Survey on IP-based Vehicular Networking for Intelligent Transportation Systems
draft-jeong-ipwave-vehicular-networking-survey-01

Abstract

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

Status of This Memo

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

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

Copyright Notice

Table of Contents

1. Introduction

   Nowadays vehicular networks have been focused on the driving safety,
   driving efficiency, and infotainment in road networks. For the
   driving safety, IEEE has standardized Wireless Access in Vehicular
   Environments (WAVE) standards, such as IEEE 802.11p, IEEE 1609.3, and
   IEEE 1609.4 [VIP-WAVE]. Along with these WAVE standards, IPv6 and
   Mobile IP protocols (e.g., MIPv4 and MIPv6) can be extended to
   vehicular networks.

   This document surveys the IP-based vehicular networking for
   Intelligent Transportation Systems (ITS), such as IP address
   autoconfiguration, vehicular network architecture, vehicular network
   routing (for multi-hop V2V, V2I, and V2V), mobility management, and
   security. This document summarizes and analyzes the previous
   research activities using IPv4 or IPv6 for vehicular networking.

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

2. Requirements Language

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

3. Terminology

   This document defines the following new terms:

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

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

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

vehicular cloud for vehicular networks.

4. IP Address Autoconfiguration

This section surveys IP address autoconfiguration schemes for vehicular networks.

4.1. Automatic IP Address Configuration in VANETs

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

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

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

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

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

   group corresponding to the lane.

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

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

   Baldessari et al. proposed an IPv6 scalable address autoconfiguration
   scheme called GeoSAC for vehicular networks [GeoSAC]. GeoSAC uses
   geographic networking concepts such that it combines the standard
   IPv6 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. Standard Activities for Vehicular Networks

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

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

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

IEEE 1609.0 provides a description of the WAVE system architecture and operations (called WAVE reference model) [WAVE-1609.0]. The reference model of a typical WAVE device includes two data plane protocol stacks (sharing a common lower stack at the data link and physical layers): (i) the standard Internet Protocol Version 6 (IPv6) and (ii) the WAVE Short Message Protocol (WSMP) designed for

optimized operation in a wireless vehicular environment. WAVE Short
Messages (WSM) may be sent on any channel. IP traffic is only
allowed on service channels (SCHs), so as to offload high-volume IP
traffic from the control channel (CCH).

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

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

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

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

WAVE Networking Services represent layer 3 (networking) and layer 4
(transport) of the Open Systems Interconnection (OSI) communications
stack. The purpose is then to provide addressing and routing
services within a WAVE system, enabling multiple stacks of upper
layers above WAVE Networking Services and multiple lower layers
beneath WAVE Networking Services. Upper layer support includes in-
vehicle applications offering safety and convenience to users.

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

The document provides requirements for IPv6 configuration, in
particular for the address setting. It specifies the details of the
different service primitives, among which is the WAVE Routing
Advertisement (WRA), part of the WAVE Service Advertisement (WSA).
When present, the WRA provides information about infrastructure
internetwork connectivity, allowing receiving devices to be
configured to participate in the advertised IPv6 network. For
example, an RSU can broadcast in the WRA portion of its WSA all the
information necessary for an OBU to access an application-service

available over IPv6 through the RSU as a router. This feature
removes the need for an IPv6 Router Advertisement message, which are
based on ICMPv6.

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

ETSI published a standard specifing the transmission of IPv6 packets
over the ETSI GeoNetworking (GN) protocol [ETSI-ITS-IPv6]. The IPv6
addressing and forwarding is defined in ETSI EN 302 636-4-1
[ETSI-ITS-Addressing] via a protocol adaptation sub-layer referred to
as the GN6ASL (GeoNetworking to IPv6 Adaptation Sub-Layer). It
enables an ITS station (ITS-S) running the GN protocol and an IPv6-
compliant protocol layer to: (i) exchange IPv6 packets with other
ITS-S; (ii) acquire globally routable IPv6 unicast addresses and
communicate with any IPv6 host located in the Internet, providing
IPv6 connectivity to the Internet is reachable directly or via other
relay ITS stations; (iii) perform the operations required by RFC 3963
[RFC3963] for a Mobile Router.

The document introduces three types of virtual link, the first one
providing symmetric reachability by means of stable geographically
scoped boundaries and two others that can be used when the dynamic
definition of the broadcast domain is required. The combination of
these three types of virtual link in the same station allows running
the Neighbour Discovery (ND) protocol including Stateless Address
Autoconfiguration (SLAAC) as specified in RFC 4862 [RFC4862] as well
as to distribute other IPv6 link-local multicast traffic and, at the
same time, to reach nodes that are outside specific geographic
boundaries. The IPv6 virtual link types are provided by the GN6ASL
to IPv6 in the form of virtual network interfaces.

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

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

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

ISO published a standard specifying the IPv6 network protocols and
services [ISO-ITS-IPv6]. These services are necessary to support the

global reachability of ITS stations (ITS-S), the continuous Internet connectivity for ITS-S, and the handover functionality required to maintain such connectivity. This functionality also allows legacy devices to effectively use an ITS-S as an access router to connect to the Internet. Essentially, this specification describes how IPv6 is configured to support ITS-S and provides the associated management functionality.

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

10. Summary and Analysis

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

Through this survey, it is learned that IPv6-based vehicular networking can be well-aligned with IEEE WAVE standards for various vehicular network applications, such as driving safety, efficient driving, and infotainment. However, since the IEEE WAVE standards do not recommend to use the IPv6 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.

11. Security Considerations

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

12. Acknowledgements

13. References

13.1. Normative References

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

[RFC5889]   Baccelli, E. and M. Townsley, "IP

                              Addressing Model in Ad Hoc Networks",
                              RFC 5889, September 2010.

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

13.2. Informative References

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

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

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

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

   [IPv6-WAVE]   Baccelli, E., Clausen, T., and R.
                              Wakikawa, "IPv6 Operation for WAVE -
                              Wireless Access in Vehicular
                              Environments", IEEE Vehicular
                              Networking Conference, December 2010.

   [Vehicular-Network-Framework] Jemaa, I., Shagdar, O., and T. Ernst,
                              "A Framework for IP and non-IP
                              Multicast Services for Vehicular

Networks", Third International
Conference on the Network of the
Future, November 2012.

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

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

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

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

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

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

[H-NEMO]   Nguyen, T. and C. Bonnet, "A Hybrid
Centralized-Distributed Mobility
Management Architecture for Network
Mobility", IEEE International
Symposium on a World of Wireless,
Mobile and Multimedia Networks,

                                 June 2015.

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

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

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

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

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

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

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

   [VNET-AAA]   Moustafa, H., Bourdon, G., and Y.

                          Gourhant, "Providing Authentication
                          and Access Control in Vehicular
                          Network Environment", IFIP TC-
                          11 International Information Security
                          Conference, May 2006.

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

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

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

   [ETSI-ITS-Addressing] ETSI Technical Committee Intelligent
                          Transport Systems, "Intelligent
                          Transport System (ITS); Vehicular
                          Communications; GeoNetworking; Part 4:
                          Geographical Addressing and Forwarding
                          for Point-to-Point and Point-to-
                          Multipoint Communications; Sub-part 1:
                          Media Independent Functionalities",
                          ETSI EN 302 636-1-1, October 2013.

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

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

   [ISO-ITS-IPv6]   ISO/TC 204, "Intelligent Transport
                          Systems - Communications Access for

                              Land Mobiles (CALM) - IPv6
                              Networking", ISO 21210:2012,
                              June 2012.

Appendix A. **Changes from**
              draft-jeong-ipwave-vehicular-networking-survey-00

   The following changes are made from
   draft-jeong-ipwave-vehicular-networking-survey-00:

   o Section 9, standard activities about vehicular networks are added
      in the standards developing organizations, such as IEEE, ETSI, and
      ISO.

Authors' Addresses

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

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

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

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

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

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

Jerome Haerri
Communication Systems Department
EURECOM
Sophia-Antipolis
France

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

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

EMail: Michelle.Wetterwald@gmail.com