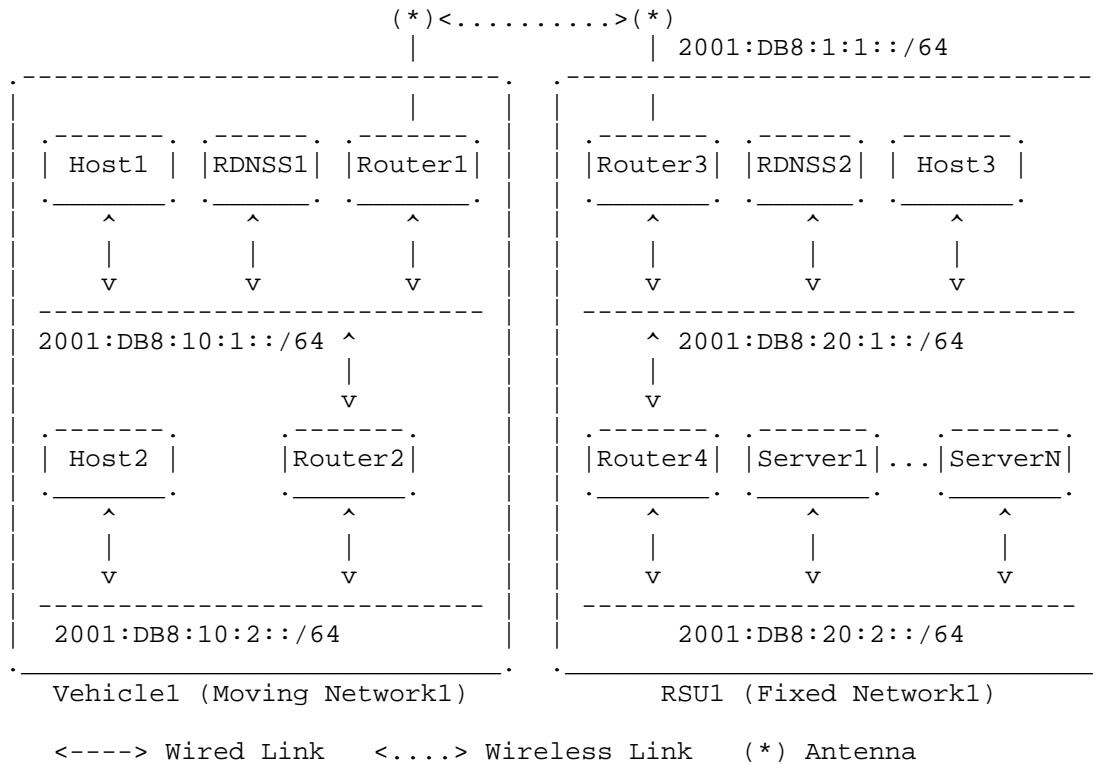   service.

```
                             (*)<..........>(*)
                              |              | 2001:DB8:1:1::/64
         .--------------------------.    .---------------------------------.
         |            |             |    |         |                       |
         | .-------. .-------. .-------. |    | .-------. .-------. .-------.      |
         | | Host1 | |RDNSS1| |Router1| |    | |Router3| |RDNSS2| | Host3 |      |
         | ._____. ._____. ._____. |    | ._____. ._____. ._____.      |
         |    ^        ^        ^      |    |    ^        ^        ^          |
         |    |        |        |      |    |    |        |        |          |
         |    v        v        v      |    |    v        v        v          |
         | -------------------------- |    | ------------------------------ |
         | 2001:DB8:10:1::/64 ^       |    |    ^ 2001:DB8:20:1::/64         |
         |                    |       |    |    |                            |
         |                    v       |    |    v                            |
         | .-------.      .-------.    |    | .-------. .-------.  .-------.      |
         | | Host2 |      |Router2|    |    | |Router4| |Server1|...|ServerN|     |
         | ._____.      ._____.    |    | ._____. ._____.  ._____.      |
         |    ^             ^        |    |    ^        ^          ^          |
         |    |             |        |    |    |        |          |          |
         |    v             v        |    |    v        v          v          |
         | -------------------------- |    | ------------------------------ |
         |  2001:DB8:10:2::/64        |    |     2001:DB8:20:2::/64           |
         ._____.    ._____.
             Vehicle1 (Moving Network1)       RSU1 (Fixed Network1)

          <----> Wired Link    <....> Wireless Link    (*) Antenna
```

       Figure 2: Internetworking between Vehicle Network and RSU Network

5. Internetworking between the Vehicle and RSU Networks

   This section discusses the internetworking between the vehicle's
   moving network and the RSU's fixed network. As shown in Figure 2, it
   is assumed that the prefix assignment for each subnet inside the
   vehicle's mobile network and the RSU's fixed network through a prefix
   delegation protocol. Problems are a prefix discovery and prefix
   exchange. The prefix discovery is defined as how routers in a moving
   network discover the prefixes of the subnets in the moving network,
   as shown in Figure 2. The prefix exchange is defined as how a
   vehicle and an RSU exchange their prefixes with each other. Once
   these prefix discovery and prefix exchange are established, the
   unicast of packets should be supported between the vehicle's moving
   network and the RSU's fixed network. Also, the DNS naming service
   should be supported for the DNS name resolution for a host or server
   in either the vehicle's moving network or the RSU's fixed network.

6. IPv6 Addressing

   This section discusses IP addressing for V2I networking. There are
   two policies for IPv6 addressing in vehicular networks. The one
   policy is to use unique local IPv6 unicast addresses (ULAs) for
   vehicular networks [RFC4193]. The other policy is to use global IPv6
   addresses for the interoperability with the Internet [RFC4291]. The
   former approach is usually used by Mobile Ad Hoc Networks (MANET) for
   a separate multi-link 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 the global IP addresses, there are two policies, which are 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 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, RSUs play a role of L3 router.

7. Neighbor Discovery

   The Neighbor Discovery (ND) is a core part of IPv6 protocol suite
   [RFC4861]. This section discusses the 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.

8. IP Address Autoconfiguration

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

procedures.

To mitigate the impact of vehicle speed on the address configuration, RSU can perform IP address autoconfiguration includig the DAD proactively for the sake of the vehicles as an ND proxy. If vehicles periodically report their mobility information (e.g., position, trajectory, speed, and direction) to TCC, TCC can coordinate 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.

9. DNS Naming Service

This section discusses a DNS naming service for V2I networking. The DNS naming service can consist 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 distributed in the world. 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.

10. IP Mobility Management

This section discusses an IP mobility support in V2I networking. In a single subnet per RSU, vehicles keep crossing the communication coverages of adjacent RSUs. During this crossing, TCP/UDP sessions can be maintained through IP mobility support, such as Mobile IPv6 (MIPv6) [RFC6275], Proxy MIPv6 [RFC5213][RFC5949], and Distributed Mobility Management (DMM) [RFC7333][RFC7429]. Since vehicles move

fast along roadways, this high speed should be considered for a
parameter configuration in the IP mobility management. With the
periodic reports of the mobility information from the vehicles, TCC
can coordinate RSUs and other network compoments 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
Mobile IPv6, the high speed of vehicles should be considered for a
parameter configuration in NEMO.

11. Service Discovery

Vehicles need to discover services (e.g., road condition
notification, navigation service, and infotainment) 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.

12. Security Considerations

The security and privacy are very important in secure vehicular
networks for V2I networking. Only valid vehicles should be allowed
to use V2I networking in vehicular networks. 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. Also, TLS

certificates can 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 secuirty and privacy can be supported for safe and reliable data services in vehicular networks.

To prevent a vehicle from being tracked by an adversary with its Media Access Control (MAC) address or IPv6 address, each vehicle needs to periodically update its MAC address and the corresponding IPv6 address using randomness [RFC4086][RFC4941]. Such an update of the MAC and IPv6 addresses should not interrupt the communications between a vehicle and an RSU in the level of network layer (i.e., IP) or transport layer (e.g., TCP and UDP).

To protect data packets exchanged between a vehicle and an RSU, they should be encrypted by a cryptography algorithm. For this confidentiality, efficient encryption and decryption algorithms can be used along with an efficient key management scheme through Internet Key Exchange version 2 (IKEv2) and Internet Protocol Security (IPsec) [Securing-VCOMM].

This document shares all the security issues of the neighbor discovery protocol. This document can get benefits from secure neighbor discovery (SEND) [RFC3971].

13. Acknowledgements

14. References

14.1. Normative References

   [RFC2119]   Bradner, S., "Key words for use in RFCs to
                      Indicate Requirement Levels", BCP 14, RFC 2119,

                          March 1997.

   [RFC2460]   Deering, S. and R. Hinden, "Internet Protocol,
                        Version 6 (IPv6) Specification", RFC 2460,
                        December 1998.

   [RFC4193]   Hinden, R. and B. Haberman, "Unique Local IPv6
                        Unicast Addresses", RFC 4193, October 2005.

   [RFC4291]   Hinden, R. and S. Deering, "IP Version 6
                        Addressing Architecture", RFC 4291, February 2006.

   [RFC4861]   Narten, T., Nordmark, E., Simpson, W., and H.
                        Soliman, "Neighbor Discovery for IP Version 6
                        (IPv6)", RFC 4861, September 2007.

   [RFC4862]   Thomson, S., Narten, T., and T. Jinmei, "IPv6
                        Stateless Address Autoconfiguration", RFC 4862,
                        September 2007.

   [RFC6106]   Jeong, J., Park, S., Beloeil, L., and S.
                        Madanapalli, "IPv6 Router Advertisement Options
                        for DNS Configuration", RFC 6106, November 2010.

   [RFC3646]   Droms, R., Ed., "DNS Configuration options for
                        Dynamic Host Configuration Protocol for IPv6
                        (DHCPv6)", RFC 3646, December 2003.

   [RFC3315]   Droms, R., Ed., Bound, J., Volz, B., Lemon, T.,
                        Perkins, C., and M. Carney, "Dynamic Host
                        Configuration Protocol for IPv6 (DHCPv6)",
                        RFC 3315, July 2003.

   [RFC3736]   Droms, R., "Stateless Dynamic Host Configuration
                        Protocol (DHCP) Service for IPv6", RFC 3736,
                        April 2004.

   [RFC6275]   Perkins, C., Ed., Johnson, D., and J. Arkko,
                        "Mobility Support in IPv6", RFC 6275, July 2011.

   [RFC5213]   Gundavelli, S., Leung, K., Devarapalli, V.,
                        Chowdhury, K., and B. Patil, "Proxy Mobile IPv6",
                        RFC 5213, August 2008.

   [RFC5949]   Yokota, H., Chowdhury, K., Koodli, R., Patil, B.,
                        and F. Xia, "Fast Handovers for Proxy Mobile
                        IPv6", RFC 5949, September 2010.

   [RFC3963]   Devarapalli, V., Wakikawa, R., Petrescu, A., and
                        P. Thubert, "Network Mobility (NEMO) Basic Support
                        Protocol", RFC 3963, January 2005.

   [RFC7333]   Chan, H., Liu, D., Seite, P., Yokota, H., and J.
                        Korhonen, "Requirements for Distributed Mobility
                        Management", RFC 7333, August 2014.

   [RFC7429]   Liu, D., Zuniga, JC., Seite, P., Chan, H., and CJ.
                        Bernardos, "Distributed Mobility Management:
                        Current Practices and Gap Analysis", RFC 7429,
                        January 2015.

   [RFC1034]   Mockapetris, P., "Domain Names - Concepts and
                        Facilities", RFC 1034, November 1987.

   [RFC1035]   Mockapetris, P., "Domain Names - Implementation
                        and Specification", RFC 1035, November 1987.

   [RFC3971]   Arkko, J., Ed., "SEcure Neighbor Discovery
                        (SEND)", RFC 3971, March 2005.

   [RFC6763]   Cheshire, S. and M. Krochmal, "DNS-Based Service
                        Discovery", RFC 6763, February 2013.

   [RFC6762]   Cheshire, S. and M. Krochmal, "Multicast DNS",
                        RFC 6762, February 2013.

14.2. Informative References

   [DSRC-WAVE]   Morgan, Y., "Notes on DSRC & WAVE Standards Suite:
                        Its Architecture, Design, and Characteristics",
                        IEEE Communications Surveys & Tutorials, 12(4),
                        2012.

   [IEEE-802.11p]   IEEE Std 802.11p, "Part 11: Wireless LAN Medium
                        Access Control (MAC) and Physical Layer (PHY)
                        Specifications Amendment 6: Wireless Access in
                        Vehicular Environments", June 2010.

   [IEEE-802.11a]   IEEE Std 802.11a, "Part 11: Wireless LAN Medium
                        Access Control (MAC) and Physical Layer (PHY)
                        specifications: High-speed Physical Layer in the 5
                        GHZ Band", September 1999.

   [ID-VN-Survey]   Jeong, J., Ed., Cespedes, S., Benamar, N., and J.
                        Haerri, "Survey on IP-based Vehicular Networking
                        for Intelligent Transportation Systems",

                       draft-jeong-its-vehicular-networking-survey-01
                       (work in progress), July 2016.

   [ID-DNSNA]   Jeong, J., Ed., Lee, S., and J. Park, "DNS Name
                       Autoconfiguration for Internet of Things Devices",
                       draft-jeong-its-iot-dns-autoconf-01 (work in
                       progress), July 2016.

   [ID-Vehicular-ND]   Jeong, J., Ed., Shen, Y., Jo, Y., Jeong, J., and
                       J. Lee, "IPv6 Neighbor Discovery for Prefix and
                       Service Discovery in Vehicular Networks",
                       draft-jeong-its-vehicular-neighbor-discovery-00
                       (work in progress), July 2016.

   [VN-Security]   Moustafa, H., Bourdon, G., and Y. Gourhant,
                       "Providing Authentication and Access Control in
                       Vehicular Network Environment", IFIP TC-
                       11 International Information Security Conference,
                       May 2006.

   [Securing-VCOMM]   Fernandez, P., Santa, J., Bernal, F., and A.
                       Skarmeta, "Securing Vehicular IPv6
                       Communications", IEEE Transactions on Dependable
                       and Secure Computing, January 2016.

   [RFC4086]   Eastlake 3rd, D., Schiller, J., and S. Crocker,
                       "Randomness Requirements for Security", RFC 4086,
                       June 2005.

   [RFC4941]   Narten, T., Draves, R., and S. Krishnan, "Privacy
                       Extensions for Stateless Address Autoconfiguration
                       in IPv6", RFC 4941, September 2007.

Appendix A. Changes from draft-jeong-its-v2i-problem-statement-02

   The following changes are made from
   draft-jeong-its-v2i-problem-statement-02:

   o In Section 12, the considerations on security and privacy are
      enhanced.

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

    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

      Survey on IP-based Vehicular Networking for Intelligent Transportation
                                 Systems
              draft-jeong-ipwave-vehicular-networking-survey-02

Abstract

   This document surveys the 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. Finally, this document summarizes
   and analyzes the previous research activities that use IPv4 or IPv6
   for vehicular networking.

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

This Internet-Draft will expire on October 1, 2017.

Copyright Notice

Table of Contents

1. Introduction

   Nowadays vehicular networks have been focused on the driving safety,
   driving efficiency, and infotainment in road networks. For the
   driving safety, IEEE has standardized Wireless Access in Vehicular
   Environments (WAVE) standards, such as IEEE 802.11p, IEEE 1609.3, and
   IEEE 1609.4 [VIP-WAVE]. 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 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 V2V), mobility management, and
   security. 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 infotainment. 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:

   o Road-Side Unit (RSU): A node that has Dedicated Short-Range
      Communications (DSRC) device for wireless communications with
      vehicles and is connected to the Internet. An RSU is usually
      deployed at an intersection.

   o Vehicle: A node that has DSRC device for wireless communications
      with vehicles and RSUs. A vehicle may also have a GPS-navigation
      system for efficient driving.

   o Traffic Control Center (TCC): A node that maintains road
      infrastructure information (e.g., RSUs and traffic signals),
      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.

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 addressed 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
   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 ratio 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 1609.4 specified a WAVE
stack of protocols and includes IPv6 as a network layer protocol in
data plane. 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 infotainment
applications is also considered. Thus, in order to support
infotainment 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 pseudonimity 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
at 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. The innovative aspect is an early proposal to separate the
Control 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.

9.1. IEEE Guide for Wireless Access in Vehicular Environments (WAVE) -
     Architecture

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.

9.2. IEEE Standard for Wireless Access in Vehicular Environments (WAVE)
      - Networking Services

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
(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.

9.3.   ETSI Intelligent Transport Systems: Transmission of IPv6 Packets
       over GeoNetworking Protocols

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 to distribute other IPv6 link-local
multicast traffic and, at the same time, to reach 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 neighbour 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.

9.4.   ISO Intelligent Transport Systems: Communications Access for Land
       Mobiles (CALM) Using IPv6 Networking

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 stations (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. 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 infotainment. 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.

11. 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).

12. Acknowledgements

13. References

13.1. Normative References

[RFC2119]   Bradner, S., "Key words for use in
                             RFCs to Indicate Requirement Levels",
                             BCP 14, RFC 2119, March 1997.

[RFC5889]   Baccelli, E. and M. Townsley, "IP
                             Addressing Model in Ad Hoc Networks",

                                   RFC 5889, September 2010.

   [RFC5949]   Yokota, H., Chowdhury, K., Koodli, R.,
                                   Patil, B., and F. Xia, "Fast Handovers
                                   for Proxy Mobile IPv6", RFC 5949,
                                   September 2010.

13.2. Informative References

   [Address-Autoconf]   Fazio, M., Palazzi, C., Das, S., and
                                   M. Gerla, "Automatic IP Address
                                   Configuration in VANETs",
                                   ACM International Workshop on
                                   Vehicular Inter-Networking,
                                   September 2016.

   [Address-Assignment]   Kato, T., Kadowaki, K., Koita, T., and
                                   K. Sato, "Routing and Address
                                   Assignment using Lane/Position
                                   Information in a Vehicular Ad-hoc
                                   Network", IEEE Asia-Pacific Services
                                   Computing Conference, December 2008.

   [GeoSAC]   Baldessari, R., Bernardos, C., and M.
                                   Calderon, "GeoSAC - Scalable Address
                                   Autoconfiguration for VANET Using
                                   Geographic Networking Concepts",
                                   IEEE International Symposium on
                                   Personal, Indoor and Mobile Radio
                                   Communications, September 2008.

   [Identities-Management]   Wetterwald, M., Hrizi, F., and P.
                                   Cataldi, "Cross-layer Identities
                                   Management in ITS Stations",
                                   10th International Conference on ITS
                                   Telecommunications, November 2010.

   [VIP-WAVE]   Cespedes, S., Lu, N., and X. Shen,
                                   "VIP-WAVE: On the Feasibility of IP
                                   Communications in 802.11p Vehicular
                                   Networks", IEEE Transactions on
                                   Intelligent Transportation Systems,
                                   March 2013.

   [IPv6-WAVE]   Baccelli, E., Clausen, T., and R.
                                   Wakikawa, "IPv6 Operation for WAVE -
                                   Wireless Access in Vehicular
                                   Environments", IEEE Vehicular

                               Networking Conference, December 2010.

   [Vehicular-Network-Framework] Jemaa, I., Shagdar, O., and T. Ernst,
                               "A Framework for IP and non-IP
                               Multicast Services for Vehicular
                               Networks", Third International
                               Conference on the Network of the
                               Future, November 2012.

   [Joint-IP-Networking]   Petrescu, A., Boc, M., and C. Ibars,
                               "Joint IP Networking and Radio
                               Architecture for Vehicular Networks",
                               11th International Conference on ITS
                               Telecommunications, August 2011.

   [FleetNet]   Bechler, M., Franz, W., and L. Wolf,
                               "Mobile Internet Access in FleetNet",
                               13th Fachtagung Kommunikation in
                               verteilten Systemen, February 2001.

   [Vehicular-DTN]   Soares, V., Farahmand, F., and J.
                               Rodrigues, "A Layered Architecture for
                               Vehicular Delay-Tolerant Networks",
                               IEEE Symposium on Computers and
                               Communications, July 2009.

   [IP-Passing-Protocol]   Chen, Y., Hsu, C., and W. Yi, "An IP
                               Passing Protocol for Vehicular Ad Hoc
                               Networks with Network Fragmentation",
                               Elsevier Computers & Mathematics with
                               Applications, January 2012.

   [VANET-Geo-Routing]   Tsukada, M., Jemaa, I., Menouar, H.,
                               Zhang, W., Goleva, M., and T. Ernst,
                               "Experimental Evaluation for IPv6 over
                               VANET Geographic Routing",
                               IEEE International Wireless
                               Communications and Mobile Computing
                               Conference, June 2010.

   [H-DMM]   Nguyen, T. and C. Bonnet, "A Hybrid
                               Centralized-Distributed Mobility
                               Management for Supporting Highly
                               Mobile Users", IEEE International
                               Conference on Communications,
                               June 2015.

   [H-NEMO]   Nguyen, T. and C. Bonnet, "A Hybrid

                                   Centralized-Distributed Mobility
                                   Management Architecture for Network
                                   Mobility", IEEE International
                                   Symposium on a World of Wireless,
                                   Mobile and Multimedia Networks,
                                   June 2015.

   [NEMO-LMS]   Soto, I., Bernardos, C., Calderon, M.,
                                   Banchs, A., and A. Azcorra, "NEMO-
                                   Enabled Localized Mobility Support for
                                   Internet Access in Automotive
                                   Scenarios", IEEE Communications
                                   Magazine, May 2009.

   [NEMO-VANET]   Chen, Y., Hsu, C., and C. Cheng,
                                   "Network Mobility Protocol for
                                   Vehicular Ad Hoc Networks",
                                   Wiley International Journal of
                                   Communication Systems, November 2014.

   [PMIPv6-NEMO-Analysis]   Lee, J., Ernst, T., and N.
                                   Chilamkurti, "Performance Analysis of
                                   PMIPv6-Based Network MObility for
                                   Intelligent Transportation Systems",
                                   IEEE Transactions on Vehicular
                                   Technology, January 2012.

   [Vehicular-Network-MM]   Peng, Y. and J. Chang, "A Novel
                                   Mobility Management Scheme for
                                   Integration of Vehicular Ad Hoc
                                   Networks and Fixed IP Networks",
                                   Springer Mobile Networks and
                                   Applications, February 2010.

   [SDN-DMM]   Nguyen, T., Bonnet, C., and J. Harri,
                                   "SDN-based Distributed Mobility
                                   Management for 5G Networks",
                                   IEEE Wireless Communications and
                                   Networking Conference, April 2016.

   [Vehicular-IP-MM]   Cespedes, S., Shen, X., and C. Lazo,
                                   "IP Mobility Management for Vehicular
                                   Communication Networks: Challenges and
                                   Solutions", IEEE Communications
                                   Magazine, May 2011.

   [Securing-VCOMM]   Fernandez, P., Santa, J., Bernal, F.,
                                   and A. Skarmeta, "Securing Vehicular

                               IPv6 Communications",
                               IEEE Transactions on Dependable and
                               Secure Computing, January 2016.

   [VNET-AAA]   Moustafa, H., Bourdon, G., and Y.
                               Gourhant, "Providing Authentication
                               and Access Control in Vehicular
                               Network Environment", IFIP TC-
                               11 International Information Security
                               Conference, May 2006.

   [WAVE-1609.0]   IEEE 1609 Working Group, "IEEE Guide
                               for Wireless Access in Vehicular
                               Environments (WAVE) - Architecture",
                               IEEE Std 1609.0-2013, March 2014.

   [WAVE-1609.3]   IEEE 1609.3 Working Group, "IEEE
                               Standard for Wireless Access in
                               Vehicular Environments (WAVE) -
                               Networking Services", IEEE Std 1609.3-
                               2016, April 2016.

   [ETSI-GeoNetworking]   ETSI Technical Committee Intelligent
                               Transport Systems, "Intelligent
                               Transport Systems (ITS); Vehicular
                               Communications; GeoNetworking; Part 4:
                               Geographical addressing and forwarding
                               for point-to-point and point-to-
                               multipoint communications; Sub-part 1:
                               Media-Independent Functionality",
                               ETSI EN 302 636-4-1, May 2014.

   [ETSI-GeoNetwork-IPv6]   ETSI Technical Committee Intelligent
                               Transport Systems, "Intelligent
                               Transport Systems (ITS); Vehicular
                               Communications; GeoNetworking; Part 6:
                               Internet Integration; Sub-part 1:
                               Transmission of IPv6 Packets over
                               GeoNetworking Protocols", ETSI EN 302
                               636-6-1, October 2013.

   [RFC3963]   Devarapalli, V., Wakikawa, R.,
                               Petrescu, A., and P. Thubert, "Network
                               Mobility (NEMO) Basic Support
                               Protocol", RFC 3963, January 2005.

   [RFC4862]   Thomson, S., Narten, T., and T.
                               Jinmei, "IPv6 Stateless Address

                                    Autoconfiguration", RFC 4862,
                                    September 2007.

   [ISO-ITS-IPv6]   ISO/TC 204, "Intelligent Transport
                                    Systems - Communications Access for
                                    Land Mobiles (CALM) - IPv6
                                    Networking", ISO 21210:2012,
                                    June 2012.

Appendix A. Changes from
             draft-jeong-ipwave-vehicular-networking-survey-01

   The following changes are made from
   draft-jeong-ipwave-vehicular-networking-survey-01:

   o In Section 4.4, cross-layer identities management in ITS stations
      is added for the IP address autoconfiguration of ITS stations
      (e.g., vehicles) in vehicular networks using multiple access
      network technologies.

   o Typos are corrected.

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

Michelle Wetterwald
FBConsulting
21, Route de Luxembourg
Wasserbillig, Luxembourg L-6633
Luxembourg

EMail: Michelle.Wetterwald@gmail.com