Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 4, 2017

J. Jeong
Sungkyunkwan University
S. Cespedes
Universidad de Chile
N. Benamar
Moulay Ismail University
J. Haerri
EURECOM

October 31, 2016

Survey on IP-based Vehicular Networking for Intelligent Transportation Systems
draft-jeong-ipwave-vehicular-networking-survey-00

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 summarizes and analyzes the previous research activities that use IPv4 or IPv6 for vehicular networking.

This Internet-Draft will expire on May 4, 2017.

Table of Contents

1. Introduction 5
2. Requirements Language 5
3. Terminology 5
4. IP Address Autoconfiguration 6
4.1. Automatic IP Address Configuration in VANETs 6
4.2. Routing and Address Assignment using Lane/Position Information in a Vehicular Ad-hoc Network 6
4.3. GeoSAC: Scalable Address Autoconfiguration for VANET Using Geographic Networking Concepts 7
4.4. Key Observations 8
5. Vehicular Network Architecture 8
5.1. VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks 8
5.2. IPv6 Operation for WAVE - Wireless Access in Vehicular Environments 9
5.3. A Framework for IP and non-IP Multicast Services for Vehicular Networks 10
5.4. Joint IP Networking and Radio Architecture for Vehicular Networks 10
5.5. Mobile Internet Access in FleetNet 11
5.6. A Layered Architecture for Vehicular Delay-Tolerant Networks 12
5.7. Key Observations 13
6. Vehicular Network Routing 13
6.1. An IP Passing Protocol for Vehicular Ad Hoc Networks with Network Fragmentation 13
6.2. Experimental Evaluation for IPv6 over VANET Geographic Routing 14
6.3. Key Observations 15
7. Mobility Management in Vehicular Networks 15
7.1. A Hybrid Centralized-Distributed Mobility Management for Supporting Highly Mobile Users 15
7.2. A Hybrid Centralized-Distributed Mobility Management Architecture for Network Mobility 16
7.3. NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios 17
7.4. Network Mobility Protocol for Vehicular Ad Hoc Networks . 18
7.5. Performance Analysis of PMIPv6-Based Network MObility for Intelligent Transportation Systems 18
7.6. A Novel Mobility Management Scheme for Integration of Vehicular Ad Hoc Networks and Fixed IP Networks 19
7.7. SDN-based Distributed Mobility Management for 5G Networks 19
7.8. IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions 20
7.9. Key Observations 21

8. Vehicular Network Security 22
8.1. Securing Vehicular IPv6 Communications 22
8.2. Providing Authentication and Access Control in Vehicular Network Environment 22
8.3. Key Observations 23
9. Summary and Analysis 23
10. Security Considerations 24
11. Acknowledgements 24
12. References 25
12.1. Normative References 25
12.2. Informative References 25
Appendix A. Changes from draft-jeong-its-vehicular-networking-survey-01 . . . 28

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:

- 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.

- 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.

- 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 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. 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 Neighbor Discovery (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.

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 neighbor discovery (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 secuirty 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. 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 neighbor discovery (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.

10. 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).

11. Acknowledgements

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning). This work was supported in part by ICT R&D program of MSIP/IITP (14-824-09-013, Resilient Cyber-Physical Systems Research) and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning. This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

12. References

12.1. 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.

12.2. 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.

[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.

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

The following changes were made from draft-jeong-its-vehicular-networking-survey-01:

- Vehicular Network Security section is added.
- Key Observations subsection is added for each section.
- The editorial corrections are made.

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

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 20, 2017

J. Jeong
Sungkyunkwan University
T. Oh
Rochester Institute of Technology
July 19, 2016

Problem Statement for Vehicle-to-Infrastructure Networking
draft-jeong-its-v2i-problem-statement-02

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, such as prefix discovery, prefix exchange, and service discovery.

This Internet-Draft will expire on January 20, 2017.

Table of Contents

1. Introduction 3
2. Requirements Language 3
3. Terminology 4
4. Overview 4
5. Internetworking between the Vehicle and RSU Networks 6
6. IPv6 Addressing 7
7. Neighbor Discovery 7
8. IP Address Autoconfiguration 7
9. DNS Naming Service 8
10. IP Mobility Management 8
11. Service Discovery 9
12. Security Considerations 9
13. Acknowledgements 10
14. References 10
14.1. Normative References 10
14.2. Informative References 12
Appendix A. Changes from draft-jeong-its-v2i-problem-statement-01 13

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:

- 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.

- 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.

- 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.

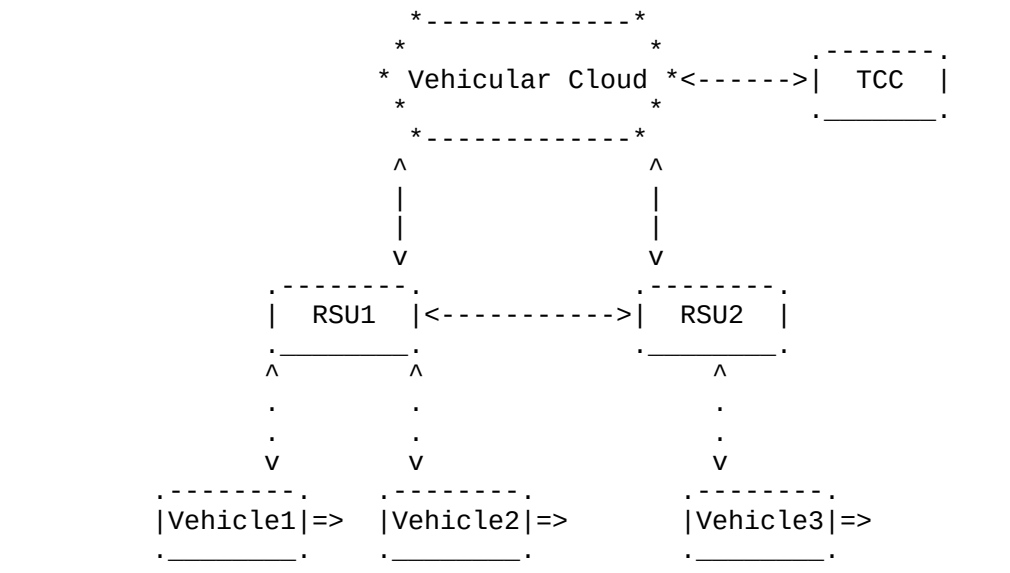


Figure 1: The Network Configuration for V2I Networking

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.

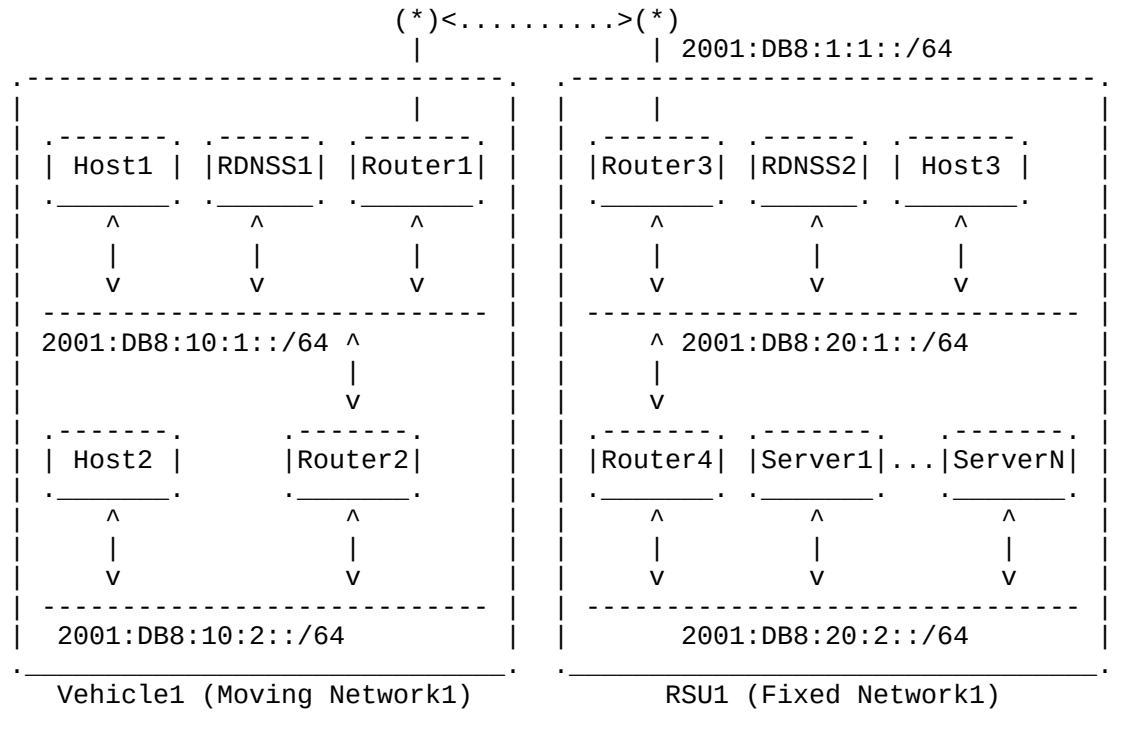


Figure 2: Internetworking between Vehicle Network and RSU Network

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. 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.

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

This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No.R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning). This work was supported in part by ICT R&D program of MSIP/IITP (14-824-09-013, Resilient Cyber-Physical Systems Research) and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning.

This document has greatly benefited from inputs by Alexandre Petrescu, Thierry Ernst, Nabil Benamar, Jerome Haerri, Richard Roy, and Sandra Cespedes. The authors sincerely appreciate their contributions.

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.

Appendix A. Changes from draft-jeong-its-v2i-problem-statement-01

The following changes were made from draft-jeong-its-v2i-problem-statement-01:

- In Section 11, an extension of IPv6 ND is added for service discovery along with prefix discovey.

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

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 4, 2017

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

J. Lee
Sangmyung University
T. Ernst
YoGoKo
T. Li
Peloton Technology
October 31, 2016

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

Abstract

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

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

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

Status of This Memo

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

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

working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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

This Internet-Draft will expire on May 4, 2017.

Table of Contents

1. Introduction 3
2. Terminology 5
3. Communication Scenarios where IEEE 802.11p Links are Used . . 6
4. Aspects introduced by 802.11p to 802.11 6
5. Design Considerations 10
5.1. Vehicle ID 10
5.2. Non IP Communications 10
5.3. Reliability Requirements 11
5.4. Privacy requirements 12
5.5. Authentication requirements 13
5.6. Multiple interfaces 13
5.7. MAC Address Generation 14
5.8. Security Certificate Generation 14
6. Layering of IPv4 and IPv6 over 802.11p as over Ethernet . . . 15
6.1. Maximum Transmission Unit (MTU) 15
6.2. Frame Format 16
6.2.1. Ethernet Adaptation Layer 17
6.2.2. MAC Address Resolution 18
6.3. Link-Local Addresses 19
6.4. Address Mapping 19
6.4.1. Address Mapping -- Unicast 19

6.4.2. Address Mapping -- Multicast 19
6.5. Stateless Autoconfiguration 20
6.6. Subnet Structure 21
7. Handovers between OCB links 22
8. Example IPv6 Packet captured over a IEEE 802.11p link 24
8.1. Capture in Monitor Mode 25
8.2. Capture in Normal Mode 27
9. Security Considerations 29
10. IANA Considerations 30
11. Contributors 30
12. Acknowledgements 30
13. References 31
13.1. Normative References 31
13.2. Informative References 32
Appendix A. ChangeLog 35
Appendix B. Explicit Prohibition of IPv6 on Channels Related to ITS Scenarios using 802.11p Networks - an Analysis 37
B.1. Interpretation of FCC and ETSI documents with respect to running IP on particular channels 37
B.2. Interpretations of Latencies of IP datagrams 38
Appendix C. Changes Needed on a software driver 802.11a to become a 802.11p driver . . . 38
Appendix D. Use of IPv6 over 802.11p for distribution of certificates 40
Authors' Addresses 41

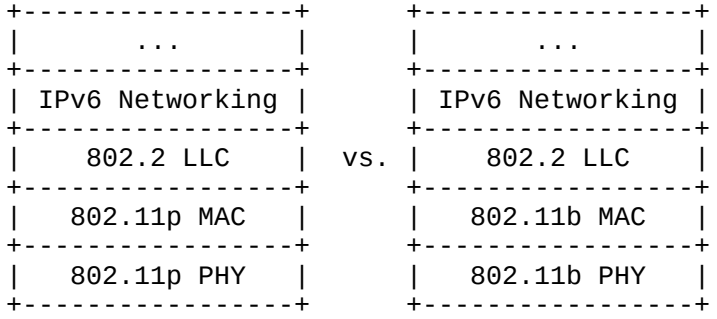
1. Introduction

This document describes the transmission of IPv6 packets on IEEE Std 802.11 OCB networks (earlier known as 802.11p). This involves the layering of IPv6 networking on top of the IEEE 802.11 MAC layer (with an LLC layer). Compared to running IPv6 over the Ethernet MAC layer, there is no modification required to the standards: IPv6 works fine directly over 802.11 OCB too (with an LLC layer).

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

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

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



However, there are several deployment considerations to optimize the performances of running IPv6 over 802.11p (e.g. in the case of handovers between 802.11p Access Points, or the consideration of using the IP security layer).

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

The document then concentrates on the parameters of layering IP over 802.11p as over Ethernet: MTU, Frame Format, Interface Identifier, Address Mapping, State-less Address Auto-configuration. The values of these parameters are precisely the same as IPv6 over Ethernet [RFC2464]: the recommended value of MTU to be 1500 octets, the Frame Format containing the Type 0x86DD, the rules for forming an Interface Identifier, the Address Mapping mechanism and the Stateless Address Auto-Configuration.

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

determine the MAC address used for an IPv4 address, exactly as is done for Ethernet.

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

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

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

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

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

2. Terminology

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

RSU: Road Side Unit.

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

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

802.11-OCB - IEEE 802.11-2012 text flagged by "dot11OCBActivated". This means: IEEE 802.11e for quality of service; 802.11j-2004 for half-clocked operations; and 802.11p for operation in the 5.9 GHz band and in mode OCB.

3. Communication Scenarios where IEEE 802.11p Links are Used

The IEEE 802.11p Networks are used for vehicular communications, as 'Wireless Access in Vehicular Environments'. The IP communication scenarios for these environments have been described in several documents, among which we refer the reader to one recently updated [I-D.petrescu-its-scenarios-reqs], about scenarios and requirements for IP in Intelligent Transportation Systems.

4. Aspects introduced by 802.11p to 802.11

In the IEEE 802.11 OCB mode, all nodes in the wireless range can directly communicate with each other without authentication/ association procedures. Briefly, the IEEE 802.11 OCB mode has the following properties:

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

The link 802.11p is specified in IEEE Std 802.11p(TM)-2010 [ieee802.11p-2010] as an amendment to the 802.11 specifications, titled "Amendment 6: Wireless Access in Vehicular Environments". Since then, these 802.11p amendments have been included in IEEE 802.11(TM)-2012 [ieee802.11-2012], titled "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"; the modifications are diffused

throughout various sections (e.g. 802.11p's Time Advertisement message is described in section 'Frame formats', and the operation outside the context of a BSS described in section 'MLME').

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

In order to delineate the aspects introduced by 802.11p to 802.11, we refer to the earlier [ieee802.11p-2010]. The amendment is concerned with vehicular communications, where the wireless link is similar to that of Wireless LAN (using a PHY layer specified by 802.11a/b/g/n), but which needs to cope with the high mobility factor inherent in scenarios of communications between moving vehicles, and between vehicles and fixed infrastructure deployed along roads. While 'p' is a letter just like 'a, b, g' and 'n' are, 'p' is concerned more with MAC modifications, and a little with PHY modifications; the others are mainly about PHY modifications. It is possible in practice to combine a 'p' MAC with an 'a' PHY by operating outside the context of a BSS with OFDM at 5.4GHz.

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

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

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

- Operation Outside the Context of a BSS (OCB): the 802.11p links are operated without a Basic Service Set (BSS). This means that the messages Beacon, Association Request/Response, Authentication Request/Response, and similar, are not used. The used identifier of BSS (BSSID) has a hexadecimal value always ff:ff:ff:ff:ff:ff (48 '1' bits, or the 'wildcard' BSSID), as opposed to an arbitrary BSSID value set by administrator (e.g. 'My-Home-AccessPoint').

The OCB operation - namely the lack of beacon-based scanning and lack of authentication - has a potentially strong impact on the use of the Mobile IPv6 protocol and on the protocols for IP layer security.

- Timing Advertisement: is a new message defined in 802.11p, which does not exist in 802.11a/b/g/n. This message is used by stations to inform other stations about the value of time. It is similar to the time as delivered by a GNSS system (Galileo, GPS, ...) or by a cellular system. This message is optional for implementation. At the date of writing, an experienced reviewer considers that currently no field testing has used this message. Another implementor considers this feature implemented in an initial manner. In the future, it is speculated that this message may be useful for very simple devices which may not have their own hardware source of time (Galileo, GPS, cellular network), or by vehicular devices situated in areas not covered by such network (in tunnels, underground, outdoors but shaded by foliage or buildings, in remote areas, etc.)

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

- Explicit prohibition of IPv6 on some channels relevant for the PHY of IEEE 802.11p, as opposed to IPv6 not being prohibited on any

channel on which 802.11a/b/g/n runs; for example, IPv6 is prohibited on the 'Control Channel' (number 178 at FCC/IEEE, and 180 at ETSI); for a detailed analysis of IEEE and ETSI prohibition of IP in particular channels see Appendix B.

- 'Half-rate' encoding: as the frequency range, this parameter is related to PHY, and thus has not much impact on the interface between the IP layer and the MAC layer. The standard IEEE 802.11p uses OFDM encoding at PHY, as other non-b 802.11 variants do. This considers 20MHz encoding to be 'full-rate' encoding, as the earlier 20MHz encoding which is used extensively by 802.11b. In addition to the full-rate encoding, the OFDM rates also involve 5MHz and 10MHz. The 10MHz encoding is named 'half-rate'. The encoding dictates the bandwidth and latency characteristics that can be afforded by the higher-layer applications of IP communications. The half-rate means that each symbol takes twice the time to be transmitted; for this to work, all 802.11 software timer values are doubled. With this, in certain channels of the "5.9GHz" band, a maximum bandwidth of 12Mbit/s is possible, whereas in other "5.9GHz" channels a minimal bandwidth of 1Mbit/s may be used. It is worth mentioning the half-rate encoding is an optional feature characteristic of OFDM PHY (compared to 802.11b's full-rate 20MHz), used by 802.11a before 802.11p used it. In addition to the half-rate (10MHz) used by 802.11p in some channels, some other 802.11p channels may use full-rate (20MHz) or quarter-rate(?) (5MHz) encoding instead.

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

- In vehicular communications using 802.11p links, there are strong privacy concerns with respect to addressing. While the 802.11p standard does not specify anything in particular with respect to MAC addresses, in these settings there exists a strong need for dynamic change of these addresses (as opposed to the non-vehicular settings - real wall protection - where fixed MAC addresses do not currently pose some privacy risks). This is further described in section Section 9.

Other aspects particular to 802.11p which are also particular to 802.11 (e.g. the 'hidden node' operation) may have an influence on the use of transmission of IPv6 packets on 802.11p networks. The subnet structure which may be assumed in 802.11p networks is strongly influenced by the mobility of vehicles.

5. Design Considerations

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

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

5.1. Vehicle ID

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

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

5.2. Non IP Communications

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

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

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

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

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

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

5.3. Reliability Requirements

The dynamically changing topology, short connectivity, mobile transmitter and receivers, different antenna heights, and many-to-many communication types, make IEEE 802.11-OCB links significantly different from other IEEE 802.11 links. Any IPv6 mechanism operating on IEEE 802.11-OCB link MUST support strong link asymetry, spatio-temporal link quality, fast address resolution and transmission.

IEEE 802.11-OCB strongly differs from other 802.11 systems to operate outside of the context of a Basic Service Set. This means in practice that IEEE 802.11-OCB does not rely on a Base Station for all Basic Service Set management. In particular, IEEE 802.11-OCB SHALL NOT use beacons. Any IPv6 mechanism requiring L2 services from IEEE 802.11 beacons MUST support an alternative service.

Channel scanning being disabled, IPv6 over IEEE 802.11-OCB MUST implement a mechanism for transmitter and receiver to converge to a common channel.

Authentication not being possible, IPv6 over IEEE 802.11-OCB MUST implement an distributed mechanism to authenticate transmitters and receivers without the support of a DHCP server.

Time synchronization not being available, IPv6 over IEEE 802.11-OCB MUST implement a higher layer mechanism for time synchronization between transmitters and receivers without the support of a NTP server.

The IEEE 802.11-OCB link being asymetic, IPv6 over IEEE 802.11-OCB MUST disable management mechanisms requesting acknowledgements or replies.

The IEEE 802.11-OCB link having a short duration time, IPv6 over IEEE 802.11-OCB MUST implement fast IPv6 mobility management mechanisms.

5.4. Privacy requirements

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

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

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

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

Changing MAC and IPv6 addresses will disrupt communications, which goes against the reliability requirements expressed in [TS103097]. We will assume that the renumbering events happen only during "safe" periods, e.g. when the vehicle has come to a full stop. The

determination of such safe periods is the responsibility of implementors. In automobile settings it is common to decide that certain operations (e.g. software update, or map update) must happen only during safe periods.

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

5.5. Authentication requirements

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

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

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

5.6. Multiple interfaces

There are considerations for 2 or more IEEE 802.11-OCB interface cards per vehicle. For each vehicle taking part in road traffic, one IEEE 802.11-OCB interface card MUST be fully allocated for Non IP safety-critical communication. Any other IEEE 802.11-OCB may be used for other type of traffic.

The mode of operation of these other wireless interfaces is not clearly defined yet. One possibility is to consider each card as an independent network interface, with a specific MAC Address and a set of IPv6 addresses. Another possibility is to consider the set of these wireless interfaces as a single network interface (not including the IEEE 802.11-OCB interface used by Non IP safety critical communications). This will require specific logic to ensure, for example, that packets meant for a vehicle in front are actually sent by the radio in the front, or that multiple copies of

the same packet received by multiple interfaces are treated as a single packet. Treating each wireless interface as a separate network interface pushes such issues to the application layer.

The privacy requirements of Section 5.4 imply that if these multiple interfaces are represented by many network interface, a single renumbering event SHALL cause renumbering of all these interfaces. If one MAC changed and another stayed constant, external observers would be able to correlate old and new values, and the privacy benefits of randomization would be lost.

The privacy requirements of Non IP safety-critical communications imply that if a change of pseudonyme occurs, renumbering of all other interfaces SHALL also occur.

5.7. MAC Address Generation

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

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

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

5.8. Security Certificate Generation

When designing the IPv6 over 802.11-OCB address mapping, we will assume that the MAC Addresses will change during well defined "renumbering events". So MUST also the Security Certificates. Unless unavailable, the Security Certificate Generation mechanisms SHOULD follow the specification in IEEE 1609.2 [ieee16094] or ETSI TS 103 097 [TS103097]. These security mechanisms have the following characteristics:

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

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

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

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

6.1. Maximum Transmission Unit (MTU)

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

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

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

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

It is possible that the application layer fragments.

Non-IP packets such as WAVE Short Message Protocol (WSMP) can be delivered on 802.11-OCB links. Specifications of these packets are

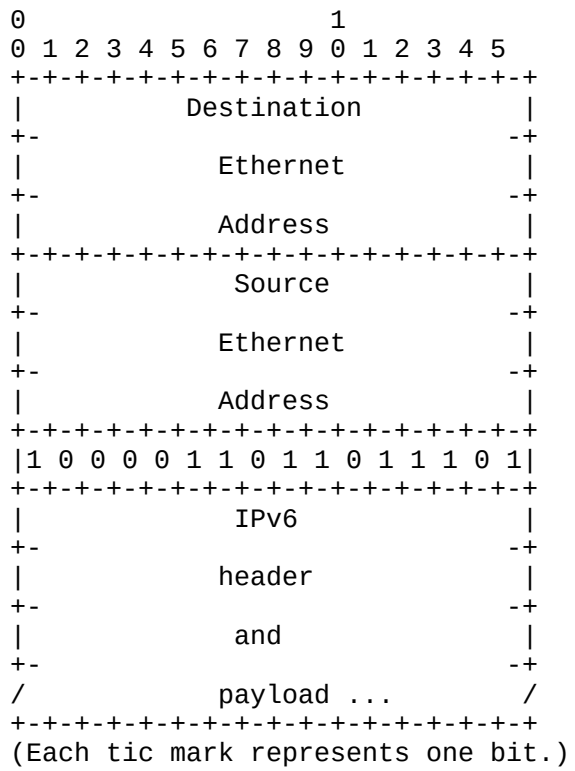
out of scope of this document, and do not impose any limit on the MTU size, allowing an arbitrary number of 'containers'. Non-IP packets such as ETSI 'geonet' packets have an MTU of 1492 bytes.

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

6.2. Frame Format

IP packets are transmitted over 802.11p as standard Ethernet packets. As with all 802.11 frames, an Ethernet adaptation layer is used with 802.11p as well. This Ethernet Adaptation Layer 802.11-to-Ethernet is described in Section 6.2.1. The Ethernet Type code (EtherType) for IPv6 is 0x86DD (hexadecimal 86DD, or otherwise #86DD). The EtherType code for IPv4 is 0x0800.

The Frame format for transmitting IPv6 on 802.11p networks is the same as transmitting IPv6 on Ethernet networks, and is described in section 3 of [RFC2464]. The Frame format for transmitting IPv4 on 802.11p networks is the same as transmitting IPv4 on Ethernet networks and is described in [RFC0894]. For sake of completeness, the frame format for transmitting IPv6 over Ethernet is illustrated below:

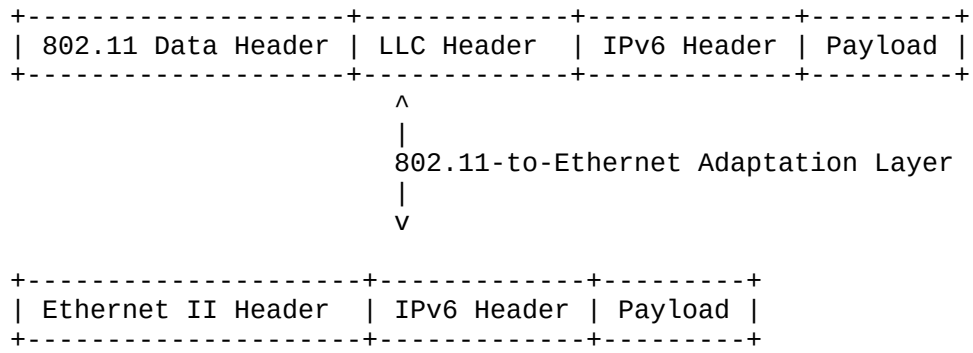


(Each tic mark represents one bit.)

6.2.1. Ethernet Adaptation Layer

In general, an ’adaptation’ layer is inserted between a MAC layer and the Networking layer. This is used to transform some parameters between their form expected by the IP stack and the form provided by the MAC layer. For example, an 802.15.4 adaptation layer may perform fragmentation and reassembly operations on a MAC whose maximum Packet Data Unit size is smaller than the minimum MTU recognized by the IPv6 Networking layer. Other examples involve link-layer address transformation, packet header insertion/removal, and so on.

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



The Receiver and Transmitter Address fields in the 802.11 Data Header contain the same values as the Destination and the Source Address fields in the Ethernet II Header, respectively. The value of the Type field in the LLC Header is the same as the value of the Type field in the Ethernet II Header. The other fields in the Data and LLC Headers are not used by the IPv6 stack.

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

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

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

The value of the field "Type/Subtype" in the 802.11 Data header is 0x0020. The value of the field "Type/Subtype" in the 802.11 QoS header is 0x0028.

6.2.2. MAC Address Resolution

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

6.3. Link-Local Addresses

For IPv6, the link-local address of an 802.11p interface is formed in the same manner as on an Ethernet interface. This manner is described in section 5 of [RFC2464].

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

6.4. Address Mapping

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

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

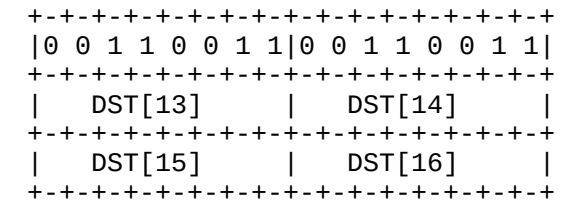
6.4.1. Address Mapping -- Unicast

6.4.2. Address Mapping -- Multicast

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

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

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



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

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

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

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

6.5. Stateless Autoconfiguration

The Interface Identifier for an 802.11p interface is formed using the same rules as the Interface Identifier for an Ethernet interface; this is described in section 4 of [RFC2464]. No changes are needed, but some care must be taken when considering the use of the SLAAC procedure.

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

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

would be

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

The bits in the the interface identifier have no generic meaning and the identifier should be treated as an opaque value. The bits 'Universal' and 'Group' in the identifier of an 802.11p interface are significant, as this is a IEEE link-layer address. The details of this significance are described in [I-D.ietf-6man-ug].

As with all Ethernet and 802.11 interface identifiers, the identifier of an 802.11p interface may involve privacy risks. A vehicle embarking an On-Board Unit whose egress interface is 802.11p may expose itself to eavesdropping and subsequent correlation of data; this may reveal data considered private by the vehicle owner. The address generation mechanism should consider these aspects, as described in [I-D.ietf-6man-ipv6-address-generation-privacy].

6.6. Subnet Structure

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

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

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

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

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

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

7. Handovers between OCB links

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

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

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

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

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

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

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

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

To summarize, efficient handovers between OCB links can be performed by using a combination of existing mechanisms. In order to improve the default router unreachability detection, the RSU and moving stations should use the Mobile IPv6 "Advertisement Interval Option" as well as rely on the NUD mechanism. In order to allow the moving station to detect potential default router faster, the RSU should also be able to be configured with a smaller minimum RA interval such

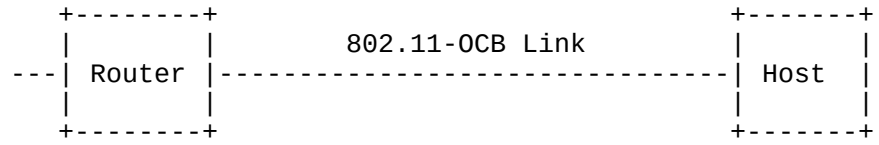
as the one recommended by Mobile IPv6. When multiple RSUs are available at the same time, the moving station should perform the handover decision based on the signal quality. Finally, optimistic DAD can be used to reduce the handover delay.

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

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

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

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



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

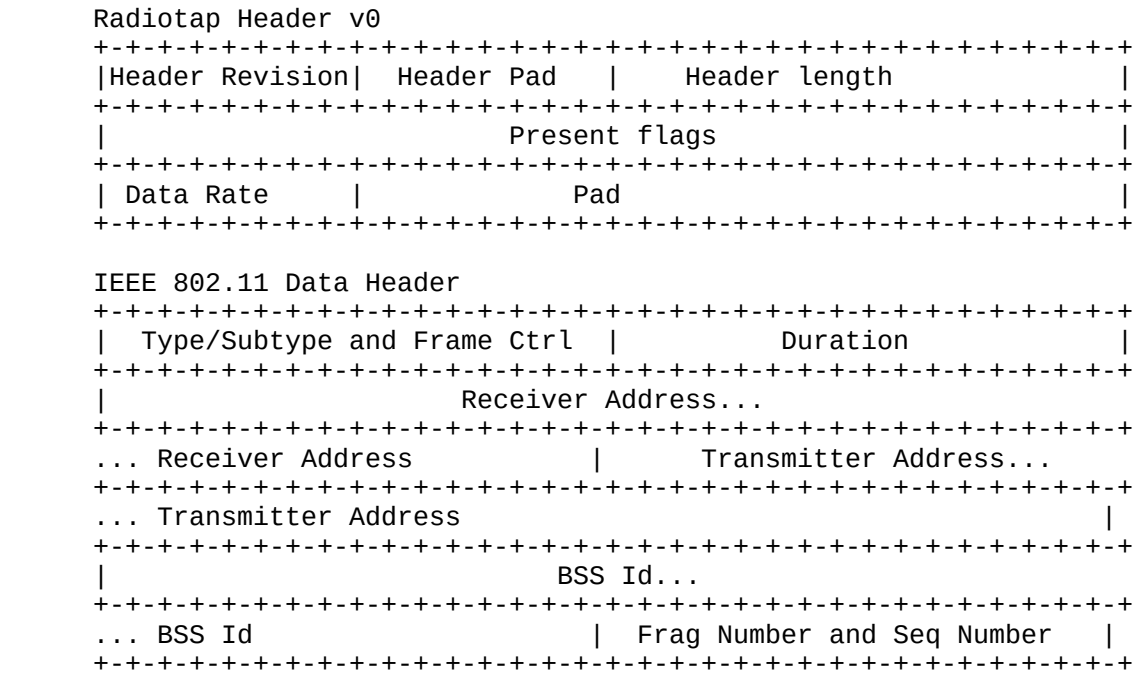
Overall, the captured message is identical with a capture of an IPv6 packet emitted on a 802.11b interface. The contents are precisely similar.

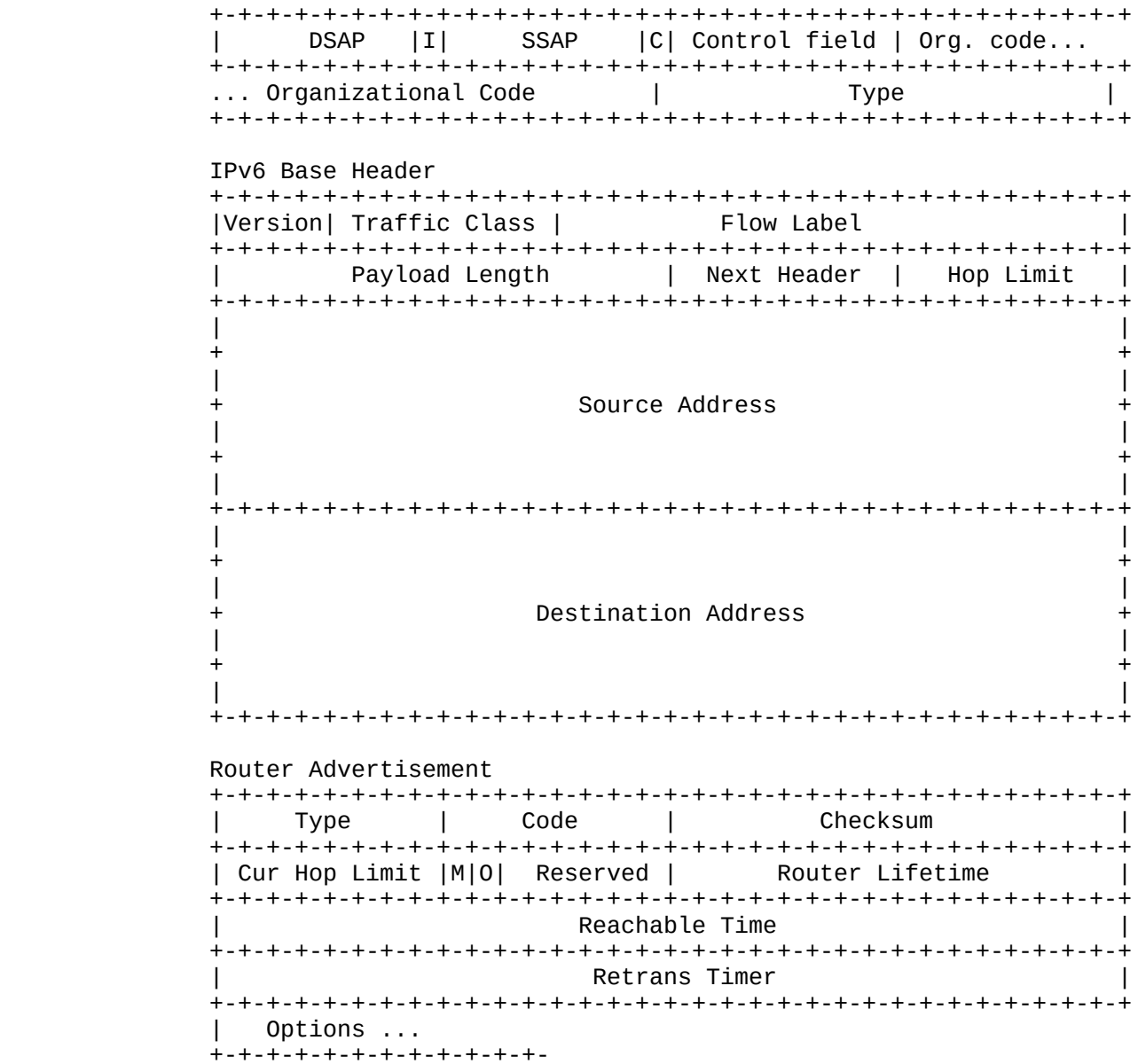
The popular wireshark network protocol analyzer is a free software tool for Windows and Unix. It includes a dissector for 802.11p features along with all other 802.11 features (i.e. it displays these features in a human-readable format).

8.1. Capture in Monitor Mode

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

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





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

The value of the Transmitter address in the IEEE 802.11 Data Header is set to a 48bit value. The value of the destination address is

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

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

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

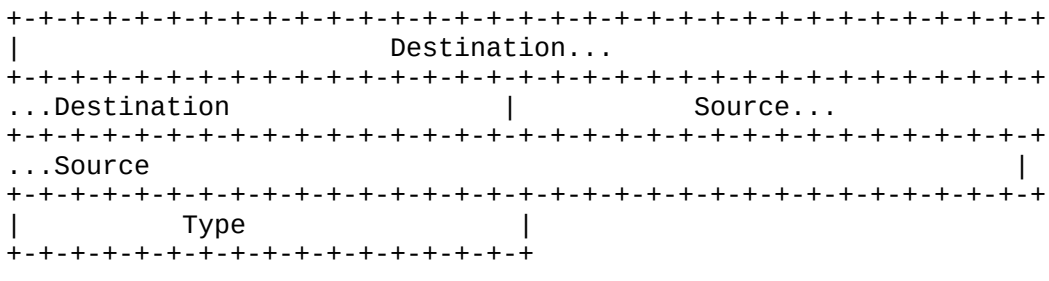
The IPv6 header contains the link local address of the router (source) configured via EUI-64 algorithm, and destination address set to ff02::1. Recent versions of network protocol analyzers (e.g. Wireshark) provide additional informations for an IP address, if a geolocalization database is present. In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

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

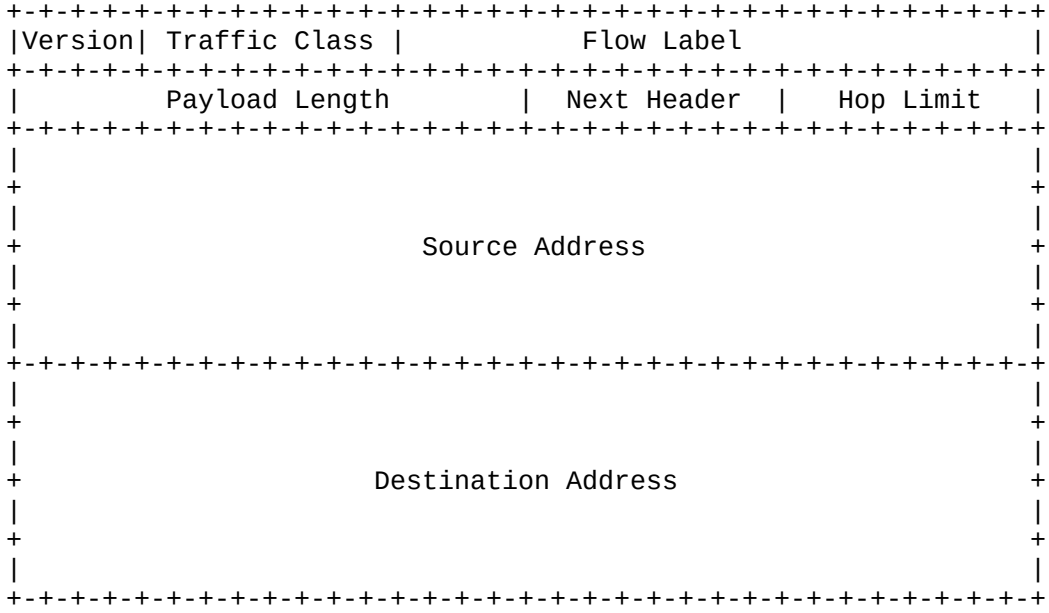
8.2. Capture in Normal Mode

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

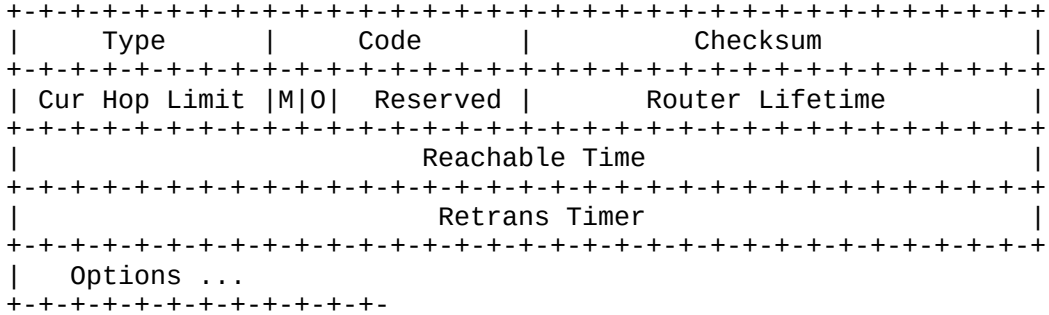
Ethernet II Header



IPv6 Base Header



Router Advertisement



One notices that the Radiotap Header is not prepended, and that the IEEE 802.11 Data Header and the Logical-Link Control Headers are not present. On another hand, a new header named Ethernet II Header is present.

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

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

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

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

9. Security Considerations

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

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

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

As with all Ethernet and 802.11 interface identifiers, there may exist privacy risks in the use of 802.11p interface identifiers. However, in outdoors vehicular settings, the privacy risks are more important than in indoors settings. New risks are induced by the possibility of attacker sniffers deployed along routes which listen for IP packets of vehicles passing by. For this reason, in the 802.11p deployments, there is a strong necessity to use protection tools such as dynamically changing MAC addresses. This may help mitigate privacy risks to a certain level. On another hand, it may have an impact in the way typical IPv6 address auto-configuration is performed for vehicles (SLAAC would rely on MAC addresses amd would hence dynamically change the affected IP address), in the way the IPv6 Privacy addresses were used, and other effects.

10. IANA Considerations

11. Contributors

Romain Kuntz contributed extensively the concepts described in Section 7 about IPv6 handovers between links running outside the context of a BSS (802.11p links).

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

Marios Makassikis, Jose Santa Lozano, Albin Severinson and Alexey Voronov provided significant feedback on the experience of using IPv4 and IPv6 messages over 802.11-OCB in initial trials.

12. Acknowledgements

The authors would like to thank Witold Klaudel, Ryuji Wakikawa, Emmanuel Baccelli, John Kenney, John Moring, Francois Simon, Dan Romascanu, Konstantin Khait, Ralph Droms, Richard Roy, Ray Hunter, Tom Kurihara, Michelle Wetterwald, Michal Sojka, Jan de Jongh, Suresh Krishnan, Dino Farinacci, Vincent Park and Gloria Gwynne. Their valuable comments clarified certain issues and generally helped to improve the document.

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

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

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

13. References

13.1. Normative References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13.2. Informative References

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

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

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

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

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

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

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

[ieee802.11-2012]
"802.11-2012 - IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Downloaded on October 17th, 2013, from IEEE Standards, document freely available at URL http://standards.ieee.org/findstds/standard/802.11-2012.html retrieved on October 17th, 2013.".

[ieee802.11p-2010]
"IEEE Std 802.11p(TM)-2010, IEEE Standard for Information Technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 6: Wireless Access in Vehicular Environments; document freely available at URL http://standards.ieee.org/getieee802/download/802.11p-2010.pdf retrieved on September 20th, 2013.".

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

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

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

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

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

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

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

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

Appendix A. ChangeLog

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

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

- Added clarification about the "OCBActivated" qualifier in the the new IEEE 802.11-2012 document; this IEEE document integrates now all earlier 802.11p features; this also signifies the dissapearance of an IEEE IEEE 802.11p document altogether.
- Added explanation about FCC not prohibiting IP on channels, and comments about engineering advice and reliability of IP messages.
- Added possibility to use 6lowpan adaptation layer when in OCB mode.
- Added appendix about the distribution of certificates to vehicles by using IPv6-over-802.11p single-hop communications.
- Refined the explanation of ’half-rate’ mode.
- Added the privacy concerns and necessity of and potential effects of dynamically changing MAC addresses.

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

- updated authorship.
- added explanation about FCC not prohibiting IP on channels, and comments about engineering advice and reliability of IP messages.
- added possibility to use 6lowpan adaptation layer when in OCB mode.
- added appendix about the distribution of certificates to vehicles by using IPv6-over-802.11p single-hop communications.
- refined the explanation of ’half-rate’ mode.
- added the privacy concerns and necessity of and potential effects of dynamically changing MAC addresses.

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

- updated one author’s affiliation detail.
- added 2 more references to published literature about IPv6 over 802.11p.

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

- first version.

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

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

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

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

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

- In Europe, basically ETSI considers FCC’s "Control Channel" to be a "Service Channel", and defines a "Control Channel" to be in a slot considered by FCC as a "Service Channel". In detail, FCC’s "Control Channel" number 178 decimal with 10MHz width (5885MHz to 5895MHz) is defined by ETSI to be a "Service Channel", and is named ’G5-SCH2’ [etsi-302663-v1.2.1p-2013]. This channel is dedicated to ’ITS Road Safety’ by ETSI. Other channels are dedicated to ’ITS road traffic efficiency’ by ETSI. The ETSI’s "Control Channel" - the "G5-CCH" - number 180 decimal (not 178) is reserved as a 10MHz-width centered on 5900MHz (5895MHz to 5905MHz)

(the 5895MHz-5905MHz channel is a Service Channel for FCC). Compared to IEEE, ETSI makes no upfront statement with respect to IP and particular channels; yet it relates the 'In car Internet' applications ('When nearby a stationary public internet access point (hotspot), application can use standard IP services for applications.') to the 'Non-safety-related ITS application' [etsi-draft-102492-2-v1.1.1-2006]. Under an interpretation of an author of this Internet Draft, this may mean ETSI may forbid IP on the 'ITS Road Safety' channels, but may allow IP on 'ITS road traffic efficiency' channels, or on other 5GHz channels re-used from BRAN (also dedicated to Broadband Radio Access Networks).

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

B.2. Interpretations of Latencies of IP datagrams

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

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

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

Conditions for a 802.11a hardware to be 802.11p compliant:

- The chip must support the frequency bands on which the regulator recommends the use of ITS communications, for example using IEEE 802.11p layer, in France: 5875MHz to 5925MHz.

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

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

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

Changes needed on the network stack in OCB mode:

- Physical layer:

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

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

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

  MAC layer:

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

  * No encryption key or method must be used.

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

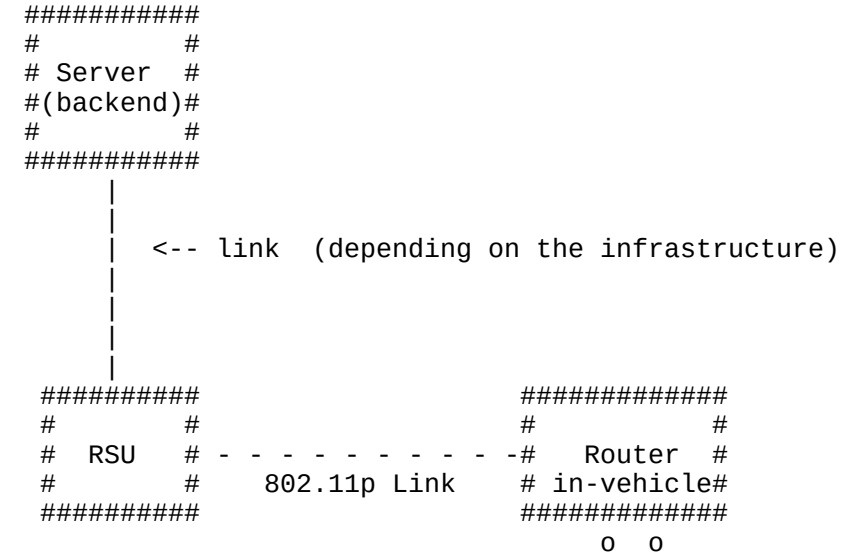
  * The functions related to joining a BSS (Association Request/ Response) and for authentication (Authentication Request/Reply, Challenge) are not called.

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

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

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

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



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

Authors' Addresses

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

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

Nabil Benamar
Moulay Ismail University
Morocco

Phone: +212670832236
Email: benamar73@gmail.com

Jerome Haerri
Eurecom
Sophia-Antipolis 06904
France

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

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

Email: huitema@huitema.net

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

Email: jonghyouk@smu.ac.kr

Thierry Ernst
YoGoKo
France

Email: thierry.ernst@yogoko.fr

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

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