Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 6, 2018

J. Jeong, Ed.
Sungkyunkwan University

March 5, 2018

IP-based Vehicular Networking: Use Cases, Survey and Problem Statement draft-ietf-ipwave-vehicular-networking-02

Abstract

This document discusses use cases, survey, and problem statement on IP-based vehicular networks, which are considered a key component of Intelligent Transportation Systems (ITS). The main topics of vehicular networking are vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) networking. First, this document surveys use cases using V2V and V2I networking. Second, this document deals with some critical aspects in vehicular networking, such as vehicular network architectures, standardization activities, IP address autoconfiguration, routing, mobility management, DNS naming service, service discovery, and security and privacy. For each aspect, this document discusses problem statement to analyze the gap between the state-of-the-art techniques and requirements in IP-based vehicular networking. Finally, this document articulates discussions including the summary and analysis of vehicular networking aspects and raises deployment issues.

Status of This Memo

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

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

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

This Internet-Draft will expire on September 6, 2018.

Table of Contents

1. Introduction

Vehicular networks have been focused on the driving safety, driving efficiency, and entertainment in road networks. The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC], service in

the Intelligent Transportation Systems (ITS) Radio Service in the 5.850 - 5.925 GHz band (5.9 GHz band). DSRC-based wireless communications can support vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle (I2V) networking.

For driving safety services based on the DSRC, IEEE has standardized Wireless Access in Vehicular Environments (WAVE) standards, such as IEEE 802.11p [IEEE-802.11p], IEEE 1609.2 [WAVE-1609.2], IEEE 1609.3 [WAVE-1609.3], and IEEE 1609.4 [WAVE-1609.4]. Note that IEEE 802.11p has been published as IEEE 802.11 Outside the Context of a Basic Service Set (OCB) [IEEE-802.11-OCB] in 2012. Along with these WAVE standards, IPv6 and Mobile IP protocols (e.g., MIPv4 and MIPv6) can be extended to vehicular networks [RFC2460][RFC6275].

This document discusses use cases, survey, and problem statements related to IP-based vehicular networking for Intelligent Transportation Systems (ITS). This document first surveys the use cases for using V2V and V2I networking in the ITS. Second, this document deals with some critical aspects in vehicular networking, such as vehicular network architectures, standardization activities, IP address autoconfiguration, routing, mobility management, DNS naming service, service discovery, and security and privacy. For each aspect, this document shows problem statement to analyze the gap between the state-of-the-art techniques and requirements in IP-based vehicular networking. Finally, this document addresses discussions including the summary and analysis of vehicular networking aspects, raising deployment issues in road environments.

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

2. Terminology

This document uses the following definitions:

- Road-Side Unit (RSU): A node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, etc.) for wireless communication with vehicles and is also connected to the Internet as a router or switch for packet forwarding. An RSU is deployed either at an intersection or in a road segment.

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

Global Positioning System (GPS)) is included in a vehicle with an OBU for efficient navigation.

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

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

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

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

3. Use Cases

This section provides use cases of V2V and V2I networking.

3.1. V2I Use Cases

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

A navigation service, such as the Self-Adaptive Interactive Navigation Tool (called SAINT) [SAINT], using V2I networking interacts with TCC for the global road traffic optimization and can guide individual vehicles for appropriate navigation paths in real

time. The enhanced SAINT (called SAINT+) [SAINTplus] can give the fast moving paths for emergency vehicles (e.g., ambulance and fire engine) toward accident spots while providing other vehicles with efficient detour paths.

The emergency communication between accident vehicles (or emergency vehicles) and TCC can be performed via either RSU or 4G-LTE networks. The First Responder Network Authority (FirstNet) [FirstNet] is provided by the US government to establish, operate, and maintain an interoperable public safety broadband network for safety and security network services, such as emergency calls. The construction of the nationwide FirstNet network requires each state in the US to have a Radio Access Network (RAN) that will connect to FirstNet's network core. The current RAN is mainly constructed by 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Annual-Report-2017], but DSRC-based vehicular networks can be used for V2I in near future [DSRC].

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

3.2. V2V Use Cases

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

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

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

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

4. Vehicular Network Architectures

This section surveys vehicular network architectures based on IP along with various radio technologies, and then discusses problem statement for a vehicular network architecture for IP-based vehicular networking.

4.1. Existing Architectures

4.1.1. VIP-WAVE: IP in 802.11p Vehicular Networks

Cespedes et al. proposed a vehicular IP in WAVE called VIP-WAVE for I2V and V2I networking [VIP-WAVE]. IEEE 1609.3 specified a WAVE stack of protocols and includes IPv6 as a network layer protocol in data plane [WAVE-1609.3]. The standard WAVE [WAVE-1609.0] [WAVE-1609.3] does not support Duplicate Address Detection (DAD) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862] by having its own efficient IP address configuration mechanism based on a WAVE Service Advertisement (WSA) management frame [WAVE-1609.3]. It does not support both seamless communications for Internet services and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU), either. To overcome these limitations of the standard WAVE 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.

4.1.2. IPv6 Operation for WAVE

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

In the analysis provided in [IPv6-WAVE], it is identified that the IEEE 1609.3 standard’s recommendations for IPv6 operation over WAVE are rather minimal. Protocols on which the operation of IPv6 relies for IP address configuration and IP-to-link-layer address translation (e.g., IPv6 ND protocol) are not recommended in the standard. Additionally, IPv6 implementations work under certain assumptions for the link model that do not necessarily hold in WAVE. For instance, some IPv6 implementations assume 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.

Baccelli 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 those challenges require the design of appropriate solutions.

4.1.3. Multicast Framework for Vehicular Networks

Jemaa et al. presented a framework that enables deploying multicast services for vehicular networks in Infrastructure-based scenarios [VNET-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, the 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 on 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, the GMAA study lacks simulations related to performance assessment.

4.1.4. Joint IP Networking and Radio Architecture

Petrescu et al. defined the joint 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.

Consider a simplified 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 their paper is to join the IP-layer relaying with radio-link channels. Their paper proposes separating 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 approach is similar to multi-channel topology management proposals in multi-hop sensor networks, yet adapted to an IP topology.

Their paper concludes 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.

4.1.5. Mobile Internet Access in FleetNet

Bechler et al. described the FleetNet project approach to integrate Internet Access in future vehicular networks [FleetNet]. The FleetNet paper is probably one of the first papers 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 IPv4/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 hybrid 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).

4.1.6. A Layered Architecture for Vehicular DTNs

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

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

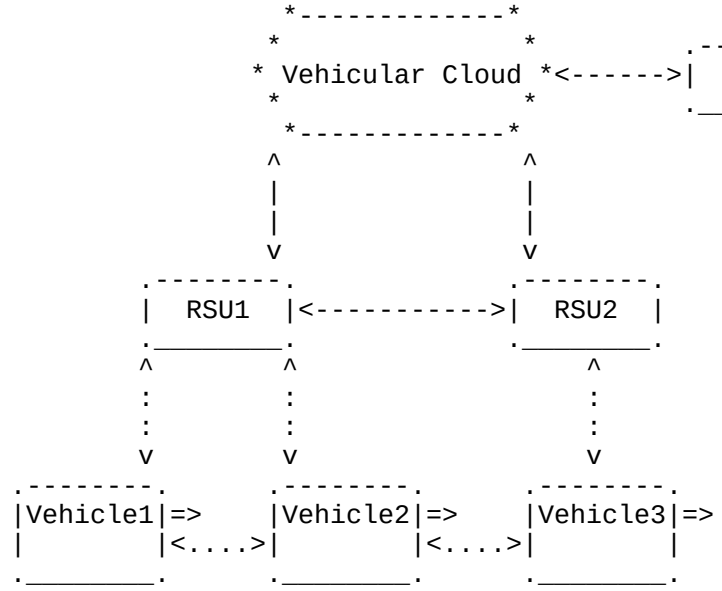
Although DTN architectures have evolved since the paper was written, the Vehicular-DTN paper takes a different approach to IP mobility management. An important aspect is to separate the Control plane from the Data plane to allow a large flexibility in a Control plane to coordinate a heterogeneous radio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

4.2. V2I and V2V Internetworking Problem Statement

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

Figure 1 shows an architecture for V2I and V2V networking in a road network. The two RSUs (RSU1 and RSU2) are deployed in the road network and are connected to a Vehicular Cloud through the Internet.

TCC is connected to the Vehicular Cloud and the two vehicles (Vehicle1 and Vehicle2) are wirelessly connected to RSU1, and the last vehicle (Vehicle3) is wirelessly connected to RSU2. Vehicle1 can communicate with Vehicle2 via V2V communication, and Vehicle2 can communicate with Vehicle3 via V2V communication. Vehicle1 can communicate with Vehicle3 via RSU1 and RSU2 via V2I communication.



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

Figure 1: A Vehicular Network Architecture for V2I and V2V Networking

In vehicular networks, unidirectional links exist and must be considered. The control plane must be separated from data plane. ID/Pseudonym change requires a lightweight DAD. IP tunneling should be avoided. The mobility information of a mobile device (e.g., vehicle), such as trajectory, position, speed, and direction, can be used by the mobile device and infrastructure nodes (e.g., TCC and RSU) for the accommodation of proactive protocols because it is usually equipped with a GPS receiver. Vehicles can use the TCC as its Home Network, so the TCC maintains the mobility information of vehicles for location management. A vehicular network architecture may be composed of three types of vehicles in Figure 1: Leaf Vehicle, Range Extending Vehicle, and Internet Vehicle[Joint-IP-Networking].

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

4.2.1. V2I-based Internetworking

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

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

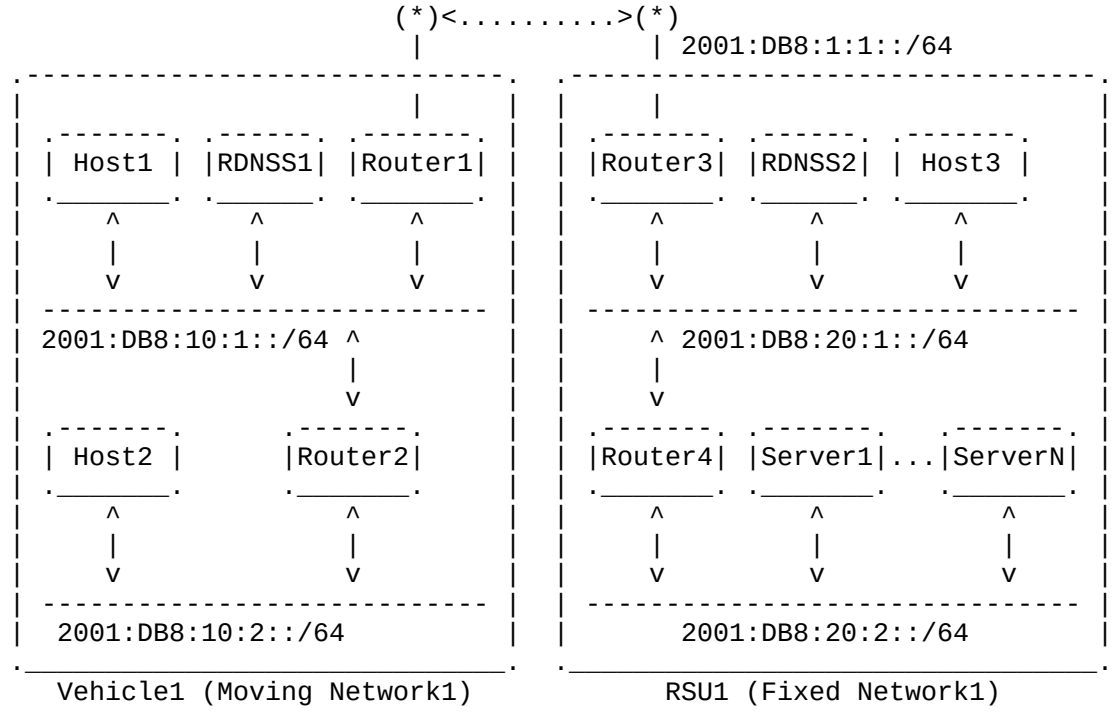


Figure 2: Internetworking between Vehicle Network and RSU Network

Once the network parameter discovery and prefix exchange operations have been performed, packets can be transmitted between the vehicle's moving network and the RSU's fixed network. DNS should be supported to enable name resolution for hosts or servers residing either in the vehicle's moving network or the RSU's fixed network.

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

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.

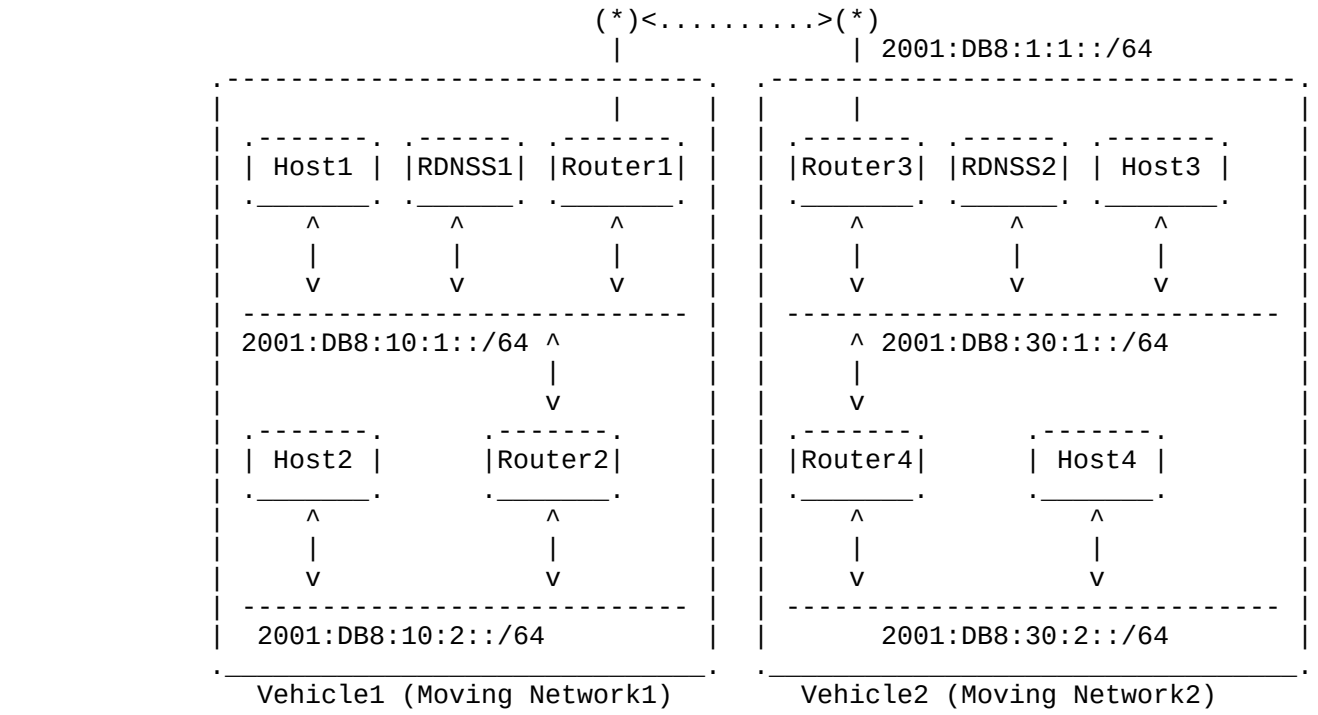


Figure 3: Internetworking between Two Vehicle Networks

4.2.2. V2V-based Internetworking

In Figure 3, the prefix assignment for each subnet inside each vehicle's mobile network is done through a prefix delegation protocol.

Figure 3 shows internetworking between the moving networks of two neighboring vehicles. There exists an internal network (Moving Network1) inside Vehicle1. Vehicle1 has the DNS Server (RDNSS1), the two hosts (Host1 and Host2), and the two routers (Router1 and Router2). There exists another internal network (Moving Network2) inside Vehicle2. Vehicle2 has the DNS Server (RDNSS2), the two hosts (Host3 and Host4), and the two routers (Router3 and Router4). Vehicle1's Router1 (called mobile router) and Vehicle2's Router3

(called mobile router) use 2001:DB8:1:1::/64 for an external link (e.g., DSRC) for V2V networking.

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

5. Standardization Activities

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

5.1. IEEE Guide for 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.

5.2. IEEE Standard for WAVE - Networking Services

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

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

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

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

5.3. ETSI Intelligent Transport Systems: GeoNetwork-IPv6

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

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

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

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

5.4. ISO Intelligent Transport Systems: IPv6 over CALM

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

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

6. IP Address Autoconfiguration

This section surveys IP address autoconfiguration schemes for vehicular networks, and then discusses problem statement for IP addressing and address autoconfiguration for vehicular networking.

6.1. Existing Protocols for Address Autoconfiguration

6.1.1. 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 within communication range. In this VANET, VAC dynamically elects a leader-vehicle to quickly provide vehicles with unique IP addresses. The leader-vehicle maintains updated information on configured addresses in its connected VANET. It aims at the reduction of the frequency of IP address reconfiguration due to mobility.

VAC defines "SCOPE" to be a delimited geographic area within which IP addresses are guaranteed to be unique. When a vehicle is allocated an IP address from a leader-vehicle with a scope, it 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.

6.1.2. Using Lane/Position Information

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 too much overhead when vehicles change their lanes frequently on the highway.

6.1.3. GeoSAC: Scalable Address Autoconfiguration

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

The GeoSAC paper identifies eight 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.

6.1.4. Cross-layer Identities Management in ITS Stations

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

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

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

6.2. Problem Statement for IP Address Autoconfiguration

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

access, web surfing and entertainment services), the latter approach is required.

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

6.2.1. Neighbor Discovery

Neighbor Discovery (ND) [RFC4861] is a core part of the IPv6 protocol suite. This section discusses the need for modifying ND for use with 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.

6.2.2. IP Address Autoconfiguration

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

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

Stateless DHCPv6) can be used for the IP address autoconfiguration [RFC3315][RFC3736].

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

For IP address autoconfiguration in V2V, vehicles can autoconfigure their address using prefixes for ULAs for vehicular networks [RFC4193].

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

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

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

7. Routing

This section surveys routing in vehicular networks, and then discusses problem statement for routing in vehicular networks.

7.1. Existing Routing Protocols

7.1.1. Experimental Evaluation for IPv6 over GeoNet

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 the C2C-CC architecture, the C2CNet layer is located between IPv6 and link layers. Thus, an IPv6 packet is delivered with an 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 the C2C 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 C2CNet, 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).

7.1.2. Location-Aided Gateway Advertisement and Discovery

Abrougui et al. presented a gateway discovery scheme for VANET, called Location-Aided Gateway Advertisement and Discovery (LAGAD) mechanism[LAGAD]. LAGAD enables vehicles to route packets toward the closest gateway quickly by discovering nearby gateways. The major problem that LAGAD tackles is to determine the radius of advertisement zone of a gateway, which depends on the location and velocity of a vehicle.

A gateway sends advertisement (GAdv) messages perodically to neighboring vehicles. When receiving a request message from a vehicle, the gateway replies to the source vehicle by a gateway reply (GRep) message. The GRep message contains the location information of the gateway and the subnet prefix of the gateway by which the source vehicle can send data packet via the gateway. The gateway sends GAdv messages through all vehicles within an advertisement zone built based on the velocity of the source vehicle.

The source vehicle starts gateway discovery process by sending routing request packets. The routing request packet is encapsulated into a Gateway Reactive Discovery (GRD) packet or a GReq message to send to the surrounding vehicles. The GRD contains both discovery

and routing information as well as the location and the velocity of the source vehicle. Meanwhile, the intermediate vehicles in an advertisement zone of the gateway forward packets sent from the source vehicle. The gateway continuously updates the advertisement zone whenever receiving a new data packet from the source vehicle.

7.2. Routing Problem Statement

IP address autoconfiguration should be modified to support the efficient networking. Due to network fragmentation, vehicles sometimes 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.

The gateway advertisement and discovery process for routing in VANET can probably work when the density of vehicle in a road network is not sparse. A sparse vehicular network challenges the gateway discovery since network fragmentation interrupts the discovery process.

8. Mobility Management

This section surveys mobility management schemes in vehicular networks to support handover, and then discusses problem statement for mobility management in vehicular networks.

8.1. Existing Protocols

8.1.1. 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.

8.1.2. Hybrid Centralized-Distributed Mobility Management

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

H-DMM proposes 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 be delayed. 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.

8.1.3. Hybrid Architecture for Network Mobility Management

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. For some measures, such as the signaling cost, H-NEMO may be 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.

8.1.4. NEMO-Enabled Localized Mobility Support

In [NEMO-LMS], the authors proposed an architecture to enable IP mobility for moving networks using a network-based mobility scheme based on PMIPv6. In PMIPv6, only mobile terminals are provided with IP mobility. In contrast to 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 using PMIPv6 signaling. 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 mMAG. 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].

8.1.5. Network Mobility 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 authorized to assist the vehicle to perform a pre-handoff.

The 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.

8.1.6. Performance Analysis of P-NEMO for ITS

Lee et al. proposed P-NEMO, which is a PMIPv6-based IP mobility management scheme to maintain the Internet connectivity at the vehicle as a mobile network, and provides a make-before-break mechanism when vehicles switch to a new access network [PMIP-NEMO-Analysis]. Since the standard PMIPv6 only supports mobility for a single node, the solution in [PMIP-NEMO-Analysis] adapts the protocol to reduce the signaling when a local network is to be served by an 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. In that way, 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 evaluated through an analytical model that is compared only 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].

8.1.7. Integration of VANets and Fixed IP Networks

Peng et al. proposed a novel mobility management scheme for integration of VANET and fixed IP networks [VNET-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).

8.1.8. SDN-based 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 (MFs) through the network instead of concentrating them in one bottleneck MF, or in a hierarchically organized backbone of MFs. Highly mobile vehicular networks impose frequent IP route optimizations that lead to suboptimal routes (detours) between CN and vehicles. The suboptimality critically increases when there are 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 has recently gained 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.

The SDN-DMM paper makes several observations leading to a strong suggestion that IP mobility management should be based on an SDN architecture. First, SDN will be integrated into future Internet and 5G in the 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.

8.1.9. IP Mobility for VANETs: 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. Also, a detour may be taken by the MR’s HA, even if the CN is nearby. Furthermore, route optimization is needed 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 requiring 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).

8.2. Problem Statement for Mobility-Management

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

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.

9. DNS Naming Service

This section surveys and analyzes DNS naming service to translate a device's DNS name into the corresponding IP address, and then discusses problem statement for DNS naming service in vehicular networks.

9.1. Existing Protocols

9.1.1. Multicast DNS

Multicast DNS (mDNS)[RFC6762] allows devices in one-hop communication range to resolve each other's DNS name into the corresponding IP address in multicast. Each device has a DNS resolver and a DNS server. The DNS resolver generates a DNS query for the device's application and the DNS server responds to a DNS query corresponding to its device's DNS name.

9.1.2. DNS Name Autoconfiguration for IoT Devices

DNS Name Autoconfiguration (DNSNA) [ID-DNSNA] proposes a DNS naming service for Internet-of-Things (IoT) devices in a large-scale network.

The DNS naming service of DNSNA consists of four steps, such as DNS name generation, DNS name duplication detection, DNS name registration, and DNS name list retrieval.

First, in DNS name generation, DNSNA allows each IoT device to generate its own DNS name with a DNS suffix (acquired from ND or DHCP) and its device information (e.g., vendor, model, and serial number).

Second, in DNS name duplication detection, each device checks whether its generated DNS name is used by another IoT device in the same subnet.

Third, in DNS name registration, each device registers its DNS name and the corresponding IPv6 address into a designated DNS server via a router. The router periodically collects DNS information of IoT devices in its the subnets corresponding ot its network interfaces.

Last, in DNS name list retrieval, a user can retrieve the DNS name list of IoT devices available to the user through the designated DNS server. Once the user retrieves the list having a DNS name and the corresponding IP address(es), it can monitor and remote-control an IoT device.

9.2. Problem Statement

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

mDNS is designed for a small ad hoc network with wireless/wired one-hop communication range. If it is used in a vehicle's mobile network having multiple subnets, mDNS cannot effectively work in such a multi-hop network. This is because the DNS query message of each DNS resolver should be multicasted into the whole mobile network, leading to a large volume of DNS traffic.

DNSNA is designed for a large-scale network with multiple subnets. If it is used in a vehicle's mobile network having multiple subnets, DNSNA can effectively work in such a multi-hop network. This is because the DNS query message of each DNS resolver should be unicasted to the designated DNS server.

DNSNA allows each host (e.g., in-vehicle device and a user's mobile device) within a vehicle's moving network to generate its unique DNS name 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. Service Discovery

This section surveys and analyzes service discovery to translate a required service into an IP address of a device to provide such a service, and then discusses problem statement for service discovery in vehicular networks.

10.1. Existing Protocols

10.1.1. mDNS-based Service Discovery

As a popular existing service discovery protocol, DNS-based Service Discovery (DNS-SD) [RFC6763] with mDNS [RFC6762] provides service discovery.

DNS-SD uses a DNS service (SRV) resource record (RR) [RFC2782] to support the service discovery of services provided by a device or server. An SRV RR contains a service instance name, consisting of an instance name (i.e., device), a service name, a transport layer protocol, a domain name, the corresponding port number, and the DNS name of the device eligible for the requested service. With this DNS-SD, a host can search for a service instance with the SRV RR to discover a list of devices corresponding to the searched service type.

10.1.2. ND-based Service Discovery

Vehicular ND [ID-Vehicular-ND] proposes an extension of IPv6 ND for the prefix and service discovery. 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.

10.2. Problem Statement

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

mDNS-based DNS-SD [RFC6762][RFC6763] can be used for service discovery between vehicles or between a vehicle and an RSU by using a multicast protocol, the service discovery requires a nonnegligible service delay due to service discovery. This is because the service discovery message should traverse the mobile network or fixed network through multicasting. This 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. The Vehicular ND [ID-Vehicular-ND] can support this approach efficiently.

11. Security and Privacy

This section surveys security and privacy in vehicular networks, and then discusses problem statement for security and privacy in vehicular networks.

11.1. Existing Protocols

11.1.1. 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.

11.1.2. Authentication and Access Control

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.

11.2. Problem Statement

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

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

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

communication, the secure channel between a mobile router in a vehicle and a mobile router in another vehicle should be established, as shown in Figure 3.

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.

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

12. Discussions

12.1. Summary and Analysis

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

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

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

For IP-based networking, IP address autoconfiguration is a prerequisite function. Since vehicles can communicate intermittently

with TCC via RSUs through V2I communications, TCC can play a role of a DHCP server to allocate unique IPv6 addresses to the vehicles. This centralized address allocation can remove the delay of the DAD procedure for testing the uniqueness of IPv6 addresses.

For routing and mobility management, most of vehicles are equipped with a GPS navigator as a dedicated navigation system or a smartphone App. With this GPS navigator, vehicles can share their current position and trajectory (i.e., navigation path) with TCC. TCC can predict the future positions of the vehicles with their mobility information (i.e., the current position, speed, direction, and trajectory). With the prediction of the vehicle mobility, TCC supports RSUs to perform data packet routing and handover proactively.

12.2. Deployment Issues

Some automobile companies (e.g., BMW and Hyundai) started to use Ethernet for a vehicle’s internal network instead of the traditional Contoller Area Network (CAN) for high-speed interconnectivity among electronic control units. With this trend, the IP-based vehicular networking in this document will be popular in near future.

Self-driving technologies are being developed by many automobile companies (e.g., Tesla, BMW, GM, Honda, Toyota, and Hyundai) and IT companies (e.g., Google and Apple). Since they require high-speed interaction among vehicles, infrastructure nodes (e.g., RSU), and cloud, IP-based networking will be mandatory.

Therefore, key component technologies for the IP-based vehicular networking need to be developed for future demands along with an efficient vehicular network architecture.

13. Security Considerations

Section 11 discusses security and privacy for IP-based vehicular networking.

The security for key components in vehicular networking, such as IP address autoconfiguration, routing, mobility management, DNS naming service, and service discovery, needs to be analyzed in depth.

14. Informative References

[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.

[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.

[CA-Cuise-Control]
California Partners for Advanced Transportation Technology (PATH), "Cooperative Adaptive Cruise Control", [Online] Available: http://www.path.berkeley.edu/research/automated-and-connected-vehicles/cooperative-adaptive-cruise-control, 2017.

[CASD] Shen, Y., Jeong, J., Oh, T., and S. Son, "CASD: A Framework of Context-Awareness Safety Driving in Vehicular Networks", International Workshop on Device Centric Cloud (DC2), March 2016.

[DMM] Chan, H., "Requirements for Distributed Mobility Management", RFC 7333, August 2014.

[DSRC] ASTM International, "Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ASTM E2213-03(2010), October 2010.

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

[FirstNet]
U.S. National Telecommunications and Information Administration (NTIA), "First Responder Network Authority (FirstNet)", [Online]
Available: https://www.firstnet.gov/, 2012.

[FirstNet-Annual-Report-2017]
First Responder Network Authority, "FY 2017: ANNUAL REPORT TO CONGRESS, Advancing Public Safety Broadband Communications", FirstNet FY 2017, December 2017.

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

[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.

[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.

[ID-DNSNA]
Jeong, J., Ed., Lee, S., and J. Park, "DNS Name Autoconfiguration for Internet of Things Devices", draft-jeong-ipwave-iot-dns-autoconf-02 (work in progress), March 2018.

[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-ipwave-vehicular-neighbor-discovery-02 (work in progress), March 2018.

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

[IEEE-802.11-OCB]
IEEE 802.11 Working Group, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11-2012, February 2012.

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

[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.

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

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

[LAGAD] Abrougui, K., Boukerche, A., and R. Pazzi, "Location-Aided Gateway Advertisement and Discovery Protocol for VANets", IEEE Transactions on Vehicular Technology, Vol. 59, No. 8, October 2010.

[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.

[PMIP-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.

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

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

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

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for Specifying the Location of Services (DNS SRV)", RFC 2782, February 2000.

[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.

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

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

[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.

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

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

[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.

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

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

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

[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.

[SAINT] Jeong, J., Jeong, H., Lee, E., Oh, T., and D. Du, "SAINT: Self-Adaptive Interactive Navigation Tool for Cloud-Based Vehicular Traffic Optimization", IEEE Transactions on Vehicular Technology, Vol. 65, No. 6, June 2016.

[SAINTplus] Shen, Y., Lee, J., Jeong, H., Jeong, J., Lee, E., and D. Du, "SAINT+: Self-Adaptive Interactive Navigation Tool+ for Emergency Service Delivery Optimization", IEEE Transactions on Intelligent Transportation Systems, June 2017.

[SANA] Hwang, T. and J. Jeong, "SANA: Safety-Aware Navigation Application for Pedestrian Protection in Vehicular Networks", Springer Lecture Notes in Computer Science (LNCS), Vol. 9502, December 2015.

[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.

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

[Truck-Platooning] California Partners for Advanced Transportation Technology (PATH), "Automated Truck Platooning", [Online] Available: http://www.path.berkeley.edu/research/automated-and-connected-vehicles/truck-platooning, 2017.

[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.

[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.

[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.

[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.

[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.

[VNET-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.

[VNET-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.

[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-1609.2]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", IEEE Std 1609.2-2016, March 2016.

[WAVE-1609.3]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services", IEEE Std 1609.3-2016, April 2016.

[WAVE-1609.4]
IEEE 1609 Working Group, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation", IEEE Std 1609.4-2016, March 2016.

Appendix A. Acknowledgments

This work was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2017M3C4A7065980). This work was supported in part by the Global Research Laboratory Program (2013K1A1A2A02078326) through NRF and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science and ICT. This work was supported in part by the French research project DataTweet (ANR-13-INFR-0008) and in part by the HIGHTS project funded by the European Commission I (636537-H2020).

Appendix B. Contributors

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

The following are co-authors of this document:

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

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

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

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

Jerome Haerri
Communication Systems Department
EURECOM

Sophia-Antipolis
France

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

Dapeng Liu
Alibaba
Beijing, Beijing 100022
China

Phone: +86 13911788933
EMail: max.ldp@alibaba-inc.com

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

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1 408 330 4586
EMail: charliep@computer.org

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

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

Yiwen Chris Shen

Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

Phone: +82 31 299 4106
Fax: +82 31 290 7996
EMail: chrisshen@skku.edu
URI: http://iotlab.skku.edu/people-chris-shen.php

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

EMail: Michelle.Wetterwald@gmail.com

Appendix C. Changes from draft-ietf-ipwave-vehicular-networking-01

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

- In Section 1, the following sentence is added: The Federal Communications Commission (FCC) in the US allocated wireless channels for Dedicated Short-Range Communications (DSRC) [DSRC], service in the Intelligent Transportation Systems (ITS Radio Service in the 5.850 - 5.925 GHz band (5.9 GHz band).

- In Section 2, the definition of Road-Side Unit (RSU) is modified as a node that has physical communication devices (e.g., DSRC, Visible Light Communication, 802.15.4, etc.) for wireless communication with vehicles and is also connected to the Internet as a router or switch for packet forwarding.

- In Section 2, DMM is defined as the acronym for "Distributed Mobility Management" [DMM].

- In Section 3.1, the following sentence is clarified along with relevant references: The current RAN is mainly constructed by 4G-LTE for the communication between a vehicle and an infrastructure node (i.e., V2I) [FirstNet-Annual-Report-2017], but DSRC-based vehicular networks can be used for V2I in near future [DSRC].

- In Section 4.1.1, the following sentences are clarified along with relevant references: The standard WAVE [WAVE-1609.0][WAVE-1609.3] does not support Duplicate Address Detection (DAD) of IPv6 Stateless Address Autoconfiguration (SLAAC) [RFC4862] by having its own efficient IP address configuration mechanism based on a WAVE Service Advertisement (WSA) management frame [WAVE-1609.3]. It does not support both seamless communications for Internet services and multi-hop communications between a vehicle and an infrastructure node (e.g., RSU), either.

- The contents are clarified with typo corrections and rephrasing.

Author's Address

Jaehoon Paul Jeong (editor)
Department of Software
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon, Gyeonggi-Do 16419
Republic of Korea

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