Large scale addressing and routing mechanisms for highly mobile networks of networks

Sofiane Imadali

▶ **To cite this version:**

Sofiane Imadali. Large scale addressing and routing mechanisms for highly mobile networks of networks. Other. Université Paris Sud - Paris XI, 2015. English. NNT : 2015PA112049 . tel-01180150

HAL Id: tel-01180150
https://theses.hal.science/tel-01180150

Submitted on 24 Jul 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

UNIVERSITE PARIS-SUD

ÉCOLE DOCTORALE : STITS
DIASI, LIST, Laboratoire des Système Communicants (LSC)

THÈSE DE DOCTORAT
Discipline: *Sciences de l'information et de la communication*

soutenue le 02/04/2015

par

Sofiane IMADALI

ALGORITHMES D'ADRESSAGE ET ROUTAGE POUR DES RÉSEAUX FORTEMENT MOBILES À GRANDE ÉCHELLE

Directeur de thèse :	Véronique Vèque	Professeur à l'université de Paris-Sud
Encadrant CEA :	Alexandre Petrescu	Ingénieur-chercheur au CEA-Saclay

Composition du jury :

Rapporteurs :	Yacine Ghamri-Doudane	Professeur à l'université de La Rochelle
	Jérome Haerri	Maitre de conférences, HDR à Eurecom
Président du jury :	Samir Tohme	Professeur à l'université de Versailles (UVSQ)
Examinateurs :	Anthony Busson	Professeur à l'université de Lyon 1
	Anne Fladenmuller	Maitre de conférences, HDR Université Paris 6 (UPMC)

Abstract

After successfully connecting machines and people later (world wide web), the new era of Internet is about connecting things. Due to increasing demands in terms of addresses, mobility, scalability, security and other new unattended challenges, the evolution of current Internet architecture is subject to major debate worldwide. The Internet Architecture Board (IAB) workshop on Routing and Addressing report described the serious scalability problems faced by large backbone operators in terms of routing and addressing, illustrated by the unsustainable growth of the Default Free Zone (DFZ) routing tables. Some proposals tackled the scalability and IP semantics overload issues with two different approaches: *evolutionary* approach (backward compatibility) or a *revolutionary* approach. Several design objectives (technical or high-level) guided researchers in their proposals. Mobility is definitely one of the main challenges.

Inter-Vehicle Communication (IVC) attracts considerable attention from the research community and the industry for its potential in providing Intelligent Transportation Systems (ITS) and passengers services. Vehicular Ad-Hoc Networks (VANETs) are emerging as a class of wireless network, formed between moving vehicles equipped with wireless interfaces (cellular and WiFi) employing heterogeneous communication systems. A VANET is a form of mobile ad-hoc network that provides IVC among nearby vehicles and may involve the use of a nearby fixed equipment on the roadside. The impact of Internet-based vehicular services (infotainment) are quickly developing. Some of these applications, driver assistance services or traffic reports, have been there for a while. But market-enabling applications may also be an argument in favor of a more convenient journey. Such use cases are viewed as a motivation to further adoption of the ITS standards developed within IEEE, ETSI, and ISO.

This thesis focuses on applying Future Internet paradigm to vehicle-to-Internet communications in an attempt to define the solution space of Future Vehicular Internet. We first introduce two possible vehicle-to-Internet use cases and great enablers for IP based services : eHealth and Fully-electric Vehicles. We show how to integrate those use cases into IPv6 enabled networks. We further focus on the mobility architectures and determine the fundamental components of a mobility architecture. We then classify those approaches into centralized and distributed to show the current trends in terms of network mobility extension, an essential component to vehicular networking. We eventually analyze the performance of these proposals.

In order to define an identifier namespace for vehicular communications, we introduce the Vehicle Identification Numbers are possible candidates. We then propose a conversion algorithm that preserves the VIN characteristics while mapping it onto usable IPv6 networking objects (addresses, prefixes, and Mobile Node Identifiers). We make use of this result to extend LISP-MN protocol with the support of our VIN6 addressing architecture. We also apply those results to group IP-based communications, when the cluster head is in charge of a group of followers.

Keywords: Future Internet, Future Vehicular Internet, Addressing architecture, Mobility management protocols, Vehicle Identification Number, Vehicle-to-Internet communications, Analytical Model, Performance evaluation.

Acknowledgments

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 General context

After successfully connecting machines and people later (world wide web), the new era of Internet is about connecting things. Due to increasing demands in terms of addresses, mobility, scalability, security and other new unattended challenges, the evolution of current Internet architecture is subject to major debate worldwide [75].

The evolution of such a large system as Internet implies addressing unforeseen applications at the time the system was originally designed. Non-related technical and non-technical factors influence the growth of the architecture and obscure the overall vision of the system [160]. In terms of implementation, additional requirements are often added to the system as immediate patches, or protocol extensions, to fix a known issue rather than a full redesign implying a global and coordinated vision among several actors with sometimes contradictory interests [48].

The Internet Architecture Board (IAB) workshop on Routing and Addressing report [146] described the serious scalability problems faced by large backbone operators in terms of routing and addressing, illustrated by the unsustainable growth of the DFZ routing tables. These concerns originated mainly from the success of the Internet Protocol (universality) leading to addressing pool exhaustion and the flexibility of system design which engineers used to extend existing protocols to different ends (traffic engineering, policy routing). Among the results reported in this workshop, overloaded IP semantics (a.k.a. location/identifier split) problem has been pointed out as being one fundamental reason for the scalability issues mentioned above: the same object (IP address) is used as label for the Internet graph vertices and addresses guiding the global routing operations [187] [160].

Following the IAB workshop, some proposals tackled the scalability and IP semantics overload issues with two different approaches putting the future Internet design as innovation vector [183]. This area of networking research stresses that changing a complex system should follow an *evolutionary* approach (backward compatibility) or a *revolutionary* approach, designing an extended Internet with the first method, or *clean slate* architectures with the second [75]. Several design objectives (technical or high-level) guided researchers in their proposals. Mobility is definitely one of the main challenges.

In the last two decades, IVC has attracted considerable attention from the research community and the automotive industry, for its potential in providing ITS as well as drivers and passengers services. In this context, VANETs are emerging as a class of wireless network, formed between moving vehicles equipped with wireless interfaces (cellular and WiFi) employing short-range to medium-range communication systems. A VANET is a form of mobile ad-hoc network that provides IVC among nearby vehicles and may involve the use of a nearby fixed equipment

on the roadside. IVC among VANETs has a significant potential to enable diverse applications associated with traffic safety and efficiency. Radio access networks (cellular and WiFi) may be employed to enable vehicular communications with strict latency requirements for safety-oriented and emergency communications. These activities have resulted in a standardization effort among IEEE, ISO and ETSI for a new 802.11p WLAN extension specifically designed for such activities. This new WLAN standard defines a low-latency alternative network for vehicular communications, and their main focus has been the effective, secure, and timely delivery of safety-related information.

Nonetheless, the deployment of IP-based services including infotainment and commercial applications is believed to accelerate the market penetration of those deployments and leverage the costs of the infrastructure required by IVC.The support of IP-based traffic comes through the integration of IPv6 as well as transport protocols such as TCP and UDP in the above mentioned standards. With regards to these technology enablers, new business opportunities are offered by vehicular networks for car manufacturers, automotive OEMs, network operators and service providers. The use of IP in a heterogeneous context (very common to IVC) has the ability to make the design of end-to-end (E2E) protocols easier.

The impact of Internet-based vehicular services (infotainment) are quickly spreading and developing. Some of these application, such as driver assistance services or traffic reports have been there for a while. But market-enabling and innovative applications may also be an argument in favor of a more convenient and pleasant traveling experience. Such use cases are viewed as a motivation to further adoption of the ITS standards developed within IEEE, ETSI, and ISO.

The potential of vehicle-to-Internet architecture as defined by SDOs is promising. Vehicular to Internet access and communications will allow for IP-based services to drivers and passengers. However, some technical challenges are of paramount importance in this matter: Managing the scalability of IP-services, IPv6 address (auto)configuration and mobility management of addresses and embedded networks. These challenges affect the service quality and continuity which are part of the IP-based applications quality-of-experience. This implies, with regards to the vehicular networks specific characteristics, a carriage of a stable IP addressing which is configured automatically and in a distributed manner. From a standardization point of view, there is no main and definitive standard IP auto-configuration method specific to ad hoc networks, and hence the problem is still posed in terms of vehicular networking [84].

In the Future Internet context described above, IPv6 still needs to undergo some upgrades to better vehicular IP-based services and follow the current Future Internet approaches [168]. Indeed, the recommendations for Identifier/Locator split must be included in Future Vehicular Internet architecture design. The objective is the support of mobile vehicle-to-Internet communications in a scalable manner.

1.2 Research challenges

The special characteristics of Future Vehicular Internet communication networks create unique requirements for IP-based services deployment. Some challenges come from the vehicular system itself, such as the high speeds, the dynamic topology, and the spatial-temporal traffic variability. Additional research challenges inherent to the locator/identifier split paradigm proper to Future Internet research.

1.2.1 Future Vehicular Internet architecture design

Vehicle-to-Internet communications are integrated into all SDOs' protocol stacks and IPv6 as the default protocol. However, the Future Internet movement through the IAB impulse [146]

considers the Locator/Identifier split issue as a priority, which is not taken into consideration in prior definitions of vehicle-to-Internet architectures. Recently, different approaches tackled the issue of scalability in the core network and defined new Future Internet architectures. As for the case of vehicle-to-Internet communications, it is usually regarded as a use case among others.

1.2.2 Efficient group mobility support

Mobility management in IP-based infrastructures for the vehicle-to-Internet communications can be classified into *network-based* or *host-based* approaches. Due to the inherent dynamics of the vehicular network, and the heterogeneity of the supporting infrastructure, it is reasonable to assume that vehicles may transfer their active connections through different IPv6 access networks. Thus, the on-going IPv6 sessions may be affected by the change of IPv6 addresses (in particular, the announced prefix), and consequently become broken connections. Previously, the research on IP mobility support has focused on vehicles using one-hop connections to the infrastructure. The objective is to enhance the performance of existing IPv6 mobility protocols, or to extend the support for the in-vehicle network nodes.

1.2.3 IVC fast IP configuration mechanisms

Dynamic IPv6 addressing and routing configuration in vehicular networks is an important challenge that has attracted a fair amount of attention recently. Early proposals adapted fixed-infrastructure and MANET models and thus inherited their latency and overhead. Later, researchers relaxed some of the often restrictive assumptions (e.g., Router Advertisement TTL extension) but still focused on certain limited scenarios. Beyond usual V2I and V2V architectures, recent proposals argue for an extended IP-based group (cluster) vehicle to infrastructure communications paradigm. In a cluster, vehicles can have a role of a leader or a follower. The leader providing the IP-based configuration for its followers [127]. In the IP terminology (NEMO in particular) these structures can be referred to as *nested* networks.

1.2.4 Impact of market penetration

In practice, vehicular clusters may be enabled by the recent evolution of 802.11p related standards, field deployments and experiments. While 802.11p Road Side Units (RSUs) continue their deployment, the support of 802.11p interface may become mandatory in vehicles (cf. eCall [116]). Recently car manufacturers proposed V2I communications through LTE due to higher market penetration and large coverage, making permanently Internet connected vehicles a reality. Therefore, IP mobility solutions should handle the different market penetration rates of vehicular communications equipments over the short, medium, and long term and design solutions that accommodate these cases.

1.3 Contributions

The contributions of this thesis report are as follows:

1. An in-depth study of current Future Internet approaches and their potential application the vehicle-to-Internet communications. In this part, we define the problem statement that originated the Future Internet movement and present the main trends. We then explore the requirements for Future Vehicular Internet communications as defined in the state of the art.

2. Use cases that benefit from vehicle-to-Internet communications. Through mobile eHealth and Fully-Electric Vehicles, we illustrate the use of IP-services in a vehicle-to-Internet scenario and show the common technical requirements.

3. Analytical study of Network Mobility extensions in host-based, network-based and distributed mobility management protocols. In this study, we discuss the implementation of network mobility extensions in different standards and show the message exchange diagrams in different approaches. We then propose two extensions to support network mobility in DMM. We also compare the protocols from an analytical standpoint and discuss their performance.

4. Introduction of Vehicle Identification Numbers (VIN) as a new namespace for Future Vehicular Internet communications. We define our communication architecture and present the advantages of integrating vehicle-to-Internet communications as a core part of the Future Internet architecture. We then integrate VIN6 addressing architecture to LISP-MN protocol and analyze the performance of our solution.

5. An in-depth study of auto-configuration protocols for vehicular cluster communications. We show the importance of a local unique addressing pool (based on VIN) for the leader and followers in a cluster for vehicle-to-Internet communication use cases. We then compare the proposals from different viewpoints.

1.4 Publications

This work has produced the following publications so far:

1.4.1 Journals

- Imadali, S.; Kaiser, A.; Sivrikaya, F.; El Sayed, N.; Boc, M.; Klaudel, W.; Petrescu, A.; Veque, V., A Review of Network Mobility Protocols for Fully Electrical Vehicles Services, Intelligent Transportation Systems Magazine, IEEE , vol.6, no.3, pp.80,95, Fall 2014

- Imadali, S.; Karanasiou, A. ; Petrescu, A. ; Sifianidis, I. ; Velidou, V. ; Vèque, V. and Angelidis, P., eHealth Service Support in Future IPv6 Vehicular Networks, Future Internet 5, No. 3, pp 317-335, 2013.

1.4.2 Confrences

- Imadali, S.; Veque, V.; Petrescu, A., Analyzing dynamic IPv6 address auto-configuration techniques for group IP-based vehicular communications, Local Computer Networks Workshops (LCN Workshops), 2014 IEEE 39th Conference on , vol., no., pp.722,729, 8-11 Sept. 2014

- Decremps, S.; Imadali, S.; and Boc, M.; Fast Deployment of Services in SDN-Based Networks: The Case of Proxy Mobile IPv6, 2014 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNet'2014), Rome, Italy, 2014.

- Imadali, S. ; Veque, V. ; Petrescu, P. and Boc, M., VIN6 : VIN-based IPv6 Provider Independent Addressing for Future Vehicular Internet Communications, 24th annual IEEE Internantional Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC'13), London (UK), 2013

- Imadali, S. ; Kaiser, K. ; Decremps, S. ; Petrescu, A. and Veque, V., V2V2I: Extended Inter-Vehicles to Infrastructure Communication Paradigm, 4th Global Information Infrastructure And Networking Symposium (GIIS), Trento (Italy), 2013.

- Imadali, S. ; Petrescu, A. and Veque, V., Algorithmes d'Adressage et Routage pour des Reseaux Fortement Mobiles à Grande echelle, Journees Nationales des Communications dans les Transports, 29 et 30 Mai 2013, Nevers (France) (Best paper award)

- Imadali, S. ; Karanasiou, A. ; Petrescu, A. ; Sifianidis, I. ; Velidou, V. and Angelidis, P., Integration of eHealth service in IPv6 Vehicular Networks, 3rd International Conference on Ambient Media and Systems (Ambi-sys), Athens (Greece), 2013

- Imadali, S.; Karanasiou, A. Petrescu, A.; I. Sifniadis, and V. Veque (CEA, VIDAVO), EHealth Service Support In IPv6 Vehicular Networks, VECON 2012, 2nd Int'l Workshop on Vehicular Communications and Networking (in conjunction with IEEE WiMob 2012), Barcelona (Spain), October 2012

1.4.3 Patents

- S. Imadali, A. Petrescu, C. Janneteau, Dispositif et procede d'adressage d'equipements embarques a bord d'un vehicule, CEA, Avril 2014.

- S. Imadali, A. Petrescu, C. Janneteau, Methode pour la translation (mapping) d'un numero d'identificateur de vehicule (VIN) vers des numeros d'adressage IPv6 (adresse, prefixe, adresse et prefixe), Patent Application (CEA), July 2012.

1.4.4 Internet drafts

- Imadali, S. ; Petrescu, A. and Janneteau, C., Vehicle Identification Number-based IPv6 Interface Identifier (VIID), IETF Internet draft, 2013

- Imadali, S. ; Petrescu, A. and Janneteau, C., Vehicle Identification Number-based Unique Local IPv6 Unicast Address (VULA), IETF Internet draft, 2013

- Petrescu,A.; Janneteau, C.; Demailly, N. and Imadali, S.; Router Advertisements for Routing between Moving Networks, IETF Internet draft, 2012.

1.5 Dissertation outline

This dissertation is structured as follows:

- **Chapter 2:** reviews the deployed Internet architecture and its actual growth over time. It also presents main Future Internet approaches and trends. On a second part, we give a review of current enabling technologies and network protocols for vehicular communications.

- **Chapter 3:** covers two scenarios of vehicle-to-Internet communications: eHealth and Fully-Electric Vehicle services.

- **Chapter 4:** reviews and analyzes network mobility extensions in centralized and distributed mobility management protocols.

- **Chapter 5:** defines the solution space that enhances scalable Future Vehicular Internet communications and the technical requirements to be met. VIN6 is introduced and integrated to LISP-MN protocol.
- **Chapter 6:** discusses the application of VIN namespace to vehicular cluster communications and analyzes its benefits when compared to state of the art approaches.
- **Chapter 8:** outlines directions for future work, and concludes the dissertation.

Chapter 2

Background and Related Work

The Internet experienced massive growth since its inception, especially by interconnecting research networks (ARPANET) to commercial network owners (ISPs) in 1988 by the NSFNET project [192]. One of the keys to its success is the simplicity of its network architecture, often referred to as "dumb network, smart ends" [164]: complex functionalities resides on the computers connecting to the network; the latter focuses on routing data between those computers. This principle allowed the development of complex applications with no modification to the underlying network. Other technical and non-technical principles have driven the current Internet architecture expansion. These requirements originated from different design objectives such as survivability, distribution of management, resource sharing and supporting different types of services [40]. The first part of this chapter discusses briefly the design directions and core principles involved in Internet Protocol design.

However, as stated by the Internet Architecture Board (IAB) Workshop on Routing and Addressing document [146], there is a particular concern about the impacts of scalability on Internet routing. Indeed, the use of more specific IP routing-prefixes (usually, Provider Independent addressing) to support Multihoming, Mobility, Traffic Engineering and other unforeseen applications at the early Internet stages, increases significantly both entropy and sizes of Border Gateway Protocol (BGP) inter-routing tables [10]. The Internet can be broken down to a set of Autonomous Systems (ASes) as a collection of interconnected networks [38]. This design choice results in the unbound growth of routing information stored into the routing hardware keeping state for every destination. These scalability concerns are worsen by the introduction of novel use cases including Machine-to-Machine communications, Internet of things, Vehicle-to-Internet communications and an ever growing number of mobile users [101]. The second part of this chapter focuses on Future Internet research and presents a topology of main trends.

Vehicle-to-Internet communications with regards to standardization run on an IPv6 end-to-end model [132]. Recent efforts within IETF pushed the IP version upgrade from IPv4 (depleted addressing pools [8]) to version 6, that is provisioned to uniquely address all mobile consumer electronics devices and all vehicles [112]. With the native support of mobility, privacy, security and optimized auto-configuration techniques, IPv6 brings some upgrades when compared to IPv4. In the third part of this section, we present some of the IPv6 features that are of interest to the Vehicle-to-Internet communications. We also discuss the main applications and standards trends in the vehicular environment.

2.1 Evolution of IP

The Internet architecture evolves following the layers of standard protocols deployed around a set of building blocks [75] [38] [23]. However, some principles at the heart of the architecture design are now challenged. This section will describe these design principles and explain how they influenced the expansion of the Internet, and why these principles are made obsolete by the new challenges, in particular the *Locator/Identifier split*.

2.1.1 Fundamental building blocks

The literature describes a set of principles referred to as the "Internet building blocks". These principles were introduced gradually to reach certain goals such as *survivability* in case of military attack, be *cost effective*, allow *distributed* management or include a *variety* of physical networks [75][38]. We here mention a (non-exhaustive) list of those concepts.

2.1.1.1 End-to-End Argument

The E2E argument is one of the most cited of the Internet design principles. It states that a mechanism *should not* be placed in the network if it can be placed at the end node, and that the core of the network should provide a general service, not one that is tailored to a specific application [40] [188]. One of the consequences of this approach is the design of a 'dumb' network and 'smart' endpoints [164] [113]. The rise of the Internet, in the 90's, has benefited from the widespread use of the Personal Computer including natively a TCP/IP stack in the operating system. Cheap deployment of this dumb network was due to the smart endpoints that would use it eventually. This migration of intelligence (when compared to earlier telecommunication networks) toward the edges led to the concentration of administration and maintenance in the edges also [164].

The main advantage of the end-to-end approach is *innovation*. The deployment of various applications is due to the simplicity of the Internet protocol and its very general purpose design and objective (carry a set of bits). Another advantage that arose from the E2E principle is the reliability of applications as long as the network stays simple [40]. The E2E is not an absolute rule but rather a guideline for application and protocol design analysis [188]. Mail delivery system, where users send their mails to mail servers (SMTP) rather than endpoints, is one example where the E2E principle does not apply.

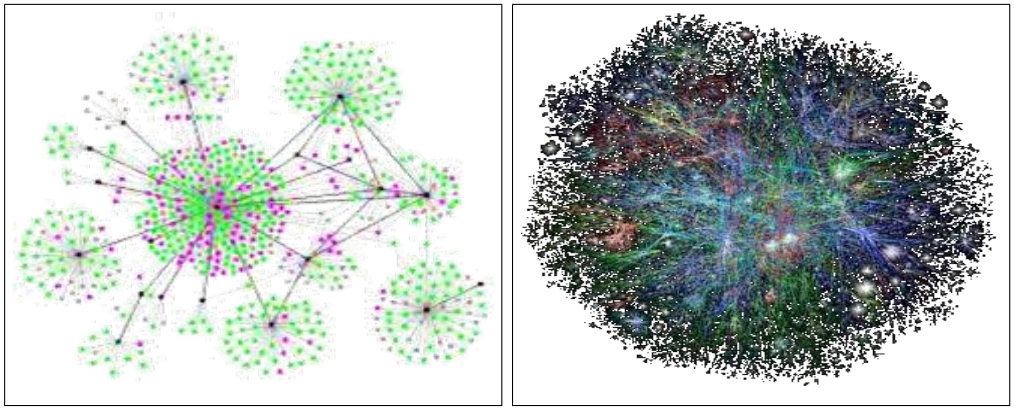
In today's Internet, other mechanisms are clouding up our vision of the entire system and challenging the E2E concept. If encryption was the E2E principle designers answer to the security concerns [188], deploying firewalls at the network boundaries is much more common these days. Firewalls break the E2E model, and change the nature of the Internet *flat* architecture which is less transparent and no longer trusted [40]. Network Address Translation (NAT) mechanism is another technical concept breaking the E2E design of the early Internet. NAT mechanism is the answer to the IPv4 addressing space shortage, privacy concerns and private address space management [181] [210]. Due to NAT Boxes, the non-mutability characteristic of the IP address; that is, the source and destination addresses sent in a packet are those received by the destination, is no longer valid. The same goes for the omniscience of an IP address; that is each host knows what address a peer host could use to send packets to it [148] [158].

Revisiting the E2E concept and redefining it is an ongoing tussle between those who want to enhance their applications with more functionality and reliability and those who want to preserve the simplicity and transparency that made the success of the Internet design [40].

2.1.1.2 Network of interconnected networks

One major concern of the DARPA Internet Architecture was the development of effective techniques to interconnect and use already interconnected networks [38]. The interconnection of the packet radio network [126] with the already existing ARPANET in the late 70's was a major achievement in this context. The goal was to access services offered by the ARPANET servers (measurements and analysis). The Internet's original components are networks, and one main design objective is to interconnect them in order to provide a larger service. The Internet follows a *down to top* design approach. The alternative *top-down* design would have been a unified large system incorporating the needed technologies and *modular* enough to allow extensions for unforeseen applications; an impossible task [75].

Figure 2.1: Network of interconnected networks.



(a) Network of networks. The overall picture represents a decentralized network (Source: Scale-free networks, Guido Caldarelli, Oxford Finance Series).

(b) Internet map as of 16th January 2009 (Source: Cisco IBSG, 2006-2011, Guo-Qing Zhang New Journal of Physics, Guardian, UK)

The *universality* of the Internet protocol is also due to the universality of the IP layer [30] that runs on top of (almost) any technology and allows interactions between heterogeneous technologies like Ethernet, X.25, FDDI, Cellular, modem and other communication technology standards. The wide use of IP is clearly one of the reasons of the IPv4 addressing space shortage. The advent of the IPv6 with its huge addressing space (2^{96} times bigger) will certainly encourage other technologies to consider merging with the Internet, using Address Translation Gateways, speaking IPv6 on their egress interface and some other technology (802.15.4, for example) on the ingress interface. Note that the initial meaning of E2E principle is changing, as the gateways are responsible of managing translation tables between nodes IDs in the non IP technology part of the network and IPv6 addresses for these same nodes.

This mapping is essential for maintaining E2E communication sessions (as in 6LowPAN). This is a broad scope problem faced by the Internet of things [101]. A high-level overview of the Internet shows that it can be broken down into a set of Autonomous Systems (ASes) each composed of multiple routers organized into collaborating networks. The routing decisions are taken based on a routing table at each router calculated in a distributed manner: within an AS, interior gateway protocols (IS-IS and OSPF) are used and exterior gateway protocols (BGP) between two (or more) ASes [75]. This distributed design which continues to provide communications service, even when networks and gateways are failing (survivability) is a military context legacy [38].

Along with the *survivability* objective, the *down to top* design of the Internet architecture

allowed to achieve distributed management of its resources and to support multiple types of services. These design goals have strongly shaped the Internet as we know it [75] [38].

2.1.1.3 Packets as the basic unit of data exchange

The datagram is a self-describing packet containing an invariant source and destination IP addresses, a source and destination port numbers and a data payload. A shortest path between the source and the destination addresses is selected in a distributed manner (no coordination between routers) in order to carry the packet to the destination host. The destination port number is used within the host to deliver the payload to the right application. Delivering packets is then a two-phased dispatch operation: First, between nodes on an IP-layer decision basis, second, within the node on a port-ID decision basis [37].

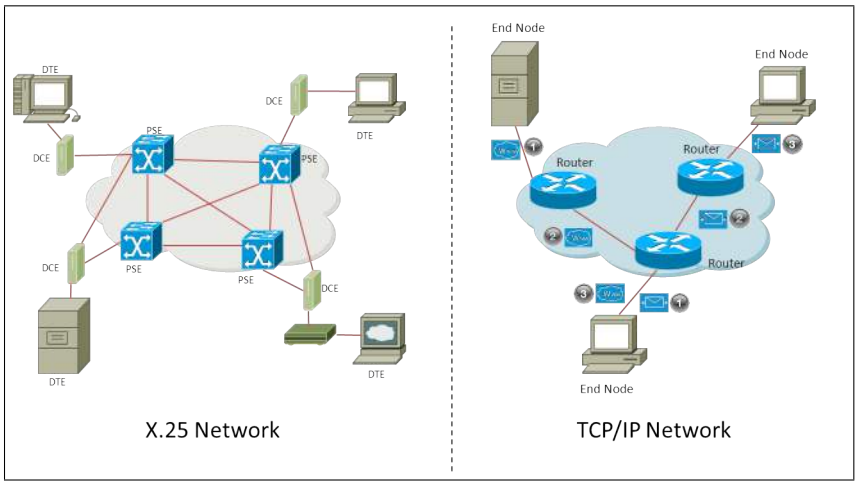


Figure 2.2: A comparison between virtual circuit-switched networks and TCP/IP networks

Experience has proven that the datagrams for universal fine-grained statistical multiplexing is the right data exchange model to apply in large heterogeneous networks, especially for bursty and intermittent traffic [39]. The best effort model and QoS mechanisms are direct consequences of this design choice. A *global stateless routing system* is another important design objective achieved by packet switching. There is no *connection state* saved within the intermediate switching nodes (routers) and thus, after a failure, these nodes can recover without concerns about state. Only endpoints will save the current state information of communication sessions (TCP); when failing (the session), this is highly likely due to host failure, what is often referred to as "fate-sharing" [38].

2.1.1.4 Layering

The network layering model (or vertical integration) has various advantages as reduction of complexity, isolation of functionality and a unified model for designing network protocols. These layers, during a communication session between two (or more) hosts, show a bilateral agreement (logical communication) between the endpoints.

The network layer is the only layer requiring universal agreement [117]. The TCP/IP layered model is the Internet protocol stack (from top to down) application, transport (known as upper layers), network (IP), link and physical (bottom layers). The upper and bottom layers experience frequent and rapid innovations, whereas the network layer is difficult to evolve as it implies a universal change. This state is sometimes referred to as *ossification* [5].

The IP layer, for its simplicity and capacity to run on top of (almost) any technology, is the main reason for the Internet's success. Another view of the Internet protocol architecture [51] shows the protocol stack as an hourglass where the IP is the common waist between all IP-capable nodes regardless of the communication technology used in lower layers and applications above. This is what enabled the integration of heterogeneous network technologies into the global Internet architecture [75].

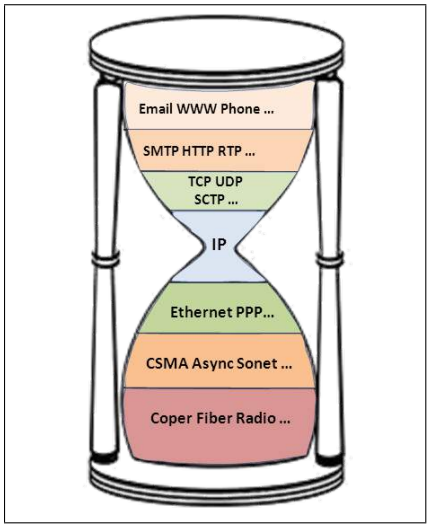


Figure 2.3: The hourglass model of the TCP/IP stack

The IP layer comes with a *universal IP numbering space that allows identifying every IP-capable unambiguously.* The IP address is carried on each packet sent and according to the original Internet design (E2E principle), the address is unchanged across the network towards the destination [23]. The advent of private addressing space [181] as an answer to the IPv4 address space shortage and the use of NAT boxes have changed the classical network-layer addressing characteristics. IP addresses are now ephemeral, non-unique and a same node (its interface) can be assigned a different address each time it connects to the network, even if it does so from the same location.

Another issue related to the *layering mis-specification*, is the semantic overload of the IP address. According to authors of [38] and [48], historically, the TCP/IP was a single protocol in the original architecture design, but the desire to provide another type of transport service (connectionless; that is UDP) caused the separation of the two protocols into a network-layer and a transport layer. The 2006 IAB Workshop on Routing & Addressing [146] has clearly pointed to the overloading of IP address semantics as one of the major causes of the scalability problems experienced in the Default Free Zone (DFZ) within the tier-1 ISPs routing tables.

The IP semantic overload, or locator/identifier overload of IP, can be defined as follows: *addressing has a "who" significance (endpoint ID at the transport layer) and "where" semantics (locators for the routing system).* Different approaches aim at splitting (separating) both functionalities. Note that some solutions answer to the problematic with the addition of new layer between transport and networks [148] [161] while others try to specify two separate spaces: one for identification and one for location [71] [143], and some have tried to redefine the IP numbering space [163].

According to [48], the only addressing problem that interested the TCP/IP protocol designers was the width of the IP numbering space (hinting at the upgrade from version 4 to 6 of IP) despite seminal works on naming and addressing (such as [193] and [187]).

2.1.2 The good, the bad and the ugly: Overview of IP properties

Evolving from its original design principles, the Internet Protocol integrated a series of patches and additions to achieve novel challenges [23]. Certain IP properties are the result of deploying new addressing and routing mechanisms and others the consequence of Internet size growth. We here review some of these properties.

2.1.2.1 Early design consequences

- **Loss of universal connectivity**. Based on the original end-to-end argument [188], routers in the core network should be simply designed with one core function (routing packets) and end hosts should perform the smart processing of these packets [164]. One addressing requisite is that all *IP hosts* to be reachable to one another by the use their respective IP addresses. Modified addressing mechanisms (such as NATs, NAPT), firewalls, dual-stack IPv4 and IPv6 hosts, and dynamic IP addresses emerged and the Internet no longer has a universal addressing scheme. Recent proposals [48][158] argue for an additional layer between the transport-layer and network-layer, to identify the hosts uniquely in a universal common namespace and reinstate the end-to-end principle.

- **Mobility and Multihoming**. Mobile hosts change their point of attachment to the network frequently and wish to keep their active sessions running while roaming [52]. The original TCP/IP protocols suite were designed under the assumption of stationary hosts [38] that need to initiate a new communication session after a handover. To solve this issue from the network layer perspective, mobility was defined as an address translation problem. Basic services (location update, forwarding) and functional elements (location directory, address translation agent) were then introduced into the core network for this approach to be deployed [22]. In fact, this approach considers the IP addressing space for *two different functions*: as an *Identifier*, when the address is a *home address* and as a *locator*, when the IP address is provided by the *visited/foreign network*. The objective is then to maintain the same IP address for a host regardless of its location in order not to break the current active transport sessions. This redefinition of the IP addressing paradigm was later extended to solve multi-homing and site renumbering issues for large autonomous systems resulting in known scalability issues [49] [158].

- **Security and privacy**. Internet is becoming a critical infrastructure and indispensable for such areas as transport, health and public administrations. However, increasing concerns about vulnerable software and protocols mis-implementations make the trustworthiness of IP protocols suite a challenge in itself [101]. Firewalls and end-to-end cryptography are the obvious answers to protect users and inspect suspicious traffic, despite being insufficient at times. Nonetheless, problems such as privacy, trust and accountability cannot be solved on the technical solution space only and need to be viewed from other non-technical perspectives [158].

2.1.2.2 IP as an Identifier

Recent activities on IETF, IRTF and the networking research community focused on defining a new Internet architecture that alleviates the scalability issues due to inter-domain routing [146]. Eventually, these efforts were directed towards separating both functionalities of the IP addresses: end-systems *identifiers* and routing *locators*.

The IP semantics overload consists in considering the IP address as a name and a location depending on the use. This approach solved the mobility [22], multi-homing [81], and site-

renumbering [145] challenges to mention a few. However, these new approaches include some fundamental IP addressing invariants when viewed as identities [158] [148], namely:

- **Non-mutability**. This principle is derived from the end-to-end argument. It states that the *source and destination identities should be received as they were sent.* This means that no intermediate node on the path from the source to destination should be able to modify the source and destination fields of an IP packet. This is obviously no longer true since the advent of NAT and NAPT middle boxes.
- **Location independence**. Whether temporary or permanent, the identities allocated to both correspondents of a sessions *should not change during this association.*
- **Reversibility**. A return packet from the destination to the source should be easily built by *exchanging the source and the destination fields.* This is another consequence of the reachability in the end-to-end paradigm.
- **Omnisciency**. Authors argue that this property is a consequence of the previous properties. It states that *every host knows which identity can be used to identify him and let other peers reach him.*

2.1.2.3 Hierarchical design properties

State of the art approaches trying to achieve Identifier/Locator split of IP, define new namespaces (to derive names) that would eventually translate to IP addresses (locators) [2] [207] [77] [35]. These future Internet designs involve *resolution* at some point of the architecture. This translation from one namespace (URLs for example), to another numbering space (IP) makes use of the semantics or the location information included in the namespace definition.

Authors of [27] on the other hand, try to define a flat namespace that bears no semantics of any network hierarchy. This namespace identifies the host only, and another separate routing mechanism (based on CHORD [201]) locates the destination with no resolution like DNS. Through their proposal, the authors define some IP properties regarding its hierarchical design.

- **Isolation property**. Inter-domain routing protocols suffer from routing churns [203]. Indeed, changes inside a single domain (hosts and networks failures, renumbering and reorganization) may result in inter-domain routing protocol updates. For the core network scalability, these churns need to be rare. This is achieved by *containing the intra-domain changes inside the same domain* when possible. This is referred to as the *isolation property.* For not-directly connected autonomous systems, this also means that the packets will traverse no higher than their least-common ancestor to be delivered (regardless of installed policies).
- **Hierarchical addressing**. The IP namespace is usually used to bear hierarchical semantics representing autonomous systems internals. For example, private IPv4 addresses [181] and unique local IPv6 addresses [103] are examples of such use [210]. Such network address architectures are dependent on the topology, and thus determine the underlying routing operations.

2.1.3 The wind of change: Locator/Identifier split

The Internet is also a field of trials for engineers which results in new IP properties depending on the practice. On the one hand, *rough consensus* for protocol updates and adoption is preferred

within the IETF working groups, which strongly shapes the overall architecture [182]. On the other hand, at the Internet Service Provider (ISP) and the Autonomous System level, Traffic Engineering (TE) is very important. Traffic engineering is about optimizing the performance of networks and enabling new services. Such practice is becoming more popular due to the success of the IP-based services. Problems like TCP congestion, TCP unfairness and flow management are tempered and avoided by means of extensions to the current standards [179][183].

Other non-technical factors also promote changes to the current architecture. For example, we can consider the ISP traffic shaping due to external *political pressures* as one of these phenomena. The *loss of trust* is also one of the most critical. Indeed, the simple early Internet model when a known number of mutually trusting parties attached to a transparent network and exchanged files is gone forever. This growing concern about trust promotes new security architectures and other solutions that break the end-to-end principle which limits the innovation [40][23].

2.1.3.1 Problem statement of Internet growth

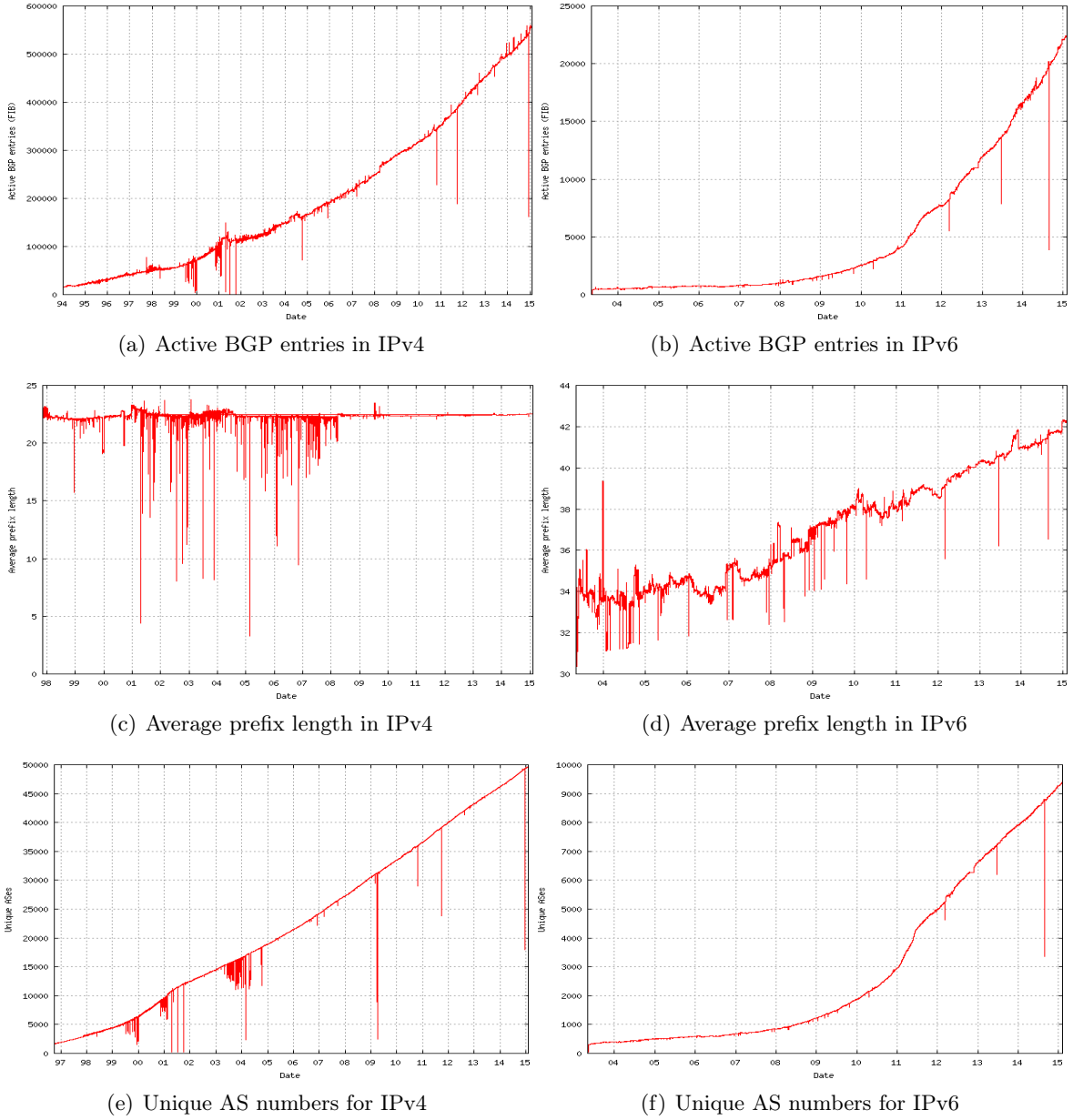
The current inter-domain protocol is the Border Gateway Protocol (BGP), the most recent specification of which is 4. The core Internet routing system is based on network prefixes and Autonomous System numbers. Network prefixes are routable IPv4 or IPv6 address pools. These prefixes can be assigned at various lengths to networks. They can be disaggregated, and it is possible for two prefixes of different lengths to be advertised, one which is a proper subset of the other. BGP deployments support Classless Inter- Domain Routing (CIDR) that which allows these variable-length prefixes. Autonomous System numbers are used to uniquely identify network providers and other companies with their own IPv4/IPv6 addressing space. Some or all of these address are advertised by ASes with the AS number of the origin attached in the BGP advertisement, propagated to other ASes and eventually installed in the BGP tables of ASes that offer transit services [202].

Figures 2.5(a) and 2.5(b) illustrate the network growth through active BGP entries as viewed from the AS6447 from the RouteViews Internet measurement project **??**. Although the IPv6 active BGP entries are far lower compared to IPv4's, both have grown exponentially over the last two decades. Figures 2.5(c) and 2.5(d) show the average length of advertised prefixes; That is how aggregated the announced prefixes are when announced by ASes. We here also observer the steady tendency in IPv4 (around 22) despite some drops, and the increase in IPv6 prefix length that will ultimately lead to more specific BGP routing entries, slower longer prefix match operations and overall scalability issues for the routing system. Figures 2.5(e) and 2.5(f) illustrate the increase of the unique AS numbers for the last two decades. We here also observe a clear advantage of IPv4 over IPv6 due to its popularity and success, also due to the fact that IPv6 deployments have only recently gained in importance and interest. The increase in the AS numbers demonstrate the huge number of Internet actors that are active to provide tailored services to their customers, or support advanced traffic engineering techniques (multi-homing and more). All these interactions lead to impacts known as BGP churns on neighboring ASes an ultimately the whole core network, when a sudden change occur in one of the systems.

2.1.3.2 Discussion and directions

The Internet is a heavy complex engineering system: any significant change to the IP layer, the waist of the hourglass that holds the system together, can lead to great instability in several domains, as more and more applications rely on the Internet as a middleware. Recently proposed enhancements, like IPv6, Mobile IP, IPSec, QoS mechanisms and multihoming despite their in-

Figure 2.4: Problem statement of IPv4 and IPv6 Internet growth



(a) Active BGP entries in IPv4

(b) Active BGP entries in IPv6

(c) Average prefix length in IPv4

(d) Average prefix length in IPv6

(e) Unique AS numbers for IPv4

(f) Unique AS numbers for IPv6

trinsic worth, cost too much in terms of deployment: triangular suboptimal routing, deployment of new entities breaking the E2E principle and more. Consequently, these enhancements remain as unresolved challenges, at least for the global Internet [183] [168].

Usually, we know two main directions to follow in order to change a system. 1) Evolving the system incrementally, by deploying new mechanisms (hardware and software) having the new desired features and stay backwards compliant with previous versions of the system. We can refer to these mechanisms by patches. Some call this approach "engineering method", as the costs of the overall solution appear amongst the first design goals. 2) Redesign the system from the scratch regardless of the already deployed system, following new core principles and having the desired features. This design method is the clean-slate approach, to which we can refer to as revolutionary method, opposed to the evolutionary one. It is often considered as a research

task, where the costs of the overall solution are the last design goals.

2.1.4 Evolutionary approaches

This section will cover the evolutionary approach for Future Internet. The IAB Workshop on Routing and Addressing [146] is the starting point of several proposals in the new IP Locator/Identifier split realm. The workshop participants pointed to the semantics overload of IP along with multihoming growing interest among ASes as the main reasons for the DFZ routing information tables growth causing overall scalability issues on the whole system [106].

We can classify proposed solutions based on the parts of the network that are affected by the patches. Indeed, some proposals (namely, Shim6 and HIP) applying the end-to-end principle, imply a change above the IP layer on all hosts and other solutions (LISP and GSE) imply an incremental deployment of routers with new capabilities in the core network.

2.1.4.1 Host-based approaches

There are two main solutions currently proposed at the IETF: Host Identity Protocol (HIP) [148] and shim6 protocol [161]. Both solutions change the network protocol stack to add a new layer in order to better handle the identities of hosts.

2.1.4.1.a Host identity Protocol (HIP)

There are two major contributions in this proposal: a host identity namespace and a new protocol layer, the host identity protocol layer. The Internet has two important namespaces widely in use: the IP addresses and the domain names.

The Host Identity namespace, defined as a set of cryptographic host identifiers, is the answer to the IP semantic overload and supposed to add completeness to already deployed namespaces [148]. The HIP protocol implies changes at the host stack. Endpoints are identified by Host identities used above the IP layer (IPv4 or IPv6) in the transport layer (TCP/UDP and more).

Hosts will be able to authenticate their peers directly when knowing the Identity, with this cryptographic namespace [158]. This additional namespace enhances the original Internet architecture by implementing the desired Identity/Locator split and changes the transport layer session binding to the Host Identifier and no longer to the IP address, making a number of networking challenges such as mobility, multihoming and even security easier to deal with.

More than an additional namespace, HIP aims at providing a new layer of indirection as it is believed that effective mobility support requires an additional level of indirection [158]. Thereby, mapping a transport session to the identity will ease handling mobility challenge. Multihoming is another hard networking problem tackled by HIP.

As part of the Base Exchange, IP addresses are used as locators and can be updated during a communication session [149] [159]. Renumbering, which is an unavoidable administrative burden, is handled as a particular case scenario of mobility. After the four-way handshake between the two peers, which is based on a sigma-compliant Diffie-Hellman key exchange using public key identifiers as a way for mutual authentication [149], shorter Host Identities are used in the HIP header to exchange packets.

The 128bit Host Identity Tag (HIT) and 32bit Local Scope Identifier (LSI) are such short identifiers. A HIT is built in an IPv6 format, where the 28bit prefix is 2001:0010::/28 and the remaining 100 bits are taken from the crypto hash of the host public key [158]. The HIT can be compared to the CGA address in the SEND context [12] where a 64bit Interface ID is generated through an algorithm where the host public key (among other parameters) is hashed to obtain the resulting IPv6 address.

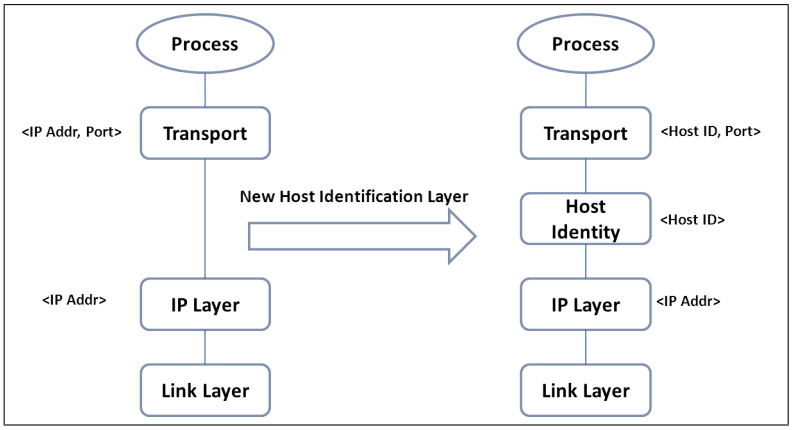


Figure 2.5: HIP layering model. The integration of a new Host Identity layer

When HITS are intended for global use as IPv6 addresses, LSIs are locally unique IPv4 addresses equivalents and cannot be reliably used to name hosts outside the network [148]. HITs are unstructured, not human friendly and not aggregatable. In order to retrieve a HIT (supposing HITs are stored in a distributed hierarchical database, such as DNS) a user must fetch the IP address, knowing a URN, along with its associated HIT. The opposite, i.e. starting with a HIT and fetching IP/URN from the DNS, is not possible currently. These issues, namely, a mapping/resolution system are discussed within the IETF HIP Working Group [158]. In order to provide mobility, a new entity is introduced: the RendezVous Server (RVS).

The RVS solves the simultaneous movement of endpoints problem and provides location management. The RVS acts as a permanent HIP host reachable whenever a correspondent becomes unreachable (it is the case during mobility). The RVS is involved in the HIP readdress packets by forwarding the I1 message to the correspondent host. RVS is solicited with HIP control packets only, once the locators are updated, hosts will communicate directly with no proxy server. The RVS is compared to the Home Agent of MIP protocol, but with more flexibility (HIP host knows more than one RVS, can change them dynamically and only solicited for control messages). In practice, stationary HIP hosts in the public Internet could provide a rendezvous service [158] [52] after a registration procedure [133]. DoS attacks is another topic addressed by HIP, for which it provides protection for transport protocols running on top of it [93]. From an implementation perspective, one can find OpenHIP, HIPL (HIP for Linux), HIP for inter.net, InfraHIP and pyHIP.

2.1.4.1.b Shim6

The shim6 addresses the multihoming problem and provides a locator/identifier split by the addition of a shim between the network and transport layers. From a technical point of view, shim6 provides stability to the upper-layer protocols (TCP, SCTP) by presenting a stable source and destination identifier pair, called Upper-Layer IDentifier (ULID) while changing IP addresses depending on the prefix in use (locators). Shim6, also known as "level 3 multihoming Shim Protocol for IPv6" [161] is designed for a better scalability of the global routing system using provider allocated prefixes (PA) to facilitate provider-based prefix aggregation [146].

This host-based approach supports a new networking layer (a shim) between the current network layer and the transport layer. An additional protocol, REAchability Porotocol (REAP) [9], is responsible of detecting failures between Shim6 communicating nodes, and switch between locators to re-establish the communication session. REAP is an enhanced ICMP protocol for

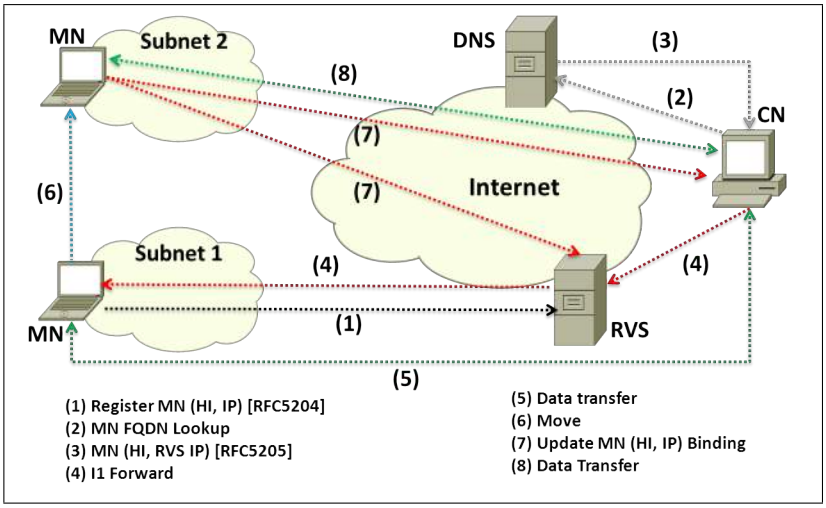


Figure 2.6: HIP mobility model

Shim6. In the protocol design, the shim layer is the one performing forwarding actions as selecting a suitable next hop for some destination, while IP contains end-to-end mechanisms, as IPSec [81].

One enhancement provided by the protocol, is the possibility of using different pair of locators (ULID) for different directions of the same communication session. Different communication sessions can use the same shim6 context. So the shim is shared between upper-layer sessions, i.e. different ULIDs may belong to the same session, and different sessions may have the same shim6 context.

In order to establish a shim6 communication between two hosts, a four-way handshake is specified. After this procedure, each host knows the different locators available for a given communication. The shim6 context creation (four-way handshake) does not have to occur at the beginning of the communication. Two messages update request and acknowledgement allow the hosts to change the set of available locators during a session. These messages can be used to support mobility or site renumbering. Once a communication context is established (creation of ULIDs with a set of locators), the context can be discarded, recovered or forked [81].

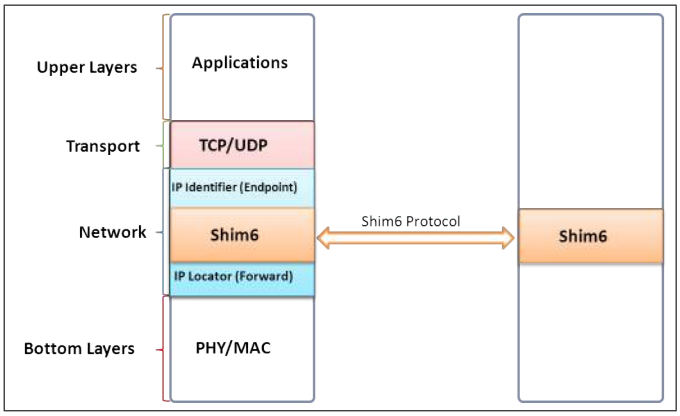


Figure 2.7: Overview of the Shim6 protocol. Communication between two Shim6 capable hosts.

The REAP protocol completes the shim6 architecture by detecting and recovering from failures [9]. REAP is implemented at the host level and allows finding new pair of locators when

unidirectional path failure occurs. A set of messages (Probe, Keepalive) and a timer (Send) are the protocol tools used to maintain the reachability of hosts and session continuity. In order to prevent Hijacking and flooding attacks, Shim6 proposes to map a cryptographic hash of Host Identity into the IPv6 address, i.e. using CGA and HBA [12] [14] and to use REAP Probe as a mean to detect communication diversion to random victims (flooding) by a shim6 context malicious update.

The overall cost of the Shim6 solution must not be neglected. First, every host stack has to be upgraded to support the new shim. The REAP protocol at the host takes responsibility of maintaining communication sessions and switching to a working identities pair when the currently used one fails. Another implication of REAP and other ULIDs facilities is the maintenance of additional information state about current communications. Also, as a host-based solution, it prevents ISPs from doing traffic engineering [146]. Finally, SHIM6 solution requires renumbering when a site changes providers. When the site changes one of its providers, it must purge the address block of that provider from the entire site. Using any of those IP addresses within policy-enforcement devices (e.g., firewalls) lead to an additional non-negligible re-configuration cost. The Shim6 working group at the IETF is now closed and (at least) two implementations exist LinShim6 and OpenHIP.

2.1.4.1.c MILSA

Authors of [121] [120] propose MILSA: A New Evolutionary Architecture for Scalability, Mobility, and Multihoming in the Future Internet. This proposal is based mainly on 3 principles:

1. ***"Evolutional Kernel"***. Changes made to the current Internet need to be evolutionary and maintain such principles as: layering, packet switching, and end-to-end argument.

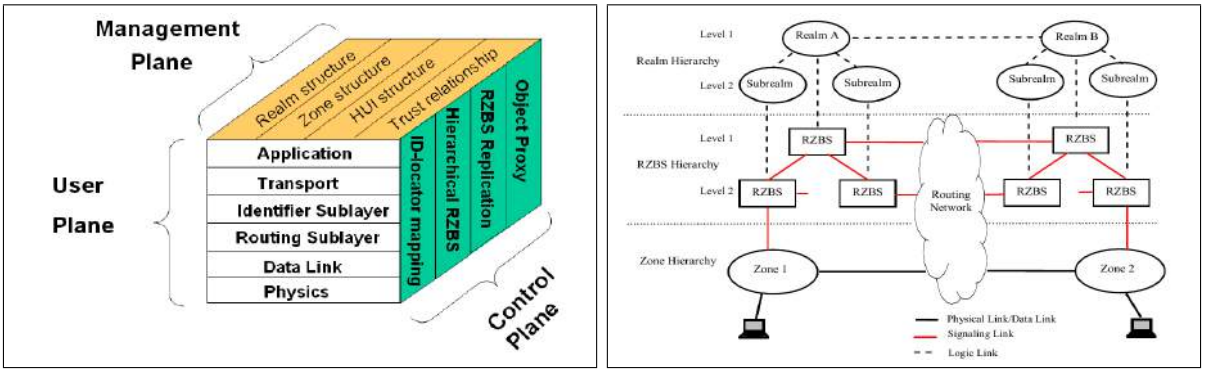
2. ***Variation and Diversity***. Diversity in terms of architecture, protocols, and applications is allowed to let the environment select the most competitive ones.

3. ***Fitness and Synergy***. Priority in the design is given to solutions with routing scalability, mobility and multihoming guarantees. If a technical solution is unfit for the chosen environment, its survival might be at stake.

Scalability of MILSA architecture is based on *Multi-Tier Separation*, i.e. neat separation of multiple logical tiers that "ossify" [209] the current Internet architecture. MILSA assumes a diversified Future Internet architecture with interfaces that interconnect different network technologies. In particular, MILSA provides a *separation of application/user/data/service, host, and routing infrastructure tiers* as the basic tiers representing communication entities. In terms of roles, the application/user/data/service tier depends on the host as the higher tier object to which it is affiliated. This is to restore scalable design and policy enforcements. MILSA includes every tier in its own realm: application/user/data/service realms (tier-1), host realms (tier-2), and routing infrastructure realms (tier-3). If we take the example of the mail infrastructure, the administration (university or corporation, for instance) provides email service to all its users; the administration may pick its routing infrastructure from different Internet service providers to which it is connected to. The core and data of mail service is then provided by the administration using one of many tier-3 realms. The hosts used to access the service may belong to one or many host realms (tier-2).

MILSA provides *Separation of Identifier Space and Routing Locator Space* and topological locators aggregation to enable routing scalability. The conventional IP addresses will be treated as IDs by Realm Managers (RMs) and mapped into locators for global routing in the core routing system (similar to the LISP approach). MILSA also advocates for *safe Traffic Engineering*

Figure 2.8: MILSA model and architecture



(a) MILSA reference model

(b) MILSA architecture

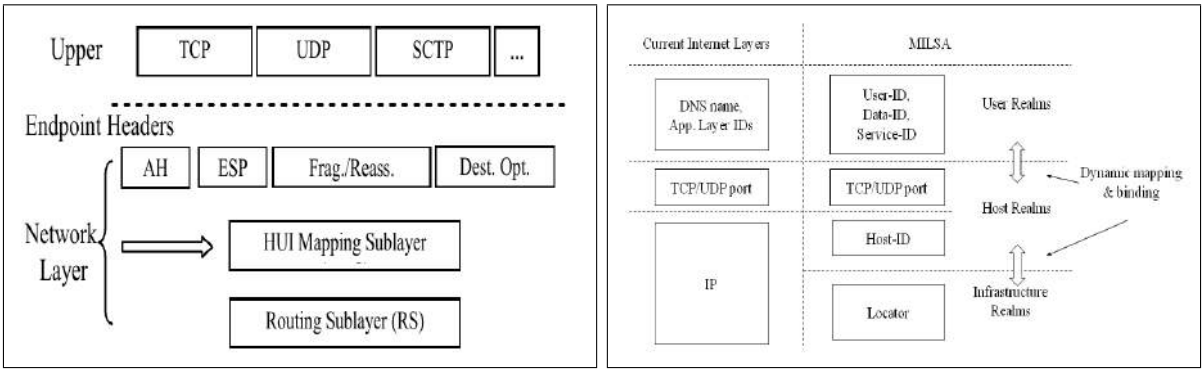
by separating the host-realm's Autonomous System policy from the routing policy, so that any commercial policy of AS will not mess with routing, and the locator aggregation can be guaranteed.

MILSA's design consists of three different functional planes to restore an end-to-end communication model based on the ID/Locator separation. The IP address is decoupled as ID and locator in *the data plane* and upper layer protocols/applications are bound to ID instead of locator. The ID to Locator mapping happens in *the control plane* as well as the locator-based routing and some host/routing-infrastructure interaction functions (such as three-tier mapping and object delegation). *Management plane* function is responsible for the management of objects and realms in various tiers. Dedicated RMs form the control plane, while the data plane consists of the MILSA Border Router (MBR) hierarchy. Signaling (control) links are set up between RMs. Trust relationships are set up among RMs and they can authenticate and act as proxies for each other. MILSA objects can have multiple IDs belonging to different realms. Hosts can have multiple locators to support multihoming. However, for future multi-tier separation, user/app/data may also have their own realms and RMs to negotiate trust or policy with other realms in different tiers and the mapping can be done between IDs of different tiers just like the mapping between Host-ID and locator.

In terms of implementation and deployment costs, MILSA requires a new host network stack to be installed and that will affect the current applications. The extra distributed global mapping system (realms and tiers) will also introduce costs. Authors argue that, although the cost may seem high, it will be beneficial in the long run in terms of better support of host mobility and multihoming, renumbering, policy enforcement, and more diverse upper-layer applications.

Noteworthy of mention, MILSA admits a variety of heterogeneous ID namespaces that can further map to a locator. Hierarchical URI-like Identifiers (HUI) name the objects in the network and may use different naming conventions. The MILSA's host-based network protocol stack includes an *HUI mapping sublayer* that maps the given HUI into a locator (using the control plane). Eventually, upper layer applications only know about the HUI they use (which is stable) and the lower layer only knows about the locator as mapped by the network. The HUI mapping sublayer is also responsible for the maintenance of multiple locators reachability in case of multihoming. Upper layer application sessions can also be bound to several HUIs with no effect on continuity in case of locator change. In terms of signaling, the MILSA approach for registering an HUI and mapping it into a locator, and further updating this locator during a mobile session, introduce a non neglectable cost. Indeed, this user-based approach requires the host to interact with the MILSA infrastructure and updates its control plane itself. In particular,

Figure 2.9: MILSA protocol stack



(a) MILSA's HUI sublayer (b) MILSA protocol stack

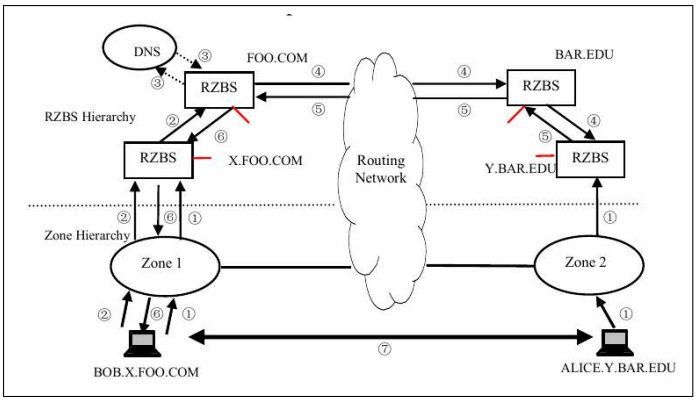


Figure 2.10: Connection establishment in MILSA

for connection setup, where the sender's realm manager (potentially, multi-level architecture) need to first reach the receiver's realm manager (also multi-level architecture) to fully locate it. As for the deployment, MILSA propose an evolutionary and incremental approach where the network infrastructure is first deployed and remains backward compatible to the current Internet.

2.1.4.1.d Other host-based approaches

Focusing on the mobility and multihoming enhancements, other host-based approaches exist. Multiple Address Service for Transport (MAST) proposal [41] [42] is another between-network-and- transport-layers approach. The author [42] suggests to use a control protocol between communicating endpoints, in order to map between a pool of locators (IP addresses) located in the bottom IP layer (IP-TR) to a unique endpoint identifier (EID) located in the upper IP layer (IP-EP). The first used IP address is the identifier presented to transport layer, while additional dynamic IP addresses as the host moves are considered as locators associated with the initial IP address (EID). A set of basic control messages (INIT, SET, PROBE and SHUT) are exchanged between hosts to start, maintain and close a MAST association. In order to maintain a permanent dynamic presence service and allow session establishment during host movement, MAST defines a new DNS SRV record [42] to associate a domain name (public stable EID) with the set of currently used IP addresses. Standard messaging operations to maintain the coherent state of this record are defined through XMPP [186]. Other approaches at the transport layer

also try to enhance the use of multiple IP locators for multiple transport flows. For example, Multipath TCP (MPTCP) allows the use of several IP addresses and interfaces on TCP, the first IP address obtained by the host being the ID of the session. A Linux implementation exists [151].

LIN6 [52] [204] uses a different approach from previous proposals, to split the IPv6 into an identifier and locator parts. The proposal considers the address as composed of a node identifier and a node locator, and the mapping operation between the two is done with the network layer. This proposal is not based on a new identification layer in the stack. In technical terms, there are three different concepts. (1) The LIN6 prefix, which is constant, (2) the LIN6 ID, which is globally unique and every LIN6 node has one, and (3) the current topologically correct IPv6 prefix. The combination between the LIN6 Prefix and ID is globally unique and remains unchanged within the host even if the node moves or is multihomed. The LIN6 address

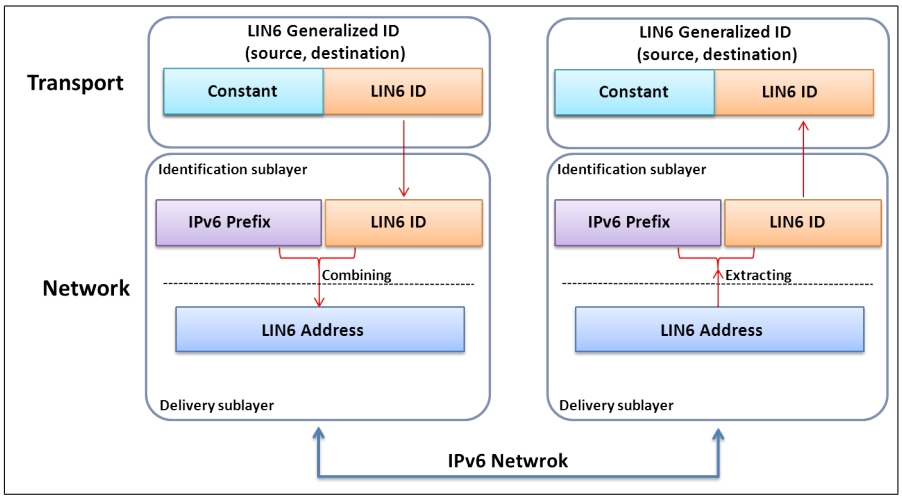


Figure 2.11: Transmission and Reception in LIN6

is composed of a LIN6 ID and a topologically correct network prefix. The resulting IPv6 address is then globally routable. The last 64bit part of the address (Interface ID for IPv6, LIN6 ID for LIN6) remains stable during node movements. To send packets across LIN6 architecture, an additional functional element is specified: the Mapping Agent (MA). The MA manages the mapping between a LIN6 ID and the current network prefix. When a peer queries DNS to obtain a mapping to an FQDN, the DNS server returns a LIN6 ID. This peer has to query the MA to obtain the topologically correct network prefix for the given LIN6 ID, and then the peer can send packets to its correspondent by concatenating the two information. The MA is updated whenever the registered node changes the network location and the CN mapping is refreshed by another control message form the mobile node. If the Refresh Request has no authentication header, the CN has to query the MA to obtain the new network location of its peer.

2.1.4.2 Network-based approaches

Unscalable core network routing tables growth is visible at the DFZ RIB and FIB size levels which evolve on an over linear growth [106]. Other issues related to scalability, like convergence time, cost and energy-consumption have been noticed. It is also believed that the advent of the IPv6 will worsen the problem with its huge addressing space, when IPv4 with its limited address space constrained the phenomenon.

Recent network-based approaches focus on the locator and identifier realms split. These

proposals describe the Internet as two parts evolving at different speeds. (1) Edge network, where the clients reside and where IP prefixes de-aggregation happens and (2) Core network, where aggressive IP prefixes aggregation should happen. By differentiating the problems, recent proposals [71] [145] [143] aim at providing a stable Internet where prefix aggregation would help reducing the routing table sizes in the core of the system. Another early proposal [163] tried to rewrite the IPv6 address to change its semantics and provide a way to enhance prefixes aggregation at different levels.

2.1.4.2.a Locator/ID Separation Protocol

LISP is a map-and-encap network-based protocol [145] [102]. The basic idea is to define two sets of elements: Routing locators (RLOCs) and Endpoint IDentifiers (EIDs) on a same numbering space, the IP, regardless of the version. EIDs will be used by hosts as identities, and RLOCs used by Ingress/Egress Tunnel Routers to route the packets in the core network. The expected advantages are similar to those of provider-allocated IP address space, where the aggregation is made simple, as opposed to provider-independent IP blocks used by some organizations to avoid the administrative burden of renumbering, even if it means additional non-aggregatable entries in core routers RIBs. Mapping-and-encapsulating was first defined in ENCAPS protocol [102]. The specification describes a simple method based on a combination of mapping operation and packet encapsulation as a medium term solution to evolve the existing Internet. The proposition is a medium term transition protocol with low costs, allowing the deployment of a new long term solution.

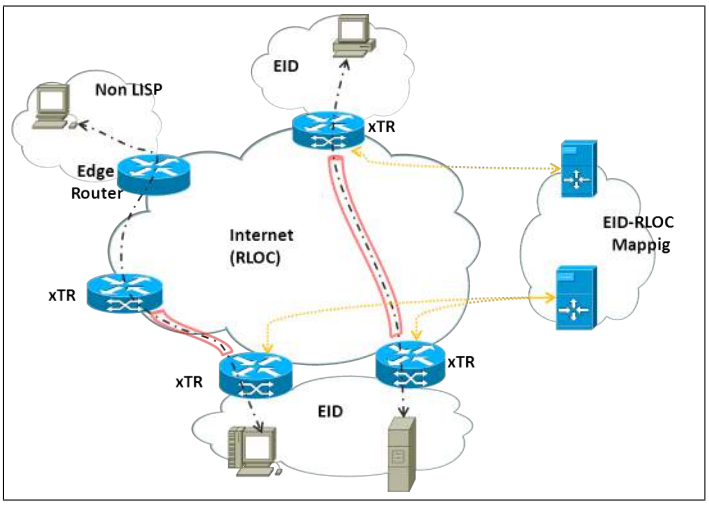


Figure 2.12: LISP Architecture

The LISP proposal aims at evolving the Internet by differentiating between hosts that use EIDs as identifiers and border routers that use RLOCs to forward (through tunnels) hosts packets to destinations. The border router decision on forwarding is made after an EID-to-RLOC mapping. The packet is then encapsulated. The inner-header will carry source and destination EIDs and outer- header the source and destination RLOCs. EIDs are much likely site scoped, but RLOCs must be global scoped.

LISP approach separates the protocol into two modules: data plane (map-and-encap) and control plane (mapping system). Various proposals for the mapping system exist, for example, based on distributed hash tables (DHT-LISP) [144]. LISP does not require host changes and does not change the core routing infrastructure. Two functional elements are needed to

deploy the solution: Ingress Tunnel Router (ITR) and Egress Tunnel Router (ETR). ITRs do LISP-encapsulation and the mapping operations, while ETRs do LISP-decapsulation and deliver packets to destinations [72]. At a host level, nodes sending data will do a DNS lookup to get destination EID before sending the packets. This does not change current hosts practice. The packets delivery will be handled by ITR/ETR routers by tunneling, after EID-to-RLOC ITR mapping operation.

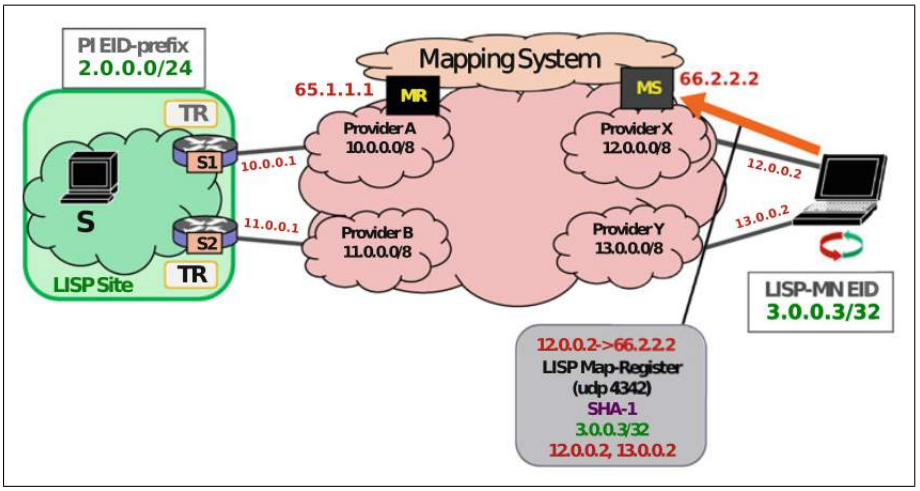


Figure 2.13: LISP Mobile Node registering procedure of an EID-to-RLOC binding

LISP specifies using an approach that is similar to MIPv4/v6 in order to handle the fast host mobility use case [72]. Indeed, the recent proposals in terms of mobility in LISP converge towards defining LISP Mobile Node (LISP-MN, illustrated in Figure 2.1.4.2.a) interactions with the Mapping System interactions, especially after a handover [73] [184]. Basically, a LISP-MN is implemented with a lightweight version of the xTR functionalities. The node is then capable of interacting with the Mapping System through Mapping Request (resp. Register) messages towards the Mapping System (resp. Server).

Similarly to the Mobile IP realm, a Mobile Node in LISP is provided with a permanent unique EID (name, Home Address in MIP) that reflects its identity. The LISP-MN when connected to a LISP-ready domain will receive an RLOC (possibly multiple RLOCs) that reflects its current point of attachment and also location (Care of Address in MIP). To be reached, the LISP-MN needs to make the obtained RLOC bound to its actual permanent EID at the mapping system where this binding record can be fetched by potential Correspondent Nodes. In order to achieve this, the LISP-MN will register this RLOC(s)-to-EID bindings into its Mapping Server. After a handover, the LISP-MN needs to ensure that CNs currently interacting with it, are able to refresh their Map cache entry that corresponds to this LISP-MN node in order for the traffic to continue without interruption.

In order to do this update and achieve seamless LISP domain handover, several mechanisms such as Map-versioning and Data-driven Solicit-Map-Request (SMR) have been defined within RFC 6833 and RFC 6834 [78] [108]. In some of this solutions, the LISP-MN has to interact with the ITR router in charge of the CN to force it (ITR) look for the updated version of the cache entry. This similarities between MIP and LISP-MN can be understood as the generalization of the Home Agent's Location Directory functionality hosted by a Mapping System.

LISP raises some performance considerations about encapsulation overhead and mapping lookup latency (control plane) [145]. In terms of implementation, we can find OpenLISP and Lisp for Cisco IOS, also LISPMob for LISP-MN implementations. Some large scale deployments

have also been reported [190].

2.1.4.2.b Global, Site, and End-system address elements (GSE)

GSE is an indirection approach to provide scalable multihoming in the network. The proposal [163] aims at providing aggressive topological aggregation to control the routing tables growth in the core network. The IPv6 address has to be redefined in order to achieve this. The address will then bear new semantics: (1) locator part, called Routing Goop (RG), (2) a local site information, called Site Topology Partition (STP), and (3) an interface ID of the endpoint, which is the End System Designator (ESD) in GSE terminology.

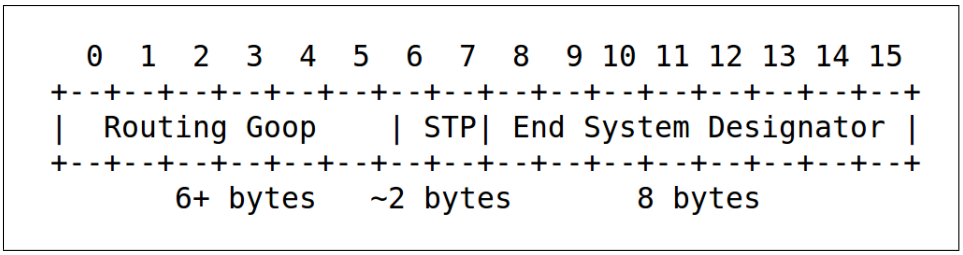


Figure 2.14: GSE IPv6 addressing format

The original proposition [162], called 8+8, of which GSE is the evolution, illustrates the IPv6 address format rewrite. The 16byte IPv6 address is split into two main parts. The first 8 bytes (left to right) are about site attachment and used to maintain compact routing tables with aggressive aggregation.

The first part of the 8 bytes (about 6 bytes) is the RG. It specifies a path from the root to a point in the topology. If a terminal is attached to this point of attachment in the topology [187] then the hosting network is a site defined by this unique RG. The Internet topology is consequently partitioned hierarchically in a tree fashion. Although cut-throughs can be defined through the hierarchy to illustrate the Directed Acyclic Graph (DAG) nature of the Internet [163], some network architecture experts [48] criticize this approach for this tree-like Internet shape that the IPv6 address will have to bear in the front part following the operating system model too closely.

The rest of the first 8 bytes (about 2 bytes) is the STP. This part is close to the meaning of the prefix. The author describes it as a partition of the site topology, or a segment. If a site administration wants to protect its network internals (as does the NAT Boxes), it can present a non-significant STP part to its peers. Otherwise, if the organization is presented as a structured site, inter-site topology will be disclosed as part of routing control messages, for example.

The second main part (last 8 bytes) of the IPv6 address is the ESD. This part is dedicated to the Endpoint (one interface on the system, to be accurate) and identifies it globally and unambiguously. The author proposes to create a new pool to generate such identifiers, especially for nodes not equipped with IEEE MAC address. Other nodes (majority) could use EUI-64 as an ESD.

The DNS mapping service will be augmented with a new association: to a name (FQDN) will be associated a (ESD, STP) pair and RG information in a "AAA" record. This will serve the source end- system before sending a packet to a destination. If the RG information is not available a special unspecified value can be put in the first 8 bytes and the border routers will replace this part with the appropriate value if the ESD is not on the site. To access on site-ressources, the site will provide a differentiated name service based on the source address: for

internal requests, only ESD (and STP) will be provided, but fully-general IPv6 addresses (actual RG information) will be returned to external queries.

The GSE proposal intends to ease renumbering burden associated with multihoming. Obviously, the RG part has to be redefined whenever a rehoming operation occurs. Different site types are assessed (provider, leaf) and rehoming courtesy and tunnels between former and new providers are presented as short-term solution reducing packet loss.

2.1.4.2.c Other network-based approaches

Another network architecture design approach [143] suggests to separate the IP addressing space into globally routable addresses (GRA) and globally deliverable addresses (GDA). Claimed enhancements are improved routing scalability and ease of site-multihoming.

GRAs are the addresses used within the DFZ domain, and are only reachable from inside the DFZ, while GDAs are globally unique and used to be reachable everywhere and do not appear in the DFZ tables. The point is that, rather than focusing on splitting between locator and identifier realms of IP, it is more effective to separate customer networks (edge) from provider networks (core) on an addressing-basis.

According to the authors, the GRA addressing space should provide a topologically aggregatable space that will help maintaining routing table size at an acceptable size. The GDA works with a mapping and tunneling system (map-and-encap) similar to the LISP approach. Border routers of source and destination (not located on the same site) hosts, encapsulate packets to traverse the DFZ, as it ignores the GDA addressing information state necessary to do the forwarding operation.

ILNP (Identifier Locator Network Protocol) [10], is inspired from the 8+8/GSE approach [163] and applies an identifier locator separation approach. The authors willing to provide an incrementally deployable solution, ILNP enhances existing IPv6. For instance, packet headers for ILNP and IPv6 are nearly identical. The 64 bit lower part of an IPv6 address in the ILNP context bears an ID semantics as in 8+8. The upper part of the address is the locator. The node ID is similar IEEE EUI-64 format, but identifies the host and no longer the interface. The identifier is not required to be globally unique. Hosts should be aware of ILNP to be able to detect failures and recover from them. ICMP protocol is used for locator updates and four new resource records should be supported by DNS. In ILNP, Hosts can be multi-addressed and by using Provider Allocated addresses. The address aggregation is possible [153].

In the previous presented solutions, we see that the host-based approaches are based on the observation that the classical layering model lacks in an identity layer. The authors proposed to add such a layer and built different protocols upon different definitions of what an identification space could be. These approaches do not contradict the network-based solution, but rather complete them. The network-based approaches try to split the global Internet into two types of networks running at different speeds. (1) The core network, where the routing operations have to be simple and routing tables compact. (2) The edge network, where as few changes as possible should be made and where prefix aggregation and deaggregation should maintain the scalability objective of the system.

2.1.5 Revolutionary approaches

New engineering challenges such as multicast, mobility, QoS mechanisms, multihoming, security and more arose with the growing interest of different domains in the Internet. Different types of applications call for different types of service which pushed the E2E design principle to the limits. A flat general purpose network design coupled with rich, complex and intelligent end

systems is far from being the answer to all these interrogations, at least from an efficiency point of view.

Some engineering approaches treated the problem, but this is not the only way to solve these issues. Clean-slate network design is another view of what could be the future Internet. Researchers and engineers of this field claim that a number of hard networking problems results from early Internet design legacy and therefore a design from the scratch could alleviate the burden and ease the integration of numerous enhancements.

By (temporarily) ignoring practical constraints and exploring a larger solution space, right solutions to current Internet technical issues should be provided and then adapted in an incrementally deployment scenario [183]. Different research initiatives tackling various problems have been described. The US Global Environment for Network Innovation (GENI) [82] initiative is a common infrastructure for future Internet proposals implementation. It is the experimental facility for the Future InterNet Design (FIND) from US National Science Foundation (NSF) research program. Future Internet is also one of the European Commission research targets as part of the Seventh Framework Program (FP7). The AKARI Japanese project is another instance of future Internet design initiatives [183] [75].

2.1.5.1 Content-Centric Networking (a.k.a. Networking Named Content)

Content-Centric Networking (CCN) [169] considers the content as being the building block and the original component of a new way to do networking. According to the authors [117] [195] the networking problem that originally guided the Internet design, namely resource sharing, is no longer a viable model to build the future Internet. The network users value the content and not the container. Instead of asking the question "where can I get this content?" (Basically, "classic" network design is about answering that question), users ask "what content can I get from the network?" (CCN makes the content as the priority and design the network according to that).

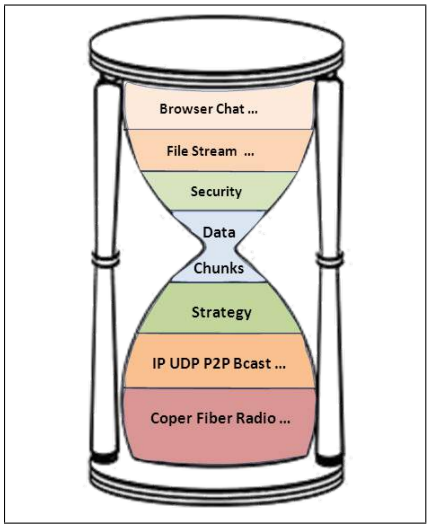


Figure 2.15: CCN's new hourglass

CCN is also concerned with security. While the first Internet design was built on trust assumptions, the CCN is designed with strong security objectives. The communication model change implies a security realm change too: when IPSec secures connections on which the packets travel, CCN secures the content itself. The communication design follows data consumer

model with only two packet types: Interest and Data. An Interest is broadcasted over available connectivity and a Data packet is sent by a node that hears the request. While the TCP congestion is handled by sliding windows, every Interest is consumed by the answering Data, so the flow control is maintained at each hop of the communication.

In order to perform basic CCN operations, three new data structures are defined. (1) The Forwarding Information Base (FIB), like IP FIB, it is used to forward Interest packets to potential sources on different interfaces (called faces in the CCN terminology). (2) The Content Store (CS), a buffer memory with maximum utility policy replacement (LRU, LFU) that enhances sharing between hosts.

When implemented in forwarding routers, CCN queries can be satisfied before arriving at the source. Data Integrity is of paramount importance in this context. (3) The pending Interest Table (PIT). The authors compare the Interest Packets journey through the network to "bread crumbs" left through the path in order, for the traversed nodes, to find a way back to the sender. The PIT is the data structure that keeps this trace. Whenever a Data packet answers an Interest, the pending PIT entry is removed.

An additional data structure, an Index, is consulted (in longest match lookup on queried Content Name basis) to find a suitable outcome for an Interest packet: if available on the Content Store, the Interest is satisfied. Otherwise, PIT then FIB will be consulted, respectively. The CCN transport provides delay tolerant networking whenever there is an opportunity to forward packets. CCN transport protocol is stateless and the application running above is responsible of resending an unsatisfied Interest request.

CCN names are hierarchical and humanly readable. In order to split data into chunks, unlike TCP sequence numbers, CCN uses versioning and segmentation notation along with a globally-routable name.

CCN enhances mobility by construction. While TCP sessions are bound to an IP address, which makes mobility a challenging concept, CCN does not need a binding at lowest layers, taking advantage of currently connected interfaces and choosing which one fits best its Interests. The strategy layer plays an active role to achieve this mission.

A CCN router can be placed in a routing domain among IP routers. For Intra-domain routing, CCN routers learn how to reach some content by some CCN router after hearing an announcement concerning this content. The router will install a FIB entry towards the announcing router, on a certain face for a given content. Same mechanisms apply for greater scope deployment (inter- domain) in a bottom-up driven deployment [117].

Security is also a central concern of the proposal [195]. Instead of trusting the original sender of the content and securing the path on which the data travels, CCN's approach is to use public keys to authenticate the link between names and content. The evaluation results show an interesting behavior of failover recovery during intermittent connectivity with no data loss. These benefits come with the price of changing the application development model.

2.1.5.2 ROFL: Routing on Flat Labels

This proposal aims at routing on host identities and ignoring network locations. In recent Locator/ID split proposals, most designs introduced a mapping or resolution service at some point in the routing process. ROFL [27] proposes a location free network layer and route on the identifier information. Hosts are named on a flat namespace with no particular semantics given to the name. These names can be public keys hashes, and are not mandatorily unique. Non-uniqueness is used in ROFL to perform anycast and multicast. ROFL work can be linked to compact routing [202]. As in CHORD [201], a circular namespace is created and notions of predecessor/successor helps to perform a reliable routing. In ROFL terminology, a host attached

to a router is said to be "resident" at this gateway router. The router is hosting that host ID.

Nodes are of three types: routers, stable and ephemeral hosts. The distinction between ephemeral and stable hosts is made by hosting router administrator. ROFL runs on top of intra-domain routing protocols, that helps detecting link failures and assumes self-certifying identifiers to prove a node's identity (spoofing prevention).

In order to achieve intra-domain routing, a newly attached host ID is considered as the predecessor ID of some (previously attached) node and the hosting router of this node is contacted, so it can install a source route to this newly attached node as well. This is the part of the CHORD join algorithm to establish source routes in the router cache. The routing is done from a node along its successor pointers: it is greedy. For inter-domain routing ROFL proposes a similar approach on an AS- level scale. To forward a packet, a router performs a host match function (known closest ID to destination) as opposed to longest-prefix match in hierarchically structured namespaces. An interesting property of routing in ROFL is the isolation; that is, of packets are exchanged between in-AS hosts, no external pointers (path across different ASes) are used. For hosts of different ASes, ROFL ensures that packets will not traverse higher than least common ancestor in the DAG resulting from merging rings. The isolation property guarantees also that failures and instability are experienced within one site and do not bias neighboring ASes routing. The authors argue that despite non-ideal performance results, the research in this should continue and the idea of routing on flat, non-hierarchical, semantic-free labels in chord-like graphs cannot be dismissed.

2.1.5.3 NIRA: A New Inter-Domain Routing Architecture

NIRA proposal [219] is about giving Internet users the choice of providers for their packets traversal. The main objective is to encourage the ISP market competitiveness, enrich the offers, reduce costs [40] and improve the end-to-end experience by giving the users the power of choice between domain- level routes. The end-to-end model [188] is redefined to contain three parts: the sender, receiver and the core. Technically, NIRA is built on top of two protocols: Topology Information Propagation Protocol (TIPP) and Name-to-Route Lookup Service (NRLS). TIPP maintains the user view of the up- graph network part of the overall architecture with two modules. (1) Path-vector part that distributes a set of available provider-level routes to the user, (2) policy based link state part that informs the user of the network conditions and allows a failure free packet delivery. Along technical concerns in the system design, some practical questions, such as payment modes, have been investigated to allow future concrete deployment. To achieve hierarchical route representation [163], NIRA chose a provider-rooted hierarchical address representation to encode the user-up-graph into the user's address.

Therefore, source and destination addresses are (both) used for forwarding and spoofing is limited since the address represents a hierarchy. The NIRA address representation can have two forms: (1) a fixed-length address with large addressing space. IPv6 is one example used by the authors [219] and (2) a variable-length address, which has not been demonstrated. For packet forwarding, NIRA proposes three forwarding tables routing model. The routing information is grouped through TIPP and forwarding decisions is made according to downhill table (for destination address) and uphill table (source address). If no match is found and no Core link is used to route the packet, a special table entry for a router with peering link may indicate the bridge table for the forwarding decision. The performance analysis of different parameters in NIRA (control overhead, convergence speed and setup latency) shows acceptable results for practical deployment. Some other issues, as temporary route oscillation and suboptimal route choice are left for future work.

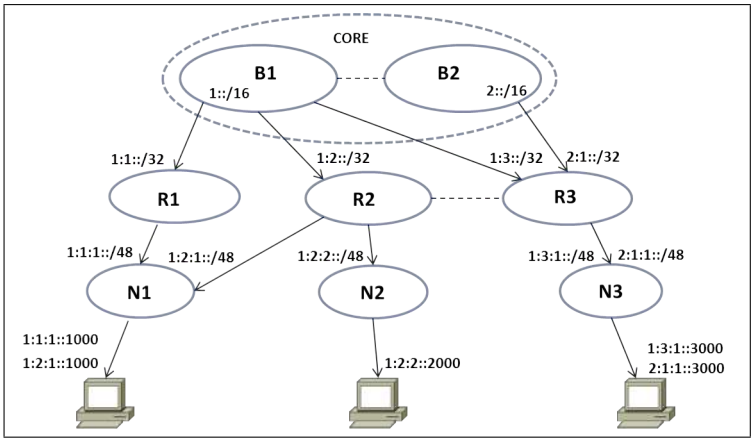


Figure 2.16: NIRA's provider rooted addresses

2.1.5.4 MobilityFirst architecture

Authors of [211] propose MobilityFirst, a revolutionary-designed future Internet architecture considering mobility and trustworthiness as central design goals. The architecture is later extended to include IoT [124], vehicular networking [15], OpenFlow [134] and more [74]. The fundamental change brought by MobilityFirst is that of a next generation Internet design that considers mobile devices, and applications, and the consequent changes in service, trustworthiness, and management as primary drivers of its architecture.

In MobilityFirst architecture, every object is identifier by a globally unique identifier (GUID) with a *flat* design that can be mapped to a locator through the Global Name Resolution service (GNRS). Due to its flat design, GUID of different entities (sensors, vehicles, laptops, content) can be visible (which differs from the hierarchical design of identifiers in MILSA, for example). Decentralized Name Certification Services (NCSs) binds securely any human-readable name (URI) to a GUID which is trustworthy. The GUID can further be a cryptographically verifiable identifier (e.g., a hash of a public key), to support strong authentication and security. For the packets that travel across the network, MobilityFirst proposes a delay-tolerant routing in order to accommodate a large set of applications and use cases, with in-transit caches that allow the data to be delivered in case of intermittent connectivity (typical of vehicular use cases).

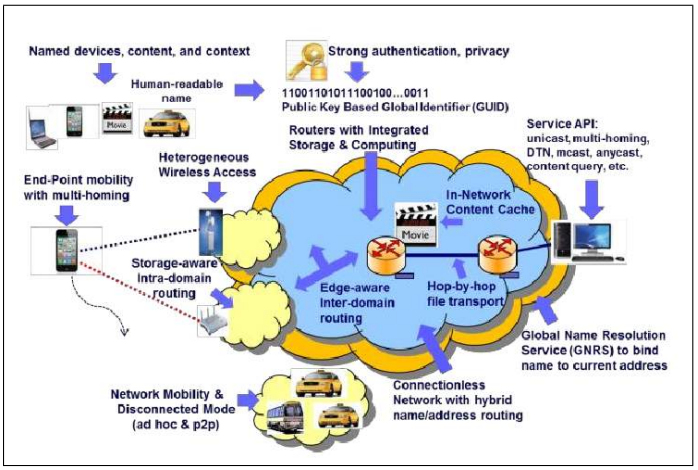


Figure 2.17: Design features of MobilityFirst architecture

Similar to LISP's centralized mapping system, MobilityFirst embeds its own mapping centralized system: global name resolution service (GNRS). The GNRS is designed to support a large number of devices, maintain the GUID and locator associations and to dynamically update it as the seamless mobility of devices would require. The GNRS has also the responsibility of separating the locators (network addresses, possibly IP) from the names (GUID, cryptographic hashes). As for the session establishment and connection setup, the interactions of the devices with their infrastructure are similar to that of todays Internet involving the DNS's resolution. As for the claimed scalability of the central GUID mapping system, unlike LISP's variety of mapping algorithms and topologies [145], it is yet unclear which approach is envisioned for mapping, dynamic update and network addresses aggregation in GUID.

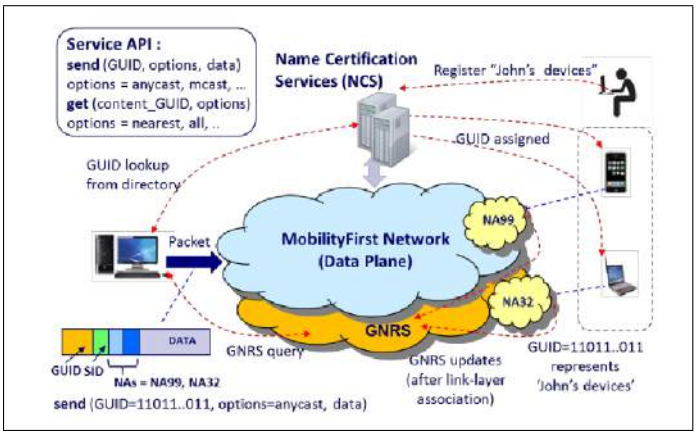


Figure 2.18: Session establishment for a typical communication of MobilityFirst hosts.

With regards to content delivery use case, the mapping updates frequency and the scalability of the naming/addressing scheme in both MobilityFirst are compared to CCN in [16]. Authors claim a better scalability in MobilityFirst's GUID system for content upload and mobility scenarios, while CCN (designed to retrieve content natively) is better at downloading chunks of data and worse in updating the routing infrastructure once the host moves. For example, in the use case of mobile VoIP calls, CCN requires the user to notify the infrastructure of its interest in receiving its correspondent's calls (if he wishes to be contacted using its original AS-dependent name). This may further result in a significant number of routing entries update with potentially large community of mobile users.

2.1.5.5 More clean-slate design approaches

Internet- architecture clean slate design is a new and widespread trend in network design. Different approaches tackling different angles are proposed [183]. The Japanese AKARI Project [4] aims at developing a deployable network architecture on short term. Different technologies have been considered for integration (radio, optical) and functionalities like guaranteed service, mobility, and security are considered early on the design. ID/Locator split is also one design goal for AKARI [125]. Hosts and border routers protocol stacks are augmented with an Identity Layer to achieve better mobility, multihoming and security. TRIAD Project [206] [35] as well as IPNL [77] considered a large scale NAT architecture, where routing could be done on FQDN-basis, considering them as hosts identifiers. TRIAD takes a content distribution perspective while IPNL focuses on routing and IPv4 addresses depletion problems. In FP7 projects, Trilogy project [207] considers the separation of naming and addressing in IP issues, in collaboration with the IETF. 4WARD [2] is another FP7 project for future Internet. Solution space includes technical issues,

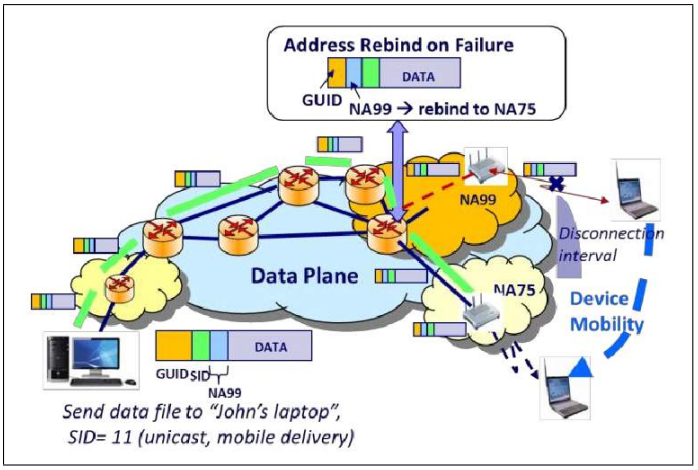


Figure 2.19: Mobile service under temporary disconnection and delivery of content.

as network virtualization and management functions, with non-technical problems, as finding innovative ways to generate value and employment opportunities. The clean-slate design model can benefit to the current Internet in many ways as some of the proposed changes can fit in the current architecture or included progressively. The security and mobility enhancements are such examples.

2.1.6 Discussion

Table 2.1 summarizes the main features of the Future Internet approaches that we reviewed in this section. The table compares Evolutionary (host and network based) approaches and Revolutionary proposals from a deployability perspective. The first criteria of analysis considers the support of mobile and multi-homed hosts/sites as well as the ability to provide for Traffic Engineering (which is very important for core network operators [179]). We also discuss the addressing/identification scheme, especially relevant in a locator/identifier separation perspective. In terms of deployability, the above proposals also need to be reviewed for modifications and new components introduced in the network. Finally, if a software prototype exists for a proposal, it is interesting to know whether it is possible to deploy the solution gradually.

Evolutionary, host-based proposals. One pattern is common among approaches of this category: *they either provide a new protocol stack, or a new naming/identification sublayer (layer 3.5)*. In his book "Patterns in Network Architecture, a return to fundamentals" [48], J. Day (network architecture veteran) questions the transport and network layers responsibilities in routing and delivering packets. Considering the pioneering works on naming, routing, and addressing of J.F. Shoch [193] and J. Saltzer [187], one of his conclusions was that IP and transport should be be considered as a whole composed of a number of sublayers (each with a function). For their *identity sublayer*, HIP and Shim6 propose to tie the identity of a host to public/private key pair for more security and trustworthiness. MILSA propose the use of hierarchical namespace (such as URLs) to derive host identities. LIN6 propose a universal identification layer of which derived LIN6 IDs can be stored as a DNS extension. MPTCP and MAST with more focus on transport layer do not assume an ID sublayer but use one of the multiple IP locators, as a stable identifier for the transport sessions.

In order to update the (multiple locators, ID) associations (at the host or the network), the previous proposals introduce their own control plane extensions. HIP and Shim6 rely on a more demanding control plane for secure base exchange among source and destination, whereas

MAST and LIN6 make use of existing DNS to extend its records with new options. MILSA also requires interaction with the infrastructure to initiate and maintain a session with the destination. MPTCP has an end-to-end control plane with no requirements on the network. These modifications also introduce new components to the network for some proposals, which means less chance to be wildly adopted with all the competing standards. These reviewed approaches can be introduced gradually as upgrades of legacy IP protocol stacks or as parallel software (with some regards to NAT traversal, retro-compatibility and scalability).

Evolutionary, network-based proposals. The main goal of the proposals in this category is to support legacy applications and devices while relieving the core network traffic overload through new components and better designed architecture. There are two opposing approaches to achieve this goal: *map-and-encap* and *address rewrite*. The first includes LISP and GRA/GDA, the latter is based on 8+8/GSE and later ILNP. These approaches have in common their support for host and site multi-homing, enhanced Traffic Engineering (load balancing, policy-based routing), and support for legacy IPv4 and IPv6 based hosts and applications.

The approaches differ when it come to to achieve locator/identifier separation at this level is the division. Map-and-encap category separates IP addressing space to locators (for core network) and identifiers (for hosts), the mapping function from one subspace to the other occurs at the site border routers (called xTR in LISP) and the data traversal happens inside a tunnel. For GSE/ILNP, the IPv6 address has to bear both the locator and identifier parts (64 bits) and the routers on the data path have to separate both parts and rewrite the locator part as the packets traverses from one site to the other. Regardless of the approach, these proposals modify the IP packet as it traverses one site to the other at the borders with no visibility at the user level. The control plane of the core network routers is mainly due to mapping entries updates/retrieval. These approaches being incrementally deployable, the main remaining concern is related to scalability of the hardware and control plane (especially for LISP [190]).

Revolutionary proposals. In order to overcome the restrictions of legacy Internet Protocol, approaches of this category propose to modify the host and network to create novel disruptive architectures. CCN and TRIAD focus on the content delivery as central in the design, while MobilityFirst architecture proposes this as an extension. ROFL states that addressing does not need to be hierarchical for the routing to be scalable. NIRA tries to empower the user by allowing him to choose the core network carrier for his data packets (based on the cost, for example). Among these approaches, CCN and MobilityFirst are currently implemented in GENI [82] and their work are ongoing. We also find proposals in IoT and vehicular and other different areas that extend the principle [6] [15] [124].

Category	Proposal	Reference	Mob., M-H., and T.E.	Add/ID scheme	Modifications	Network components	Deployment
Evolutionary, Host-based	HIP	[148, 158, 93]	Host mobility and multi-homing. No T.E.	Hosts are multi-addressed (PA addressing) and new (secure) Host Identity Layer	New host protocol stack, extensible control plane (base exchange, termination, status update)	PKI, RendezVous Points (Mobility)	Incremental with conditions [100]
	Shim6	[81, 161]	Host mobility and multi-homing. No T.E.	Multi-addressed hosts and new Shim6 sublayer for identity	New shim6 sublayer, modified control plane (context exchange and recovery)	None	Incremental
	MILSA	[121, 167]	Host and Site mobility and multi-homing. Load balancing through Locator change	Hierarchical Identifier sublayer, Locator given by Realm Managers	New stack, control plane, and Infrastructure. Interoperability through certain use cases	Realm Managers (ID/Loc mapping)	Incremental
	MPTCP	[151, 76]	Host mobility and Multi-homing. No T.E.	Compatible with current Internet. Multi-addressed hosts. One IP address plays the role of ID	Modified TCP to support parallel flows	None	Incremental
	MAST	[41, 42]	Host mobility. No T.E.	Multi-addressed hosts. First IP address is also ID. New addresses are updated in DNS	Transport layer can use parallel flows. Dynamic DNS updates for new locators	None (extends DNS)	Incremental with regards to DNS scalability
	LIN6	[165, 204]	Host and site mobility. No T.E.	LIN6 ID layer on top of IPv6. Transport runs over LIN6 ID. Mapping of LIN6 ID to IP is done through Mobility Agents	Modified control plane with extension to DNS and new MAs.	Mobility Agent	Incremental

Evolutionary, Network-based	LISP	[72, 145, 189]	Host and site mobility and multi-homing. Enhanced T.E.	Hosts can be multi-addressed (v4 and v6 EIDs). EIDs are mapped to Locators for delivery	xTR routers modify data packet headers. Control plane that includes mapping. Mapping system as part of the routing decision	Mapping System with choice of implementation	Incremental
	GSE	[46, 145]	Site Multi-homing and enhanced T.E.	Restructured address format. Aggressive network topology aggregation. The address is a path from the top to the end site	Modified address structure that encodes a hierarchical topology. Rewrite the prefix part when a data packet leaves a site towards a destination	None	Disruptive
	GRA/GDA	[143]	Host and site mobility and multi-homing. Enhanced T.E.	GRA for global transit network (tier-1 ISPs) and GDA for end sites. Border routers encapsulate data packets according to destination	Modified control plane that includes a mapping function and encapsulation of data packets	Mapping function (implementation dependent)	Incremental
	ILNP	[10, 11]	Host mobility and multi-homing. Enhanced T.E.	Hosts can be multi-addressed (locators). EUI-64 for identifying hosts. Tuple {Locator, ID} as a complete IPv6 address	Control plane (locator update) through ICMP. New resource records added to DNS	None	Incremental

Revolutionary	CCN	[118, 195]	Host mobility and Multi-homing. No T.E.	Names the content using user-friendly, hierarchical, location-independent names. Strategy layer chooses the best interface to reach a content	Routing based on the content. Hosts connected on multiple interfaces. Content-based security	CCN routers (IS-IS/OSPF/BGP with CCN extensions)	Incremental
	ROFL	[27]	Host mobility. Redefinition of policies for T.E.	Hosts are associated with a semantic-free self-certifying flat label. Routing system uses DHT (circular namespace)	Naming/addressing are based on flat labels. Routing is greedy and occurs as in Chord. ASes run their own ROFL-rings.	None	Disruptive
	NIRA	[219]	Host and site Multi-homing. Enhanced T.E. through policies	Legacy IP addressing	Use of provider-rooted hierarchical addressing and route discovery protocols to let a user discover his up-graph and choose his preferred ISP	None	Disruptive
	MobilityFirst	[211, 124, 15]	Host and site mobility and multi-homing. Enhanced T.E.	Uses Hierarchical namespace as node IDs. Supports multiple addresses by host. Mapping system associates ID and locator	New protocol stack, mapping system, control plane and naming conventions	Global Name Resolution Service, Name Certificate Service	Incremental

	TRIAD	[35]	Host mobility through redirection. Supports policy-based routing	Compatible with IP for routing. Uses URLs for naming hosts	Routing over URLs to the closest replica of the data. Use of content layer for locating and routing content	Content Routers, Content Servers	Incremental

Table 2.1: Summary of characteristics of the discussed Future Internet solutions.

2.2 Vehicle-to-Internet communications: requirements and architectures

Vehicular networking serves as one of the most important enabling technologies to support a large set of applications related to vehicles, vehicle traffic, drivers, passengers and pedestrians. Intelligent Transportation Systems (ITS) that aim to manage vehicle traffic, assist drivers with safety and provide entertainment for passengers, are no longer limited to trials and experiments [84]. Thanks to the active investments of car manufacturers and Public Transport Authorities, the essential enabling technologies components (radios, Access Points, spectrum, standards) are coming into place to finalize the deployment of VANETs (Vehicular Adhoc Network) and pave the way to unlimited market opportunities for vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-Internet applications [127].

Main examples of such services include automated toll collection systems, driver assistance systems and other information provisioning systems. The excitement surrounding vehicular networking is not only due to the applications or their potential benefits but also due to the technical challenges. High mobility of vehicles, wide range of relative speeds between nodes, real-time applications, Internet access at high speed, and a more system and application related requirements [84]. In order to tackle these challenges in coordinated manner the SDOs propose common compatible communication technologies in order to enable collaboration among actors of the field. Furthermore, considering vehicular networks as mere mobiles and apply the "business as usual" solutions and attach them via an edge gateway and delegate all interface functions and services to the edge, is becoming non economical and risky for the overall scalability of operators systems. Such challenges and opportunities serve as the background of the widespread interest in vehicular networking by governmental, industrial, and academic bodies to define technical requirements and architectures in order to find solutions [98].

This chapter reviews some of the aspects related to the vehicular networking technologies and defines some of the main requirements that academia and industry consider as essential enablers.

2.2.1 Overview of communication technologies

Leveraging wireless communication in vehicles is a motivating challenge that witnessed a large increase in research and development in the last decades. Some important enabling factors are all in favor of such an advent: the wide adoption and drop in cost of IEEE 802.11 technologies, the vehicle manufactures' and other stake holders' interest in ITS applications, and the involvement of large national agencies to allocate wireless spectrum for vehicular wireless communication.

Although cellular networks enable convenient voice communication and simple infotainment services to drivers and passengers, other wireless technologies are usually considered for applications requiring vehicle-to-vehicle or vehicle-to-infrastructure communications. With the availability since the late 1990s of low-cost, global-positioning system (GPS) receivers and wireless local area network (WLAN) transceivers, research in the field of inter-vehicular communication gained considerable momentum. Figure 2.20 illustrates an example of inter-vehicle and vehicle-to-infrastructure communications through the use of heterogeneous wireless communication technologies. The major goals of these activities are to increase road safety and transportation efficiency. Various European, US, Japanese (and more) projects are now completed and other underway to explore the potential of VANETs and the feasibility of large scale deployments. National governments also contribute licensed spectrum, generally in the 5.8/5.9-GHz band and at least in Japan, the 700-MHz band.

IVC among VANETs has a significant potential to enable diverse applications associated

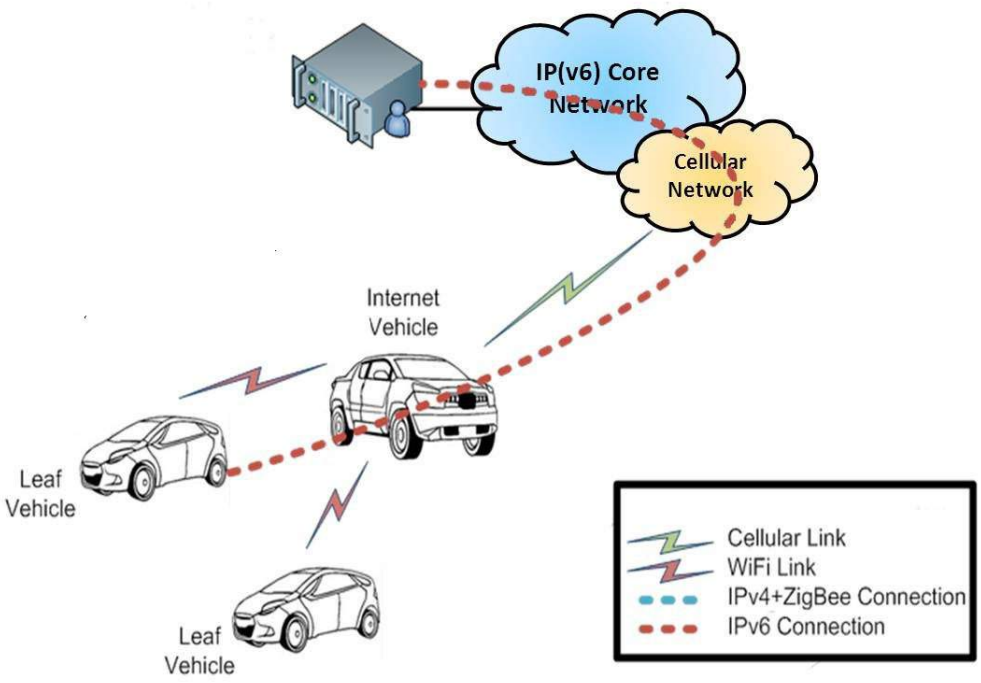


Figure 2.20: Heterogeneous wireless technologies for inter-vehicle and vehicle-to-infrastructure communications.

with traffic safety and efficiency. Radio access networks (cellular and WiFi) may be employed to enable vehicular communications with strict latency requirements for safety-oriented and emergency communications. These activities have resulted in a standardization effort among IEEE, ISO and ETSI for a new 802.11p WLAN extension specifically designed for such activities. This new WLAN standard defines a low-latency alternative network for vehicular communications, and their main focus has been the effective, secure, and timely delivery of safety-related information.

2.2.1.1 Cellular system

Starting with the GSM in the early 90s, UMTS later and now LTE/LTE-A, cellular systems are widely accepted for mobile communications and services. They are also used in vehicular environments to enable access to entertainment systems, map navigation, and traffic information. Cellular system support a wide variety of applications and are ubiquitous, with increasing performance at each major upgrade. Bidirectional information exchange (as opposed to broadcast systems, like AM/FM radio) allows manufacturers and other stake holders to propose innovative services, such as remote diagnostic or point of interests localization.

2.2.1.2 Bluetooth

Undoubtedly one of the most popular short-range wireless communication technology, the Bluetooth is managed by the Bluetooth Special Interest Group (SIG) and involves a high number of

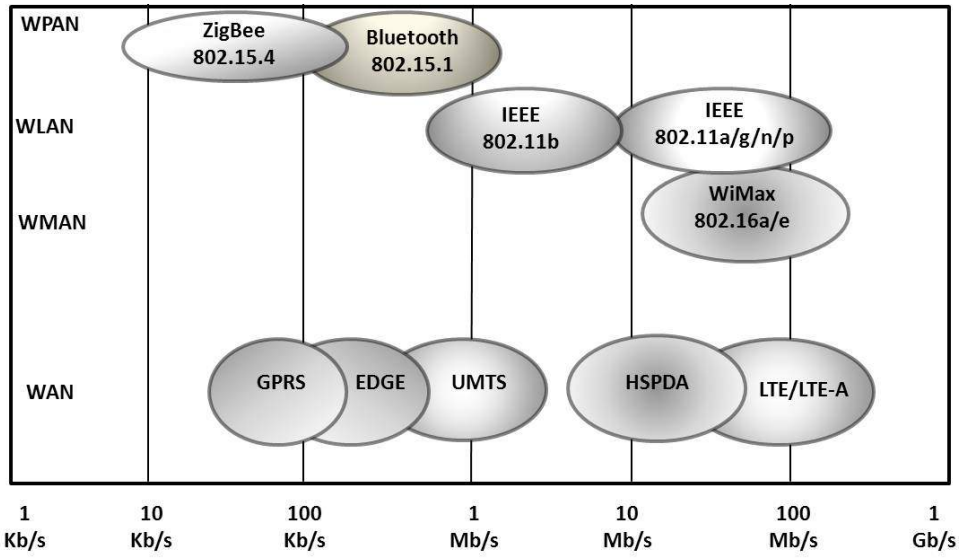


Figure 2.21: Radio transmission technologies used for IVC. A non-exhaustive list of wireless standards commonly used for vehicular-related communications. The use case depends on the radius of transmission, throughput, and the application.

interested companies. Bluetooth can send data over the unlicensed spectrum (2.4-2.485 GHz) spectrum on short distances, usually 1-100m and allows to create secure Personal Area Networks (PAN). In the vehicular networks, this technology can be used to enable interactions among in-vehicle sensors or other multimedia devices.

2.2.1.3 WLAN systems

IEEE 802.11 wlan systems groups a family of technology standards and drafts that implement and manage wireless local area networks. The used spectrum usually revolves around the 2.4 and 5 GHz spectrum. At the physical (PHY) and medium access control (MAC) layers, the 802.11p technology for wireless communications while in a vehicular environment has been proposed by the IEEE. The 802.11p works in the 5.9 GHz frequency band, and employs Orthogonal Frequency Division Multiplexing (OFDM) modulation. The Wireless Access in Vehicular Environments (WAVE) standards, namely 1609.4-2010 and 1609.3-2010, define the medium-access channel capabilities for multi-channel operation, and the management and data delivery services between WAVE devices. WAVE frequency spectrum is divided into 1 control channel (CCH) and 6 service channels (SCH), each with 10MHz bandwidth. In addition, each channel has a set of access categories and its own instance of the 802.11p MAC layer. Among the different types of frames that can be exchanged in WAVE, management frames can be transmitted in both CCH or SCH. However one limitation for the radio is being able to exchange information in one single channel at all times; therefore, a single-PHY has to continuously switch between CCH and SCHs every certain time (the default is 50ms). The latter indicates the radio is able to monitor the CCH while at the same time it can exchange data in one or more SCHs.

Usually, the vehicular networking uses case are not built around one wireless technology but rather a mix that fits one or more use cases. For example, when it comes to information and entertainment and other passenger-related applications, WLAN and cellular technologies are preferred. For other sensors and more in-vehicle communications, depending on the real-time and the security requirements, Bluetooth or Zigbee might be preferred.

2.2.2 Applications and requirements

IVC is attracting considerable attention from the research community and the automotive industry, for its potential in providing ITS as well as drivers and passengers services. In this context, VANETs are emerging as a class of wireless network, formed between moving vehicles equipped with wireless interfaces (cellular and WiFi) employing short-range to medium-range communication systems. A VANET is a form of mobile ad-hoc network that provides IVC among nearby vehicles and may involve the use of a nearby fixed equipment on the roadside [84].

The deployment of IP-based services including infotainment and commercial applications is believed to accelerate the market penetration of those deployments and leverage the costs of the infrastructure required by IVC.The support of IP-based traffic comes through the integration of IPv6 as well as transport protocols such as TCP and UDP in the above mentioned standards. With regards to these technology enablers, new business opportunities are offered by vehicular networks for car manufacturers, automotive OEMs, network operators and service providers. The use of IP in a heterogeneous context (very common to IVC) has the ability to make the design of E2E protocols easier [127].

Figure 2.22: Intelligent Transportation Systems. A different set of radio transmission technologies and standard communication protocols makes the Inter-Vehicle Communication a possibility. The main goal to achieve is to improve safety on-roads and help saving lives. ©European Telecommunication Standards Institute 2008. Further use, modification, redistribution is strictly prohibited. ETSI standards are available from http://pda.etsi.org/pda/.

Several applications can be proposed in the context of IVC and can be classified as time-critical safety-oriented applications or Internet-based services for entertainment or more [127].

2.2.2.1 Road safety and traffic efficiency applications

Active road safety applications' objective is to lower the probability of traffic hazards and help saving lives. A significant percentage of accidents that occur every year in all parts of the world are associated with intersection, head, rear-end and lateral vehicle collisions. Active road safety

applications primarily provide information and assistance to drivers to avoid such collisions with other vehicles. This can be accomplished by sharing information between vehicles and road side units which is then used to predict collisions. Such information can represent vehicle position, intersection position, speed and distance heading. Moreover, information exchange between the vehicles and the road side units is used to locate hazardous locations on roads, such as slippery sections or potholes. For example, intersection collision warnings, lane change assistance, head on collision warning, emergency vehicle warning, and pre-crash Sensing/Warning are all useful applications that can help meet those objectives.

2.2.2.2 Infotainment applications

Information and entertainment applications can be very different: tolling, point-of-interest notifications, fuel consumption management, podcasting, and multihop wireless Internet access, to mention a few. Due to this diversity, it is difficult to design a one-fits-all solution space that handles all of that diversity. Specific requirements analysis must be performed on a use case scenario basis. Vehicles are only a few hops away from the infrastructure (WiFi, cellular, satellite). Protocol and application design must account for easy access to the Internet during normal operation. In the meantime, applications such as peer to peer content sharing applications that can still operate with intermittent connectivity and sporadic vehicular traffic and connectivity do exist though. Vehicular networks are also emerging as important sensor platforms, for example for proactive urban monitoring. Each vehicle can sense one or more events (e.g., imaging from streets and detecting toxic chemicals), process sensed data (e.g., recognizing license plates), and route messages to other vehicles or to the infrastructure when available. Vehicles can generate much larger volumes of data than traditional sensor networks. They can also store the data and report it in bulks.

2.2.3 Vehicle-to-Internet communication

Among the use cases and application mentioned above, some of them require Internet access and mobility supporting protocols. Notification services, peer-to-peer applications, upload/download services, navigation services, and multimedia applications are all good examples of such applications. In some use cases, a pre-defined address belonging to the application domain is registered to the service provider. The service provider sends the updates to this address which does not change while the vehicle changes point of attachment.

Some services, through the mobility management solutions anchored at vehicle service providers, can benefit from session continuity (or resuming) after a loss of connectivity. Further uses of IP-based services can allow vehicles to be monitored from car manufacturers, car garages and other trusted parties to remotely check vehicle statistics and diagnose it with proper repair in case of a problem. Such services could deploy NEMO Home Agents and application servers to serve thousands of cars [**ehicular-networks-techniques-standards-applications-9**].

2.2.3.1 Mobility management in IP-based infrastructures

The mobility concept is tackled from different perspectives in the literature and gained more importance with ubiquitous wireless computing advent [101]. State of the art approaches considered the problem as being a consequence of protocol stack mis-specification and addressed the issue with proposals at different layers [63] of the Open System Interconnection (OSI) model [200]. We can roughly classify mobility management approaches as *network-based* or *host-based* given the necessary changes to be applied to the network and/or the host.

Table 2.2: Applications requirements

Application	**Communication model**	**Critical latency**
Overtaking vehicle warning	Broadcast	$< 100ms$
Collision warning	Broadcast	$< 100ms$
Emergency vehicles	Broadcast	$< 100ms$
Speed limit notification	Unicast	Not critical
Tolling	Unicast full duplex	$< 200ms$
Adaptive cruise control	Cooperative	$< 100ms$
Point of interest sharing	Cooperative, Broadcast or Unicast (Internet)	$< 500ms$
Multimedia	Cooperative, Broadcast or Unicast (Internet)	$< 500ms$
Fleet management	Broadcast or Unicast (Internet)	$< 500ms$

Network-based mobility architecture approaches can generally be broken down to well-known functional elements: Location update service (involving distributed database), Forwarding agents (or Rendez-vous points, depending on the mobility model) and location/address translation functionality. Some of these functionalities may be co-located in the same agents, or well distinguished depending on the goals to achieve [22].

Host-based mobility on the other hand, aims at an end-to-end redesign of the Internet Protocol suite to include mobility. This aspect which is a severe shortcoming of the original protocol was added through indirection in Mobile IP and related approaches [63]. One argument in this approach is the ill-definition of the layering system, and in particular the void between transport and network layers. For instance, some proposals that tackle this limitation extend the reference layering model (TCP/IP and OSI) and define an identity layer [52].

The Internet Engineering Task Force (IETF) standard to enhance mobility considered the mobility problem as being an *address translation* issue best handled at network layer [22]. The proposal considered the use of the same (and only) common namespace (IP addresses) in two different roles. On the one hand, home address is the IP address acting as an identifier associated with the node and topologically correct only on its home network. On the other hand, a dynamically attributed IP address at the current Point of Attachment (PoA) [187] defines the actual location of the node. In other words, the same object derived from the universal IP namespace is used as a name (identifier) and PoA address (locator) in different contexts. This use of the IP namespace for mobility, multihoming, and traffic engineering is at the heart of

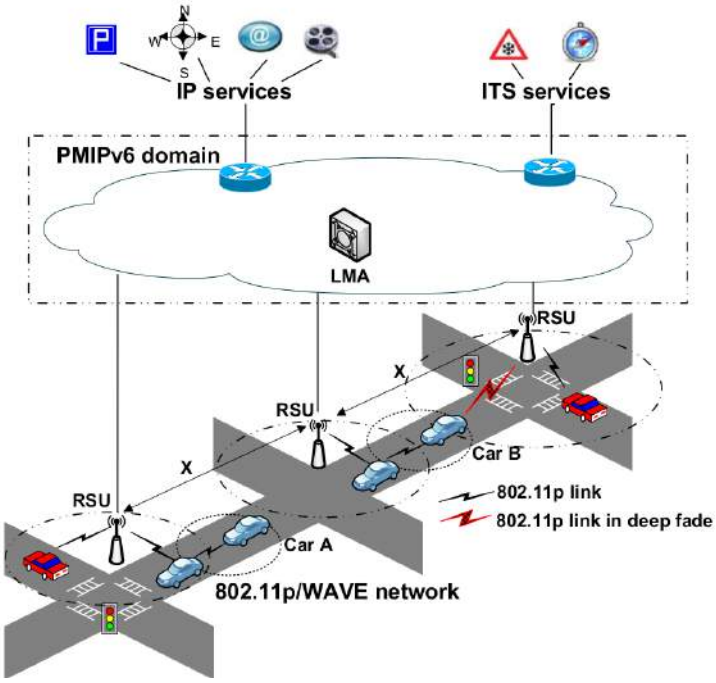


Figure 2.23: IP-enabled vehicular communications with mobility management in the infrastructure through PMIPv6.

the IP semantic overload problem to initial lack of networking objects (IP addresses and DNS names) in order to address unattended communication scenarios [179] [48].

2.2.3.2 IPv6 in vehicular networking

Vehicular networks evolved from their simple dedicated-purpose command and control applications, towards continuously evolving multi-purpose mobile networks. ITS are envisioned to play a significant role in the future Internet, making transportation safer and more efficient. With respect to these expectations, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) interactions have evolved to include various types of applications, safety-related and user-oriented.

The impact of Internet-based vehicular services (infotainment) are quickly spreading and developing. Some of these application, such as driver assistance services or traffic reports have been there for a while. But market-enabling and innovative applications may also be an argument in favor of a more convenient and pleasant traveling experience. Such use cases are viewed as a motivation to further adoption of the ITS standards developed within IEEE, ETSI, and ISO.

2.2.4 Vehicle-to-Internet communications

The potential of vehicle-to-Internet architecture as defined by SDOs is promising. Vehicular to Internet access and communications will allow for IP-based services to drivers and passengers. However, some technical challenges are of paramount importance in this matter: Managing the scalability of IP-services, IPv6 address (auto)configuration and mobility management of addresses and embedded networks.

These challenges affect the service quality and continuity which are part of the IP-based applications quality-of-experience. This implies, with regards to the vehicular networks specific characteristics, a carriage of a stable IP addressing which is configured automatically and in

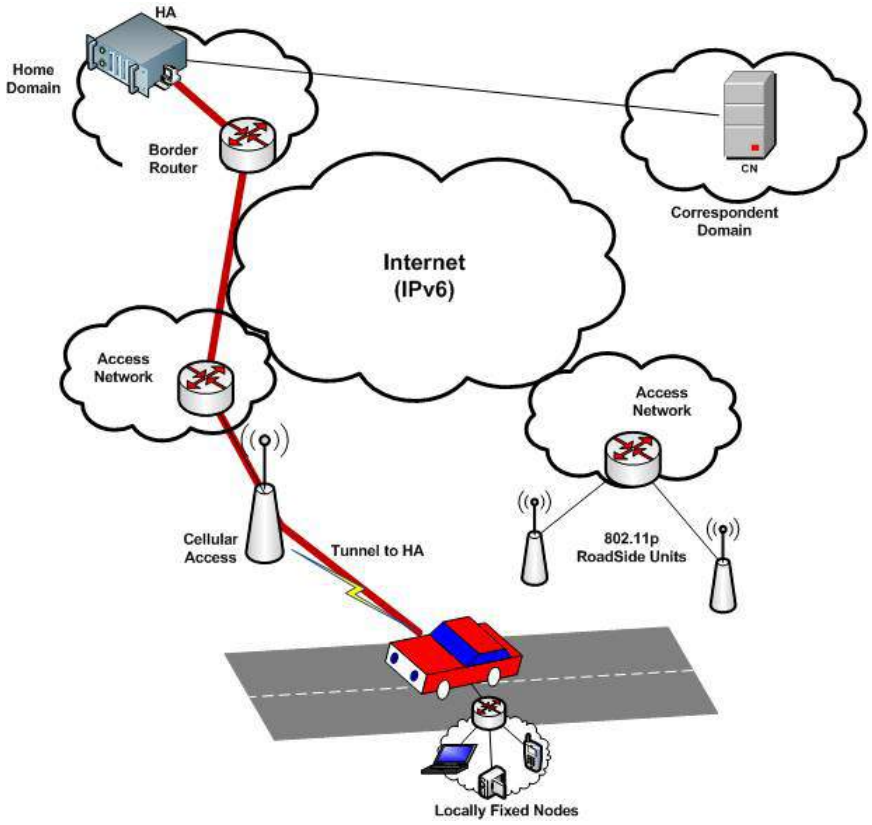


Figure 2.24: Network mobility management in vehicular networks. Using Mobile IPv6 with its extension Network Mobility (NEMO), a vehicular embedded network is globally reachable through its home addressing.

a distributed manner. From a standardization point of view, there is no main and definitive standard IP auto-configuration method specific to ad hoc networks, and hence the problem is still posed in terms of vehicular networking [84].

In the Future Internet context, the evolutions that IPv6 need to undergo for a better vehicular IP-based services support must follow the current Future Internet approaches [168]. Indeed, the recommendations for Identifier/Locator split must be included in Future Vehicular Internet architecture design. The objective is the support of mobile vehicle-to-Internet communications in a scalable manner.

Auto-configuration is the subject of considerable work in progress by a number of standardization bodies aiming to resolve this problem. We can mention IETF's efforts through the Autoconf, Netext and V6ops Working Groups, and with recent initiatives such as ITS and Geonet, that aims at developing IPv6 solutions for ad hoc networks including vehicular network scenarios. Other SDOs include international committees defining architectures for vehicular communication have included a native IPv6 stack in their protocol stacks, namely, IEEE 1609, ISO TC 204 (CALM), C2C-CC, and the newly formed ETSI TC ITS (cf. Figure 2.25).

2.2.5 Standards landscape

In order to deploy ITS services, wireless communication standards for IVC have been delivered by various standardization bodies depending on the country [90] [150]. Specialized vehicular communication systems have a DSRC spectrum reserved which allows Standard Development

Bodies (SDOs) to specify proper communications and interactions for IVC. Table 2.3 defines the frequency bands used by DSRC services in North America, Europe, and Japan respectively. SDOs also define communication stacks proper for IVC protocols and applications. Figure 2.25 compare the SDOs' protocol stacks specifications [132].

Table 2.3: DSRC spectrum by country.

North America [176]	Europe [198]	Japan [147]
Around 5.9 GHz (5.850-5.925 GHz)	5.795-5.815, 5.855-5.875, 5.905-5.925 GHz	5.770-5.850 GHz

IEEE standardized 802.11p as the WLAN technology for IVC within the working group IEEE 1609. One of the outcomes of the IEEE 1609 suite of Wireless Access in Vehicular Environments (WAVE) is the reference protocol stack illustrated in Figure 2.26(a). The reference system includes the support for safety and non-safety (infotainment) applications. The support of IPv6 networking is mandatory within IEEE WAVE. The specification [109] describes the configuration process and the transport protocols to be supported (legacy IETF TCP and UDP). Supported communication scopes are link-local, multicast, and global. With regards to the IETF RFC 2460 defining the global IPv6 address configuration procedure through neighbor discovery protocol, IEEE WAVE brings a major distinction by providing the Router Advertisement through a WMSP message (WSA). This is to address the issue of quick topology changes, proper to vehicular context [31].

Support for IPv6 in ETSI is specified in the document ETSI EN 302 665 (2009) along with the reference architecture illustrated in Figure 2.26(c). Networking (auto-configurable addressing, routing, and reachability) and mobility support of IPv6 are specified within IETF. In addition to IPv6 routing, ETSI defines GeoNetworking for safety messages transmission in a local geographic area surrounding the vehicle. Additional communication scopes are defined for GeoNetworking (inspired by IPv6) such as GeoMulticast, GeoBroadcast, GeoAnycast and GeoUnicast.

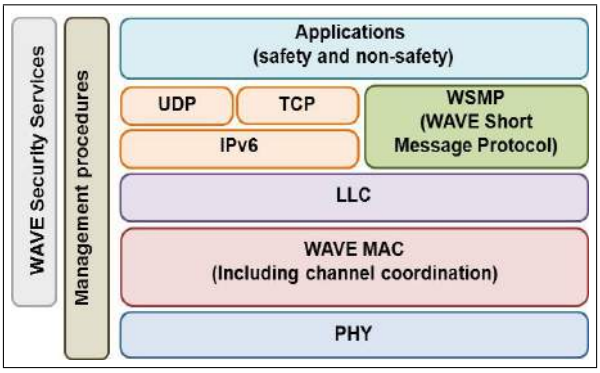
Car to Car Communication Consortium (C2C-CC) aims at establishing an open European industry standard, focused on development of active safety applications. The C2C-CC is supported by European automobile industry. For the networking part, C2C-CC specifies C2CNet protocol to support safety and non-safety applications, jointly with the support of IPv6. In particular, one can notice that support for safety applications through TCP/IPv6 is available, as well as multi-hop communications over vehicles and infrastructures (Figure 2.26(b)).

ISO 21210:2010 [111] is the ISO standard defining IPv6 usage for ITS. It specifies IPv6 network protocols and services necessary to support global reachability of ITS stations, seamless mobility and IPv6 Internet connectivity. In particular, this specification describes IPv6 support for vehicles and infrastructures (Figure 2.26(d)). In particular, this specification defines specific IPv6 signaling, addressing, routing, mobility and multi-homing support.

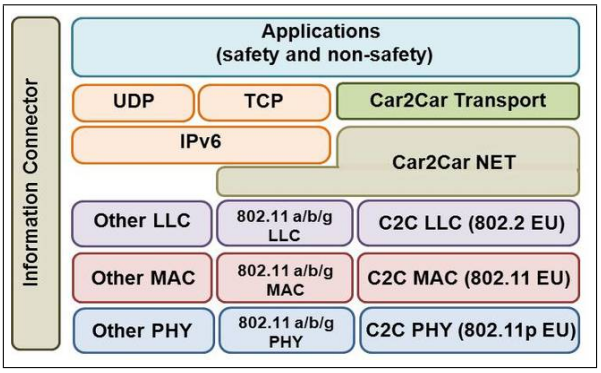
2.3 Conclusion

During the last years, the Internet growth combined with factors including mobility, multihoming and interdomain traffic engineering has lead to a huge growth of the BGP routing tables and an increase of the BGP churn. To cope with this problem, the Internet Architecture Board proposed

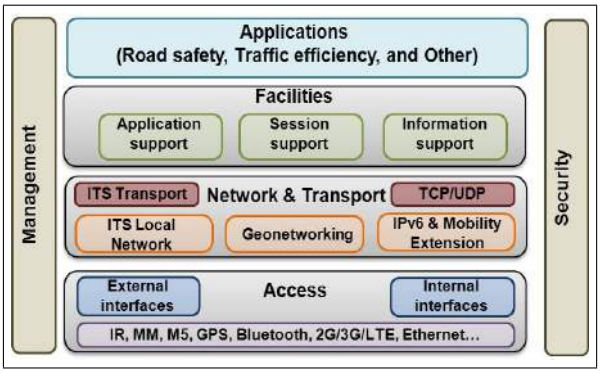
Figure 2.25: IPv6 networking support through different SDO protocol stacks



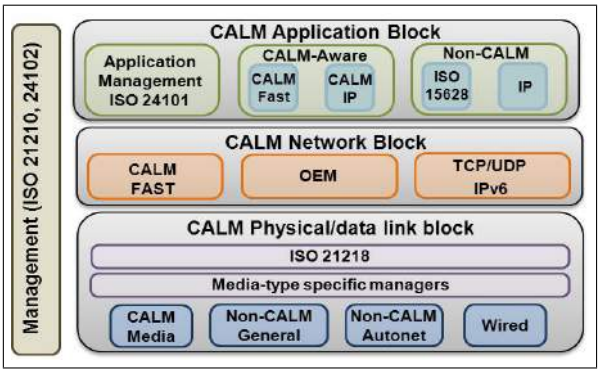
(a) IEEE WAVE/DSRC communication protocols stack. Networking services supports the use of the Internet Protocol IPv6 (IETF RFC 2460) and supports transport protocols such as UDP (IETF RFC 768) and TCP (IETF RFC 793)



(b) C2C-CC reference communication protocols stack. Safety applications can use C2C-CC transport and network layer or another standard if necessary. Infotainment IP-based services are supported through TCP/IP and can access wireless multi-hop communications with vehicles or infrastructures



(c) ETSI ITS reference communication protocols stack. Different possible networking modes are identified for ITS, such as GeoNetworking protocol, IPv6 networking with mobility support (IETF RFC 6275), IPv6 over GeoNetworking and more



(d) ISO TC204 CALM reference communication protocols stack. CALM includes IPv6 at the networking layer defined at the IETF. It is also possible to use non-IP (mainly safety) applications. Support for ad-hoc communications is also included in the CALM-FAST mode

a new design that assumes two different types of addresses: identifiers and locators. An identifier is used on an host to identify a connection endpoint while a locator refers to a node attachment point in the Internet topology. Note that, in today's Internet, an host address is at the same time its identifier and its locator. The proposals are divided in two categories: those attaching locators directly to hosts (HIP, SHIM6, or ILNP) and those attaching locators to routers (LISP). Mapping system allows to map an identifier onto a set of locators in order to reach this identifier as a new address translation phase in the network. A key advantage of the addresses separation is to offer the possibility of associating several locators to a given identifier and handle the growth of routing systems through efficient mapping systems designs. Traffic engineering has also became one major benefit from using these approaches for network operators. Among the Internet mobile users, the vehicles are a growing community with huge numbers that can affect the sustainability and the scalability of Internet architecture if not handled properly. Through various IP-based services, vehicle-to-Internet communications contribute to the scalability problem expressed by network operators. However, this can also be an opportunity for car manufacturers to become

actors in the data plane of vehicle applications and support novel innovative services. In this chapter, we presented a detailed evolution of the IP paradigm from legacy core building blocks towards recent Future Internet evolutionary and disruptive approaches. We then placed the vehicular networking as a special client of these Internet architectures to determine how the vehicular traffic may affect the Internet, as the mobile users did during the last decade.

Chapter 3

Use cases: IP-based services for Vehicle-to-Internet communications

Vehicular networking serves as a technology enabler for various multi-purpose IP-based mobile applications to fully integrate the vision of the future Internet diversity [183]. Intelligent Transportation Systems (ITSs) [67] are envisioned to play a significant role in the future, making transportation safer and more efficient. With respect to these expectations, Vehicle-to-Internet interactions have evolved to include various types of applications, safety-related and user-oriented.

Towards Future Internet

After successfully connecting computers (Internet Protocol) and later people (World Wide Web), enabling an Internet of Things is one of the great challenges of the Future Internet. According to some estimates, the size of the Internet doubles every 5.32 years, which will lead to an average of 6.58 connected devices per person by 2020 [69]. These 50 billion things [180] connected to the Internet in order to gather information for various and unattended applications that support new markets [101] will create a heavy and dense traffic on the core network. On the other hand, these new and exciting possibilities come with the requirement of a larger addressing space. The IPv4 addressing pool already exhausted [8], the transition to IPv6 with its huge numbering space (2^{96} times bigger than IPv4's) is urgent [112].

IPv6 in vehicular networks

V2I and V2V settings include several examples of eSafety and infotainment applications support. These applications can be roughly classified in two major types: safety-oriented or user-oriented (also referred to as *infotainment*) [205]. Safety applications are clearly time-critical tasks, where message delivery with short delay guarantee is the first design goal. In these use cases including eHealth and safety on road, *non-IP* communication technologies are often considered for their reliability [197]. In contrast, non-time-critical user-oriented applications include infotainment and other prevention on road applications. The use of IP (best effort) to extend the supported geographic area for these applications is possible [83].

The use of IPv6 in current standardization work for vehicular communications technologies guarantees a better integration in the Future Internet. For example, LTE technology supports IPv6 [1], which opens new V2I services perspective [90]. In recent ETSI activities, a geographic networking protocol combined with IPv6 stack layer has been experimented and standardized [83]. GeoBroadcasting safety messages by relaying messages through a vehicle-to-vehicle (V2V) mode in the same geographic zone using IEEE 802.11p, has also been experimented.

Remote Healthcare

eHealth can be used for patient monitoring, remote diagnostics, activity monitoring, lifestyle suggestions, and personal security to enable novel patient-physician interactions. In terms of challenges, new threats regarding ethical issues such as online professional practice, informed agreement, privacy and equity are posed by the remote aspect of the technology.

eHealth scenarios often consist in a combination of sensors for individual's vital signs measurements or position tracking his in case of an emergency. These sensors come in the form of lightweight portable (or wearable) devices for enhanced user acceptability. State of the art remote monitoring is achieved in two phases by combining short range communications (Personal Area Network - PAN) for the sensors and General Packet Radio Service (GPRS) access on another device.

Most eHealth applications occur in urban operational environments. Remote management includes cases in which health practitioner intervention is required. There is necessity for high reliability due to sensitive nature of data. eHealth scenario considers event-triggered connections having benefits on network signaling and scheduling. eHealth applications may use mesh routing with multi-hop connectivity. High mobility is expected because of moving objects/persons tracking.

Fully Electric Vehicles (FEVs)

Recent advances in the field of hybrid, plug-in electric, and fully electric vehicles are driving automotive and other related industries to a new revolutionary era of mobility. With the advent of electric mobility, new economic and research challenges arise for car manufacturers, utility companies, car sharing ventures, policy makers, and smart city architects [141] [212]. Basically, the growing interest in FEVs shed the light on the importance of route planning, street connectivity, and charging station placement [80]. These challenges can be faced from various perspectives, and different proposals relating to data mining [58], simulation [141], network connectivity [157] and system integration [80] may help solving the issues of large scale deployments.

In order to simplify the usage of FEV and *secure the driver's itinerary*, it is necessary to ensure optimal scheduling for charging stations (booking and charging) [157]. In such a scenario, interactions involving charging infrastructure (grid operators), road IT infrastructure and fleet management operators may occur while the FEV is moving. In particular, the FEV needs to rely on a communication network that delivers real-time status (itinerary, battery state, traffic) to the infrastructure, which provides assistance services to the FEV, such as the selection and booking of a suitable charging station [80]. In this context, the FEV may be provided with several heterogeneous network access technologies such as WLAN, UMTS/LTE, or PLC. These interfaces need to be configured properly to fit in the above mentioned use cases; in particular, to maintain seamless connectivity with as little disruption to the ongoing services as possible, when moving along different network attachment points [196].

Heterogeneous networks

IoT is about small devices (including eHealth's) limited in terms of computing and networking capabilities. Several short and long range transmission technologies might be used at this level (Figure 3.1) with optimizations that allow for lower power consumption [25]. Short range communication technologies, such as Radio Frequency Identification (RFID), Bluetooth, or IEEE 802.15.4 standard are much more common than long range communication technologies

(3G, LTE or WiMax). Therefore, an additional functional element, the gateway (GW), translates between both short and long range communication technologies and helps expending the boundaries of the current Internet. From an addressing perspective, these gateways are called Address Translation Gateways [152] due to their dual addressing function (IP and IEEE 802.15.4 in 6LoWPAN, for instance).

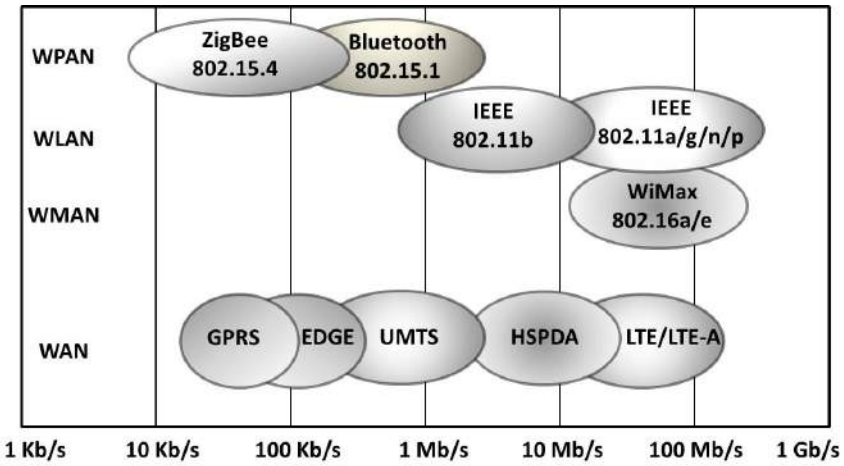


Figure 3.1: Radio transmission technologies that apply to IoT and vehicle-to-Internet use cases [43].

This section describes the technical challenges of two specific vehicle-to-Internet use cases: eHealth and FEV services. In particular, we review the characteristics of both use cases and determine their common technical requirements for in-vehicle IP-based services. We also detail their similarities with the IPv6 communication requirements for M2M applications. This section covers the following aspects:

- The integration scenario between vehicular networking (as an enabling platform) and eHealth technologies (as end user application).[1].
- FEV architecture for mobile traffic and journey planning[2].
- Discuss the technical requirements and needs for more IP-based services.

[1]This work has been performed in the framework of the ICT project ICT-258512 EXALTED, which is partly funded by the European Union

[2]This work was partly supported by the European Commission under the collaborative project eCo-FEV.

3.1 IPv6 communication requirements

The perspective of machine communications in the Internet of Things assumes that small and numerous devices beyond the scale of the number of currently deployed devices, communicate in an unattended manner. The nature of the communication links varies to such extent (sometimes inside the same local area) that only protocols from the Internet Protocol family can glue them all in a meaningful manner. Consequently, auto-configuration mechanisms of network parameters and default route play a role of paramount importance in building these IP networks.

3.1.1 Basic IP parameters

Several mechanisms exist for the auto-configuration of basic IP parameters (address, mask, default route) for a device. A rough classification groups them depending on their capacity to maintain a state related to the parameters assigned to a device. For example, DHCPv6 protocol [55] falls within a *stateful* group since it maintains an address assigned to a device, at a specific DHCPv6 Server. On another hand, *stateless* group does not maintain such state: a Router provides a prefix to device and the device forms an address for itself without further assistance from other entities [155].

In the case of in-vehicle embedded networks, the IP devices are deployed in a vehicle equipped with a Gateway offering long-range connectivity. In such a scenario (network of networks), auto-configuration mechanisms are needed: the Gateway needs not only one address for itself but a set of addresses for the embedded IP devices. The mechanisms to achieve such auto-configuration are named *Prefix Delegation*. This is an extension to the DHCPv6 [208] protocol of which the message exchange diagram is illustrated in figure 3.2. In addition to the typical functionality of DHCP to assign IP address, this extension allows the assignment of a set of prefixes to a Client. The DHCPv6 protocol is specified to work with Relay and Server entities as described in this recent reference [220].

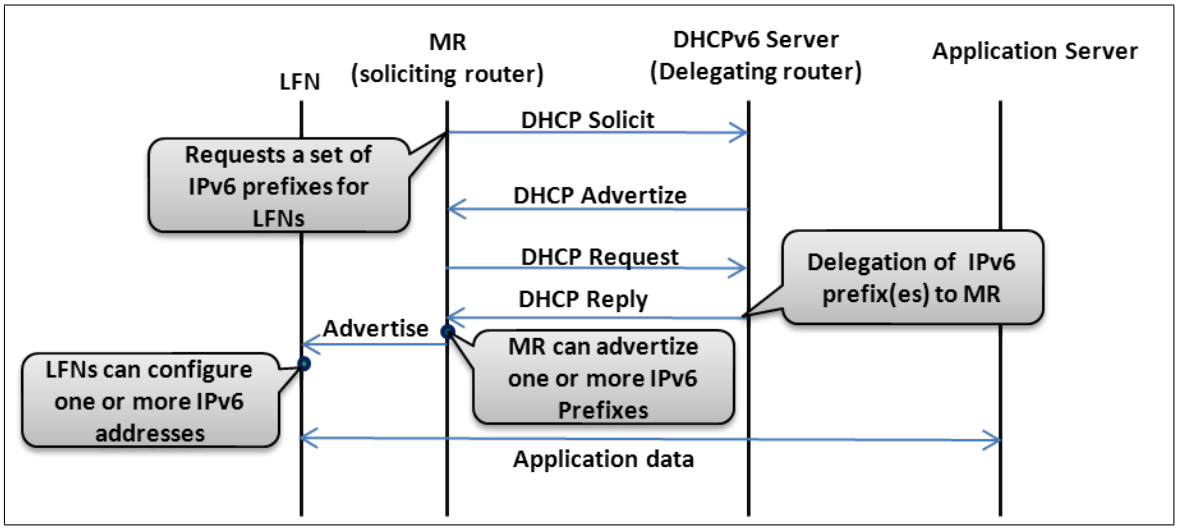


Figure 3.2: IPv6 Prefix Delegation message exchange diagram in DHCPv6 protocol.

Prefix Delegation for Network Mobility [56] is a specification of behavior for the existing DHCPv6 Prefix Delegation in the context of network mobility. Network Mobility (NEMO) is an extension of the Mobile IP protocol to support groups of devices moving together; another terminology for this group can be capillary networks. This particular prefix delegation mechanism

specifies the roles of the Requesting Router (Mobile Router) and of Delegating Router (Home Agent), as well as the placement of the DHCP Relay (Mobile Router).

3.1.2 Routing

In addition to IP addresses assignment for in-vehicle devices, routing must be set up. Configuring routes in a system comprising a huge number of devices may become a communication- and compute-intensive task. The concept of *default* route; i.e. *the route to be chosen from a routing table when no other route is matching a destination address*, provides partial resolution to this problem. Indeed, *it is sufficient for the Gateway to hold a single default route (the IP address of the next hop) instead of multiple routes towards specific destinations.*

Default route auto-configuration mechanisms exist basically under two distinct forms. The first is *RA-based* (the use of stateless address auto-configuration) and the second is a *dynamic routing protocol* such as OSPF [137]. Currently these two mechanisms are the only IETF mechanisms to assign a default route to an end node. Devices with limited CPU and memory capacities can benefit from the sole presence of a default route in their routing tables: it is sufficient to store only the default route in order to be able to reach any other node in the Internet. This is especially advantageous for machine-type communications.

Whereas stateless address auto-configuration offers a default route to an end device, it does *not* offer a set of prefixes. Similarly, the prefix delegation part of the stateful address auto-configuration does offer a set of addresses to the Gateway (in order to further deliver them to the IP eHealth devices) but does *not* offer a default route.

For a limited capacity device (a constrained vehicular Gateway, or a constrained eHealth device), it is advantageous to use a lightweight auto-configuration protocol offering both parameters:

- An IPv6 route to be used as a default route in the routing table of the Gateway.
- A set of IPv6 addresses (addresses or prefixes), to be used for address auto-configuration on the IP eHealth devices onboard the vehicle.

3.2 eHealth in ITS

In the wide field of health informatics, the special case of eHealth relates to the use of the Internet to disseminate health related information [94]. The health-related measures are captured by small and various devices and transmitted to be stored in large databases. Further process of this data helps to support diagnostics. The overall objective is to improve efficiency and save lives [166]. The eHealth protocol messages carry sensitive data and require integrity, confidentiality and availability. Privacy is one of these security issues and is usually addressed by proposing pseudonymization of medical data [194].

3.2.1 Related work

WEHealth [218] provides eHealth service for medical needs on roads and enhances security and privacy by the use of the NOTICE framework (a secure and privacy-aware architecture for the notification of traffic incidents). This infrastructure includes short-range communication capable sensor belts placed along the road. The infrastructure in NOTICE uses embedded sensor belts in the road at regular intervals (e.g., every mile or so). Each belt is composed of a collection of pressure sensors and a few small transceivers. The pressure sensors in each belt allow every message to be associated with a physical vehicle passing over the belt, eliminating the need to

uniquely identify vehicles in order to interact with them. The sensor belts do not communicate with each other directly and rely on passing cars to carry and forward a message between adjacent belts. Check station belts are authentication centers and pseudonyming proxies. They are placed on the roadside and attached to Base Stations to access the Personal Health Record (PHR) server in the Internet. Medical queries or accident alarms can be disseminated through the system to provide health records of the patients. In addition to wireless communications with external sensor nodes on the road, WEHealth platform assumes an underlying IPv4 Internet and the server side (PHR server) is accessible through Base transceivers.

eCall [116] is a recent European standard that brings the possibility of dialing the EU emergency number (112) in case of a serious road accident automatically without vehicle occupants' intervention. The European Commission adopted measures to ensure eCall will be available in new car models from 2015. Due to typical eSafety applications stringent delay requirements, eCall is to operate only on radio networks (24GHz). This chapter focuses on services that involve non-time-critical eHealth applications, therefore recorded data can be transported over IP (best-effort).

The ongoing FUI-14 project "AmbuCom" [7] set as a goal to equip about 1000 ambulance vehicles per year with advanced communicating tools that would transfer patient medical information to control rooms. The communicating ambulance would then be a key part of the emergency decision-making process and improve the information exchange between the field operators and regulating doctors. In terms of communication technologies, the vehicle is equipped with a mobile router called *universal communication box* connected to the embedded and wireless medical devices. The patient's vital signs are recorded using the eHealth devices and transferred to the operational management center via one of the ambulance's radio-communication means (among which LTE). It is not clear if the devices will communicate in an end-to-end fashion with the operational center servers and remain directly reachable or use an application level (proxy) gateway that sends the health-related data on their behalf (aggregation).

Monitoring and dealing with a large number of casualties is an important key parameter to disaster response scenarios. The CodeBlue platform [140] provides a protocol and a software framework integrating eHealth devices such as wearable vital sign sensors, handheld computers, and location-tracking tags to handle disaster response and emergency care scenarios. The prototype proposes to integrate device discovery, robust routing, traffic prioritization, security, and RF-based location tracking. In a disaster scenario, handheld computers carried by first responders receive and visualize multiple patients vital signs on the implemented application. Based on these observations, triage operation can help optimizing the chances of survival. Along with these objectives, security and privacy are studied according to legal ramifications specific to the USA regulations. We do not focus here on extreme disaster scenarios and consider a more general use case. In addition, IPv6-based protocols and extensions are used.

In a recent European project (IIP) [79], one of the priorities was to create a reliable, stable and universal implementation of IPv6 network services, including DHCPv6, DNS and mobility management mechanism as well as applications, including VoIP and IPTV. With respect to these objectives, one target concerns eHealth. By deploying wireless medical sensor technologies over IPv6 to enhance connectivity and security, delivering healthcare services remotely will be possible. One of the objectives is the removal of NAT, to allow easy access for service or/and devices and perform remote configuration and maintenance which is an important issue for the elderly and disabled persons living alone. This chapter also describes the use of IPv6 but considers a vehicular setting for the deployment.

3.2.2 eHealth scenario overview

We present our eHealth platform embedded in a vehicular setting that integrates IP-based eHealth devices and aims at improving the connectivity by enhancing next-generation communication capabilities. We describe the system architecture during the integration phase of the vehicular and eHealth testbeds. The hardware specifications and the testbed are further detailed in the implementation section.

Figure 3.3 depicts the overall system architecture of the integrated testbed. The system includes 4 functional elements and 2 types of interactions (short and long-range). The eHealth devices supported by this platform, namely Electrocardiograph (ECG), Spirometer, Oximeter and Blood Glucose meter send health-related measurements over Bluetooth to an IPv6-ready phone application. This cluster head (phone) is attached to an IPv6 Mobile Router (second part of the testbed) connected to the infrastructure. The phone sends these measurements after user review, to an application server in the IPv6 Internet. The gathered data is viewed remotely by the user's physician on his/her personal terminal. From left to right, these elements are:

- **The eHealth Device** provides real time health-related measurements. These measurements can be of different nature such as blood glucose levels or oxygen saturation levels. These M2M devices are provided with Bluetooth technology to send recorded data to another authorized peer.

- **The Application Phone** is in the middle of two different communication technologies. On the one hand, short-range Bluetooth technology to communicate with M2M Devices and capture the eHealth data and on the other hand, short-range WiFi technology to send secure IPv6 packets to the server via the Gateway. The phone allows to process the gathered data before sending it to the server along with user comments, which is not possible with a standalone gateway.

- **The Mobile Router (MR)** provides IPv6 connectivity to in-vehicle devices and a default-route towards the server in the Internet. The gateway uses WiFi to advertise internal IPv6 prefix to the attached nodes. For the long-range communication technology (path towards the server), only LTE provides full IPv6 path from end to end. For testbed purposes, we demonstrate the concept over Ethernet (IEEE 802.3). The MR has a powerful CPU and provides some resources demanding networking applications, not available to run on a limited battery power device like a smartphone.

- **The Application Server** collects the data from patients and provides a web interface for doctors to support diagnostic. The software running on the server includes a web server accessed over a secure connection (SSL) and a limited-access database server to gather the data by patients. A Java Applet is required to view ECG graphs on the doctor screen.

Vehicular networking and eHealth technologies are combined (Figure 3.4) in the form of an ambulance equipped with special telemedicine devices that can record as well as transmit the patient's vital signs (body temperature, pulse rate, respiration rate, blood pressure) and critical physiological parameters (ECG, blood glucose levels, oxygen saturation levels) to the nearest hospital in order for the resident health professionals to optimally prepare the patient's admittance. This typical V2I scenario can be enhanced through IPv6 connectivity.

Assuming a road accident where a serious trauma should be taken into consideration, the ambulance crew has in its disposition a set of handheld lightweight devices that can transfer emergency data to the hospital. The objective in such a situation is to maximize clinical value through a limited set of measurements. All involved devices communicate via Bluetooth to

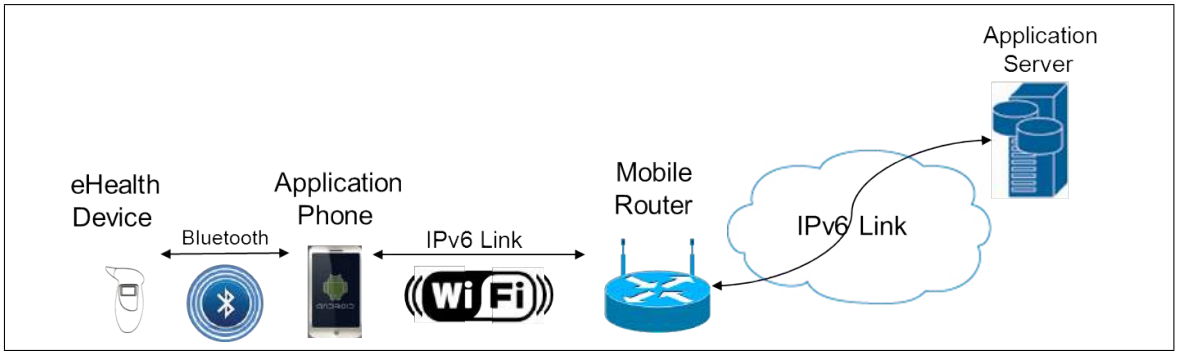


Figure 3.3: System General Architecture. First step of the testbeds integration.

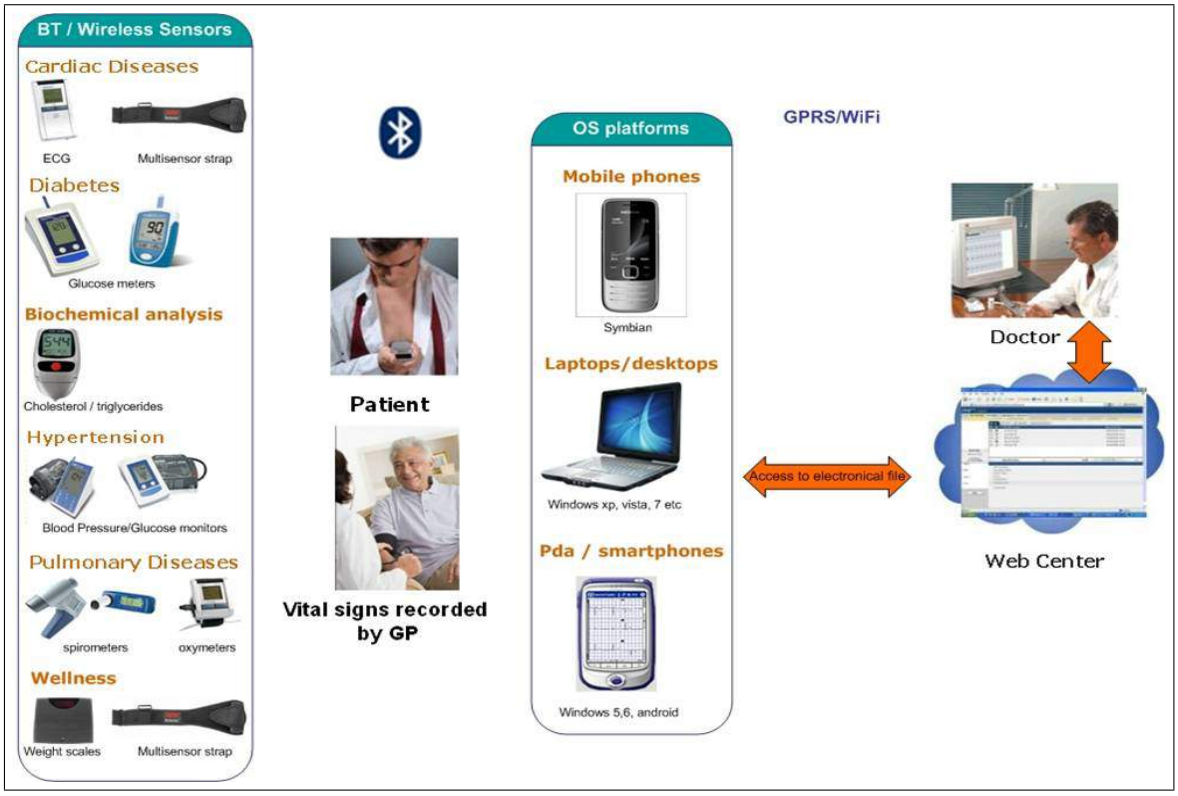


Figure 3.4: eHealth Operational Scenario. Vital signs recorded by the patient are sent to the expert for diagnosis.

an Android smartphone providing for IPv6 connectivity. This smartphone can later on be generalized to compatible ruggedized devices/tables used by the medical crew.

However in an emergency situation (natural disaster, road accidents) where numerous vehicles of different functions (ambulances, fire brigade, police cars) are involved, the scenario could differentiate in order to accommodate for the optimum data transfer to the interested parties (health care provision, law enforcement) via V2V communications. This topic is out of scope of the scenario considered here.

3.2.3 Auto-configuration Protocol

As exposed earlier, our auto-configuration protocol is lightweight and provides IP addresses to the eHealth devices as well as a default route to the Gateway deployed in the vehicle. The protocol used for configuring default routes on the gateway with DHCPv6 is illustrated in Figure 3.5. The protocol has been documented in further details in [173].

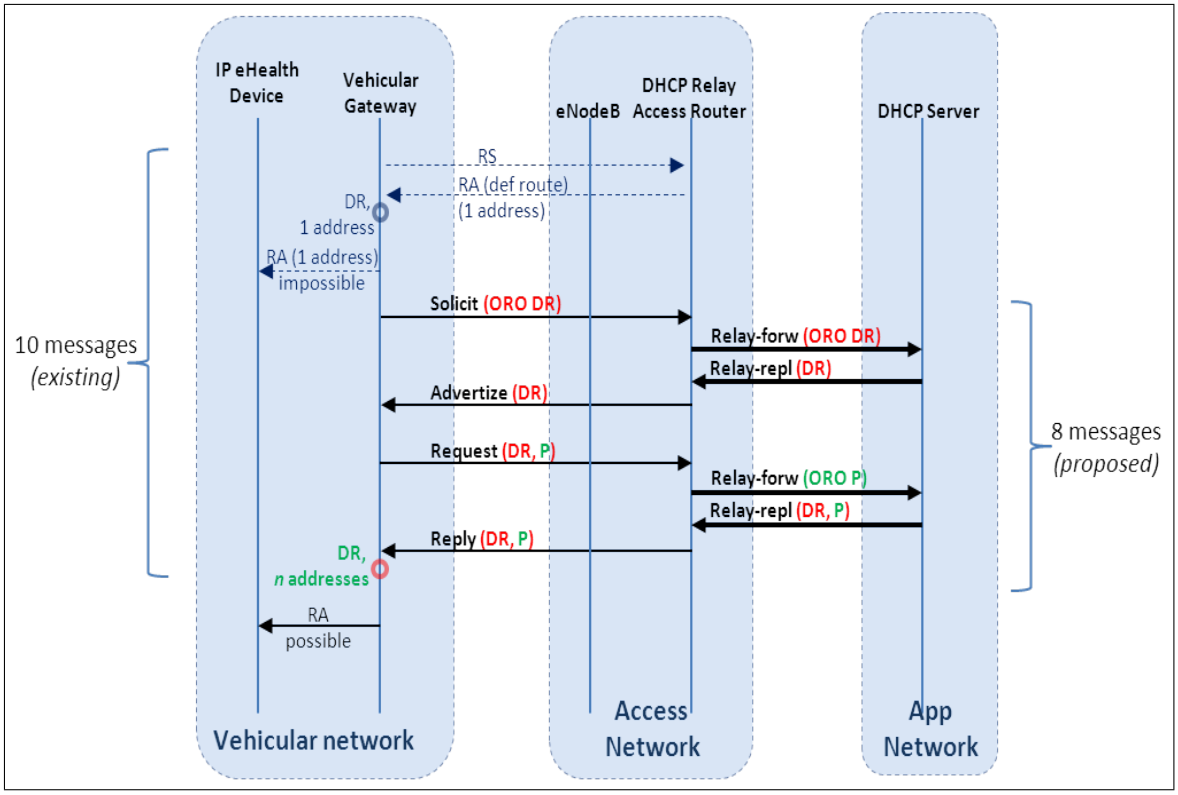


Figure 3.5: Auto-configuration Protocol Messages. A comparison of the number of messages between current auto-configuration methods and the proposed one. DR stands for Default Route, P for prefix, and ORO for Option-Request Option.

The above figure describes the extended message exchange performed by the vehicular Gateway and the DHCPv6 entities in the infrastructure. In the original DHCPv6 protocol, to obtain a set of addresses and a default route, **10 messages** are necessary (including Neighbor Discovery messages). The initial Router Solicitation (RS)/Router Advertisement (RA) offer the default route whereas the subsequent DHCP Solicit/Advertize/Request/Reply offer the set of addresses to the Gateway (to advertise for the eHealth devices).

Our proposal is based on DHCPv6 messages *only* to provide the default route in addition to the set of addresses. As depicted in Figure 3.5, the total number of messages in the earlier exchange (Gateway-Infrastructure) is *reduced from 10 to 8*. The control plane is thus optimized and the bandwidth gain depends on the quality of the link between the gateway and the infrastructure (V2I wireless link).

In our proposal a Solicit/Request packet a client lists the wanted options in the Option Request Option (ORO), composed of a list of option codes. The DHCPv6 Server answers those packets with Advertise/Reply packets containing values for the options asked by the Client.

The relay receives the message from the client and forwards it to the server in a Relay-forward message. The server replies to the relay with an advertise/reply message encapsulated

in a Relay-reply message. The content of this message is extracted by the relay and sent to the client.

In its DHCPv6 requests, the client sends a list of required options in the option request option (ORO). This option contains 3 mandatory fields: OPTION_ORO, option-len and requested-option-code, followed by new option fields.

The proposed option is named here OPTION_DEFAULT_ROUTER_LIST. It is possible to concatenate this value with several other existing requested-option-codes. The value of this code in this option is to be assigned. Obviously, this option needs to be understood by the server as well.

In the server side, the default router list option of DHCPv6 (Figure 3.6) contains: OPTION_DEFAULT_ROUTER_LIST, option-len, router-address, router-lifetime, lla_len (link-layer address length) and optionally router_link_layer_address. As this option contains a list, the pattern containing router_address, router_lifetime, lla_len and optionally router_link_layer_address can be repeated.

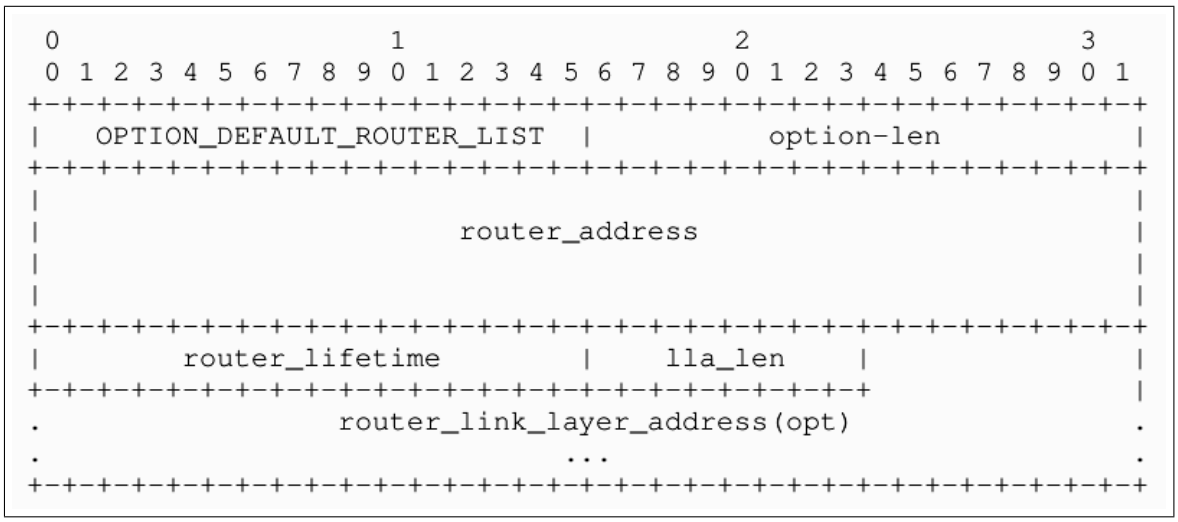


Figure 3.6: DHCPv6 default router list option fields. This option is used by the server to answer ORO option sent by the client.

3.2.4 Prototype implementation

This section describes the experimentation of testbed integration performed in the context of the FP7 EXALTED project[3] to demonstrate the capability to communicate eHealth specific data on the next-generation Internet from a vehicular setting. The underlying network communication protocols used were relying exclusively on IPv6. The application-layer protocols included, but were not limited to, HTTP and HTTPS.

3.2.4.1 Hardware specifications

The Kerlink Wirma Road (Figure 3.7) is an energy-efficient ARM926EJ-S platform provided with a 2.6.27 Linux kernel. The ARM926EJ-S processor is one of the most popular ARM processors. The MR includes some M2M services and provides several communication capabilities. An integrated chipset provides GSM/GPRS Cellular network service. An integrated WiFi module

[3]EXALTED (EXpAnding LTE for Devices), http://www.ict-exalted.eu.

provides IEEE 802.11b/g connection. An integrated GPS module provides accurate geographic coordinates. GPRS, WiFi and GPS antennas are unified in one vehicle roof antenna. In the front panel, an Ethernet Hub and Serial connections (CAN, RS 232) are present. According to the manufacturer, 10% of the regional buses company in Paris (France) are equipped with this gateway. For testbed purposes, an additional NETGEAR Access Point (AP) is plugged into the Brick with a USB-Ethernet converter. Its purpose is to ease mobile phones attachment to the network advertised by the AP (essid "EXALTED", WEP Key).

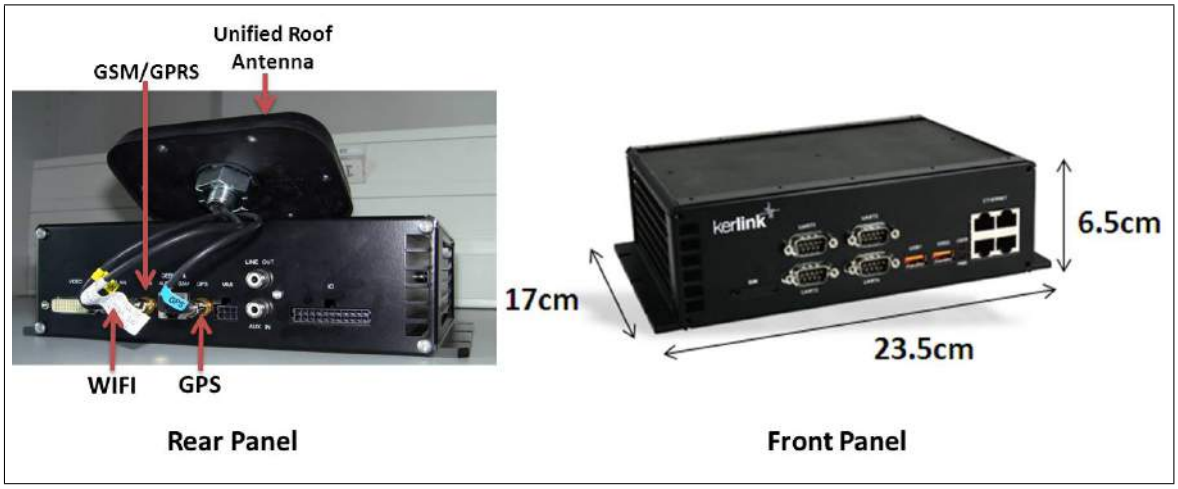


Figure 3.7: Kerlink Wirma Road Gateway.

The eHealth devices (Figure 3.8) used for the testbed are manufactured by CardGuard [29]. The oxygen saturation level is measured by OxyPro, a wireless pulse oximeter. It provides for real time measurements and can be operated in continuous mode. It also provides for pulse monitoring. It displays oxygen saturation and pulse rate averages with the absolute maximum and minimum measurements.

The blood glucose and pressure measurement is performed by Easy2Check device. Blood glucose is measured with the use of an amperometric biosensor where fresh capillary blood is deposited. Its accuracy ranges from ±15mg/dL when glucose <75mg/dL to ±20% when glucose >75mg/dL. Accordingly for the pressure measurements the accuracy is ±3mmHg or ±2% of reading.

Self-check ECG offers 1 to 12 leads ECG events monitoring. It is intended for monitoring symptoms that may suggest abnormal heart function: skipped beats, palpitations, racing heart, irregular pulse, faintness, lightheadedness, or a history of arrhythmia. The recording period is set at 32 seconds while the bandwidth is 0.05 - 35 Hz for the 12 Leads and 0.4 - 35 Hz for the 1 Lead.

Spiro Pro is a spirometer that records Volume (Time and Volume) Flow curves according to international performance standards. It measures lung ventilatory functions during Forced Vital Capacity (FVC) tests. The recording lasts for 17 seconds and its accuracy for the FVC and FEV 1 is +5% or +0.1L. It is mostly used for asthma or COPD monitoring.

A medical application is installed on an Android smartphone (IPv6-capable) which receives the vital signs from the portable monitoring devices via Bluetooth. The recorded data from the devices are transferred automatically (in the absence of the Mobile Router) through the smartphone via GPRS, Ethernet or WiFi to a designated web center (over IPv4). The application provides a simple Electronic Health Record (EHR) for disease management and treatment and initiates patients' active involvement in healthcare. Analytically, it features browsing on the

Figure 3.8: Vidavo eHealth Devices.

exams history, viewing of the recorded data, downloading of a diagnosis or advice from a doctor, comments addition and more. The final destination of these data is the EHR of the patient who uses the devices and it is resident in a dedicated server from where it is accessible for reviewing under secure credentials by the treating physicians.

3.2.4.2 Platform Integration

Although the experimentation was performed in a laboratory setting, the hardware equipment is deployable in a vehicle as is: Kerlink's Wirma Road (IPv6 Gateway) is a low-consumption PC platform dedicated to vehicles, whereas eHealth devices are used by professionals of health periodic check-up and continuous monitoring. The kernel support of IPv6 and its associated extensions has been implemented in the gateway during the first phase of the testbed integration. The overall architecture is summarized in Figure 3.9. In the joint testbed, the MR runs Router ADVertisement Daemon (radvd), version 1.8.5 compiled for ARM platforms and available for Debian distributions [171].

The radvd is configured to advertise at regular intervals or immediately on solicitations, two different prefixes for two different interfaces. On the Air Interface (AP), which is bridged to the MR, the 2001:DB8:B:2::/64 prefix is advertised for the devices which connect to the "EXALTED" essid. This is the Ingress Interface of the Brick. On the Ethernet side, the 2001:DB8:A:1::/64 prefix is announced for the connected devices. This is the Egress Interface of the Brick. The server is connected on this side of the Brick, and the traffic is routed through the gateway from one end to the other. These devices form the basis of what will be deployed in a vehicle such as an ambulance.

As illustrated in Figure 3.9, on the vehicle side (ingress interface) two smartphones are used. (1) Samsung Galaxy 3 which runs Android 2.2 system. This phone is peered with the ECG and Spirometer devices over Bluetooth. (2) HTC Hero which runs Android 2.3 system. This phone is peered with the Glucometer and the oximeter over Bluetooth as well. Both phones are

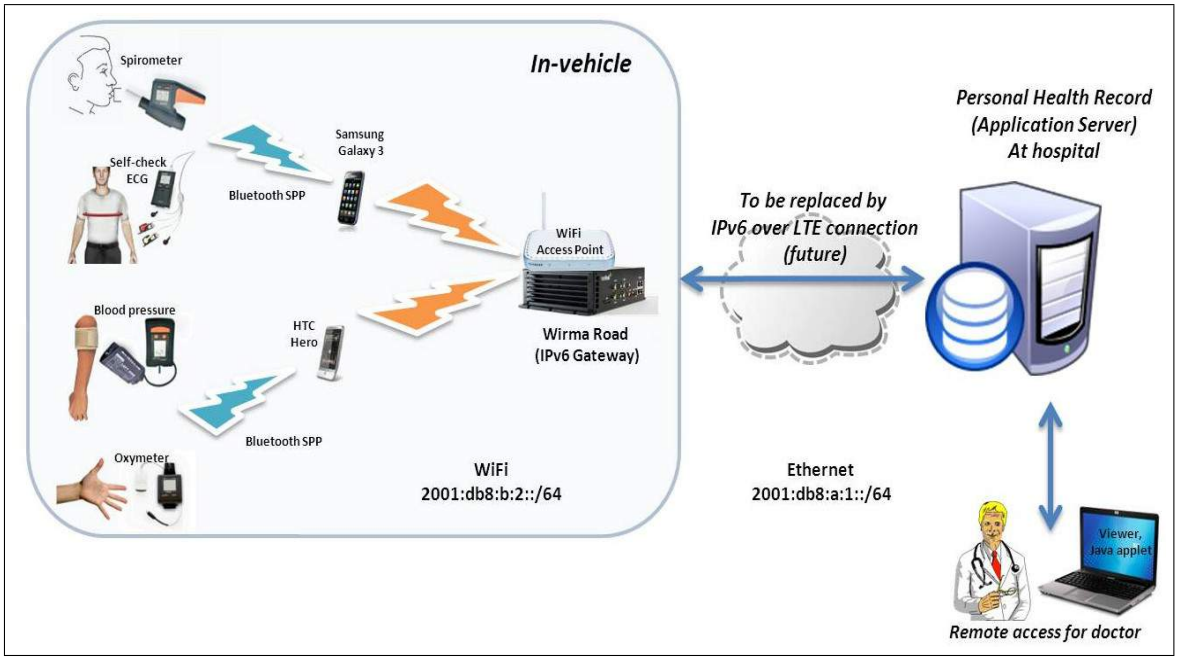


Figure 3.9: eHalth and Vehicular testbeds integration.

attached to the AP and configure IPv6 addresses on the 2001:DB8:B:2::/64 prefix. The devices are then used with the Vidavo Android Application that collects the data before sending it to the server over HTTPS along with a user comment (optional).

Figure 3.10: Web Interface for remote viewer. The health care specialist will have access to the collected information along with patient comments.

The server, which is located in the Internet side (Egress interface), configures an IPv6 ad-

dresse on the 2001:DB8:A:1::/64 prefix. The server is then ready to receive the data. The server application runs over Java (tomcat webserver) and includes a MySQL database, where the collected data is stored and organized per user ID. The physician can then issue a remote access to the server in order to observe the data as depicted in Figure 3.10. In order to observe these measurements (path from the viewer to the server), IPv4 and IPv6 access to the application server are possible.

The energy spent on sending a message from an eHealth end device through the Android Cluster Head has also been measured using the Vida24 application (Android client application) on the Android phone. The results show an average smartphone energy consumption at minimum usage of 5% phone battery energy consumed per hour. The eHealth end device (Oxymeter for instance) on the other hand, will consume 60mW in a typical operating mode (off the shelf, manufacturer default configuration). Figure 3.11 shows the IPv6 configuration of the Android phone in a typical setting behind the Mobile Router.

Figure 3.11 illustrates the state of the smartphone connected to the MR. In particular, RFC 4941 "Privacy Extensions IPv6 addresses" (part of the 2.6.X linux kernel in the smartphones) is here used to issue connections towards the PHR. This is a privacy-related precaution that prevents the user from being tracked. This is completed by the use of secure HTTPS connection on the application layer to meet the privacy requirement for eHealth's sensitive data.

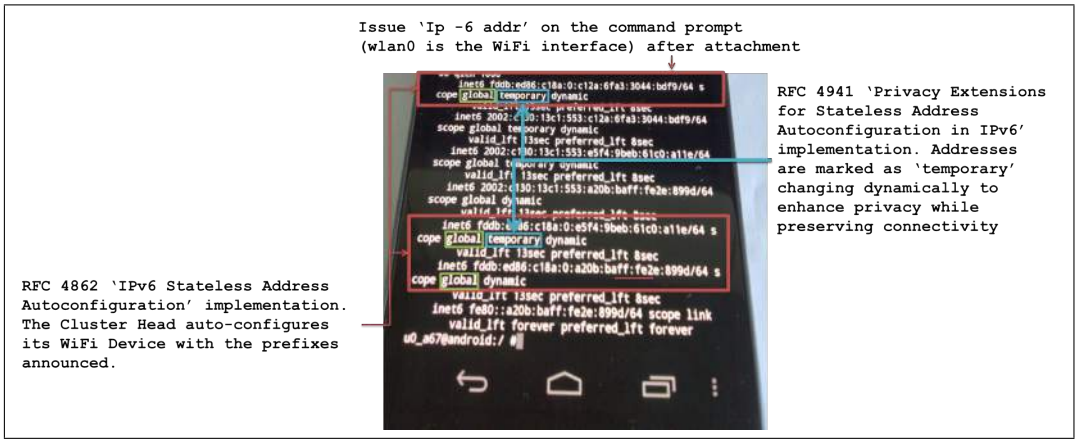


Figure 3.11: Android phone as connected to the MR.

3.3 Fully Electric Vehicles

Vehicular communications emerged as a promising area for the deployment of safety and infotainment applications. A detailed study of the vehicular networking requirements, standards and solutions can be found in [127]. Usual state of the art studies [90] consider V2I and V2V interactions as the basis for vehicular networking use cases. Major applications as eSafety, traffic efficiency, and infotainment often require infrastructure end-to-end access, hence the use of V2I Due to higher market penetration and ubiquitous coverage with high throughput, some recent FP7 initiatives [70] propose V2I use cases through LTE. Main technical motivations are the conservation of an IPv6 end-to-end communication model among heterogeneous nodes and the support of multi-hop communications for in-vehicle networks.

The recent advent of Fully-Electric Vehicles in many big cities aiming at improving transport efficiency and sustainability make use of such V2I interactions. Indeed, on the one hand, reducing emissions, extending mobility opportunities and creating new markets following gradual

introduction of FEVs on the roads, are expected to leverage the deployment costs of the charging stations and more infrastructure [60]. On the other hand, in order to accelerate the users' adoption of FEVs, the driver need to be confident in his ability to reach an arbitrary destination and adapt his driving behavior to the specifics of electric mobility (regenerative breaking, for example) [99]. With respect to these objectives, car manufacturers, standard development bodies and other contributors from industry and academia proposed use cases and scenarios to improve the energy efficiency and extend the driving range. These use cases usually involve traffic efficiency management applications and collaboration between traffic management infrastructures and energy provision infrastructures and/or other relevant infrastructure systems.

3.3.1 Related work

In the last decade, several European projects proposed to simplify the usage of FEVs and improve its acceptance among drivers. The European project e-DASH [59], aims at supporting a high quality of service for FEV drivers while ensuring the electricity grid stability. The project considers the vehicles as moving batteries at the service of the grid: capable of storing energy at production peaks, and capable of restring that energy when required at high consumption periods. To this end the Vehicle-to-Grid (V2G) interface has been developed to include bidirectional communication with charge spots and grid by extending the ISO/IEC 15118 standard.

The eCoMove project [62] focuses on the development greener ITS composed of cooperative mobility systems and services. To improve energy efficiency, eCoMove provides on-board driving assistance systems that help the driver to choose the greenest route and to optimize his driving behavior. Furthermore, the project also develops traffic efficiency management applications to improve the overall traffic management in terms of energy consumption.

The ongoing EU project eCo-FEV [61] aims at achieving a breakthrough in FEV introduction by proposing a general architecture for integration of FEVs with different infrastructure systems cooperating with each other. This collaboration should provide precise FEV mobility services and charging management services based on real time information. The cooperative e-mobility infrastructure enables the information exchanges between independent infrastructure systems in order to provide efficient telematics and ITS services to FEV users. This requires that the FEV specific constraints and mobility needs are taken into account. Eventually, the goal is to integrate efficiently the FEVs and their back-end with road and charging infrastructures.

The projects e-DASH, eCoMove and eCo-FEV are complimentary. While e-Dash focuses on the the integration of electric mobility into the global electricity transportation and distribution network, eCo-FEV takes care of the daily operation of FEVs (eCoMove architecture can be be seen as a subset of eCo-FEV's). More projects, such as CVIS [47], iTETRIS [115] and PRECIOSA [178] focused on other aspects of infrastructure integration, simulation of large scale architectures and security/privacy of ICT in the ITS context.

Authors of [157] investigate the use of network-based IPv6 mobility management protocol PMIPv6 for the electric vehicle charging service use case. In particular, authors study the handover time for communications over PLC and WLAN in a local testbed (for the EU project VELCRI) to assert IEEE 1646 compatibility. In comparison, this section enlarges the use case considerations and take into account other infrastructures such as described in the eCo-FEV project. Moreover, we consider the use of Vehicle Identification Numbers (VINs) in PMIPv6 to *uniquely identify* vehicles even when using heterogeneous communication interfaces (PLC, WiFi, LTE or other).

Related to the topic of Vehicle-to-Internet and Vehicle-to-Grid communications, authors of [185] and [104] study the implications of such use cases onto the user's privacy. One major concern being the possibility for a malicious third party to follow the driver's trip and be able to

portray his profile and habits, authors propose to enhance privacy through anonymous credentials for payments and not to disclose critical information in the network (such as the current battery charge level, the amount of refilled energy, or the time periods in which the vehicles are actually plugged in).

3.3.2 IP-based services for eMobility in ITS

Figure 3.12 illustrates the reference architecture that aims at simplifying the usage of FEVs. In this architecture, FEV's IP mobility is handled using PMIPv6 [92]. IP-based services should play the role of facilitator between the travelers and the existing infrastructure operators to enable advanced use cases and services to FEV users. For example, trip planning and assistance during a journey, which usually consists in easy booking user interfaces for charging and parking billing. Multi-modal transportation applications that optimize the usage of individual FEV and public transport, and ease the car sharing experience. We can also integrate other applications for quick trip reconfiguration according to traffic events. This section analyses the scenarios that relates to the everyday usage of FEVs. In particular, we explain how to provide IP connectivity in different contexts to interface the FEV with the operator's infrastructure.

3.3.2.1 Fully-Electric Vehicle charging

In order to ensure the driver's confidence in reaching arbitrary destinations despite well-known limitations such as battery technologies, and mitigating the risks involved by the use of inherently insecure basic IP datagram exchanges, a trip planning is necessary. It corresponds to the pre-starting phase of travelling. Nevertheless, in some situations (e.g. using the FEV for a touristic visit without precise target, driving on the well-known route) the planning can be omitted. When planned, the trip can be characterized by many features like multiple or simple destinations, one way or round trip, trip timing, schedule and duration constraints, or parking and charging preferences. In this use case, the traveler issues a navigation request to its IP-based application and the system calculates the route according to the request. If requested by the traveler, the system may select and book the required facilities along the calculated route. Connecting the FEV to the infrastructure may be achieved using different communication or network interfaces: Wireless (IEEE 802.11p), Cellular (3G/LTE) or Electric (PLC). Valid FEV credentials (validated by AAA servers) ensure correct driver profile, identity and permissions. This allows different operators to propose services related to billing (time and cost), booking and trip management.

3.3.2.2 IP at a charge spot: ISO-15118 and V2Grid overview

In the context of future energy grids or "smart grids", the FEV could play an important role in regulating the energy consumption by dynamically defining a charging schedule for each FEV that could also be used as energy storage and eventually supplies the grid itself with energy. Furthermore, the Electric Vehicle Supply Equipment (EVSE) has to identify and authenticate the FEV or the FEV-User, and perform authorization and accounting. Therefore, communication between the grid and FEV becomes essential. The ISO-15118 standard defines such a communication protocol, which follows the client/server-model and uses IPv6 at the network layer. While Parts 2-3 of the standard, describing the OSI network layer specifications, are in the state of Draft ISO Standard (DIS); the first part (ISO-15118-1), which describes the use cases for the protocol, is already an International Standard (IS) [199]. It envisages to offer services for charging scheduling (using different power levels) between FEV and EVSE that allows the FEV user to keep his charging goals on one hand, and gives room for charging optimization based on different utility functions, such as optimal price, on the other.

Another important use case identified in the standard is called Value-Added Services (VAS), where other IP-based services, including information exchange between FEV, EVSE, and/or secondary actors are supported. Examples to this could be requesting charging spot availability information or charging spot reservation.

FEV or FEV-user authentication in ISO-15118 can be done by the EVSE either locally or by contacting a secondary actor, which may or may not authorize the FEV. The second case requires IP connectivity between EVSE and the secondary actor. In case the EVSE does not have any Internet capabilities (making it less expensive) the SECC (Supply Equipment Communication Controller) could use the internet connectivity of the FEV. This can be the other way around, where an FEV without Internet connectivity can use the EVSE's connectivity over the ISO-15118 VAS.

3.3.2.3 More IP-based services for FEV

Currently, FEV is not yet fully accepted by customers. One of the obstacles to this acceptance is the lack of confidence that customers have towards FEV, especially with the charging aspects. Indeed, electrical charging stations are not yet as heavily deployed as fuel stations are. Therefore, the FEV charging service has to be as precise and reliable as possible in order to reach customers' confidence. Providing IP connectivity to FEV helps solving the aforementioned issue as it allows FEV to access a wide variety of services over the Internet. Indeed, many of them can be used to strengthen the charging service but also to improve the user's driving conditions:

- *Real-time traffic conditions:* knowing the current traffic conditions, a FEV is able to compute an alternative itinerary that, for instance, avoids traffic jam. Also, these information help FEV to compute more accurately the remaining distance that can be traveled before the battery is empty, and therefore to start the charging procedure on time.
- *Weather conditions:* weather conditions are also an important factor that should be taken into account as it directly impacts driving conditions (e.g. reducing driving speed, increasing brake distances, turning on lights/wipers, etc.) and, consequently, the FEV energy consumption.
- *Roads state:* open or closed roads, presence of deviations, roadwork, or any unexpected event that impacts driving conditions (e.g. modification of the maximum allowed speed limit) are also useful information that can be exploited by FEV.

In addition to the above mentioned services related to driving conditions, IP connectivity also grants access to any other services available on the Internet. For instance, entertainment-related services such as Video-On-Demand, e- mailing, video calls or video gaming can be used by FEV passengers during the trip.

3.3.3 Integrated architecture for electric mobility

Figure 3.12 illustrates the reference architecture that aims at simplifying the usage of FEVs. In this architecture, FEV's IP mobility is handled using PMIPv6 [92]. To achieve this objective the system will play the role of facilitator between the travelers and the already existing infrastructure operators. This system will provide communication interfaces to enable data exchanges between multiple infrastructures and FEVs to guarantee advanced use cases and services to FEV users. The main functions relate to trip planning and assistance during a journey: easy booking of the charging and parking facilities, providing secure payment facilities, optimizing the balance

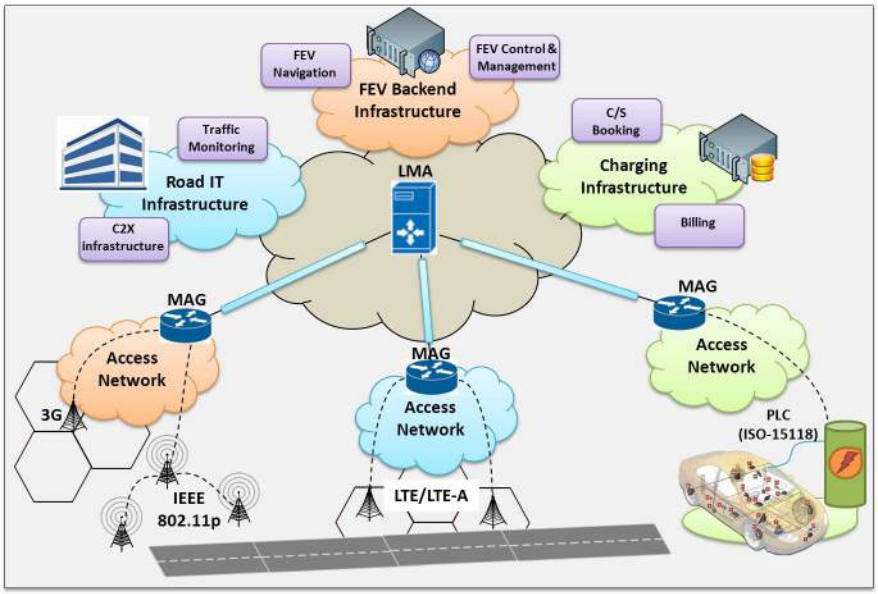


Figure 3.12: Architecture of integrated collaborating infrastructure systems for FEV service management and network mobility support for IP-based services.

between usage of individual FEV and public transport, and quick trip reconfiguration according to traffic events.

When it comes to the use cases described above, the FEV might be involved in Vehicle-to-Internet communications at different places from home to work or any other random location. PMIPv6 being a network-based protocol, it is able to support heterogeneous communication technologies transparently from the FEV perspective. The seamless vertical handover between communication technologies and IP session continuity allows a better support of FEV-related services. The network-based nature and centralized architecture of PMIPv6 also allows it to integrate different infrastructures such as illustrated in Figure 3.12. PMIPv6 is further detailed in Chapter 4.

PMIPv6 supports mobility through the use of the Mobile Access Gateway (MAG) and the Local Mobility Anchor (LMA). On the one hand, the MAG detects the presence of the vehicle and performs the mobility-related signaling on its behalf. On the other hand, the LMA saves the current location of the vehicle to deliver its traffic. In order to identify a mobile node inside the PMIPv6 domain, each mobile node has a distinct RFC4283-compliant Mobile Node Identifier (MNID) [170]. The LMA stores this MNID and uses it to lookup mobile nodes and update their status if the MAG notifies it with a change. The MNID is usually a layer-2 identifier (such as the MAC of the interface). This approach is not compatible with our heterogeneous FEV that connects to the network through multiple communication interfaces each with its own MAC address. If not handled properly, each FEV interface might be perceived by the LMA as a new mobile node, resulting in poor support of IP mobility and incoherent data transfer/delivery.

This situation in J. Day's "Patterns in Network Architecture, a return to fundamentals" book [48] is explained as a result of the IPv6 address being proper to one interface rather than one host with multiple interfaces, hence the argument about the MAC address being a bad choice for the Interface ID part of the address (EUI-64). We are here confronted to the same argument and we need a new node identity to map onto our RFC-4283 MNID option. Some examples of identifiers include Network Access Identifier (NAI), Fully Qualified Domain Name (FQDN),

International Mobile Station Identifier (IMSI), and Mobile Subscriber Number (MSISDN). While these identifiers might be mapped to the MNID option, we here focus on describing how the ISO-3780 Vehicle Identification Number (VIN) maps into this option.

3.3.3.1 VIN as RFC 4283 identifier

The Mobile Node Identifier option is an optional data field that is carried in the MIPv6-defined (and by extension, in the PMIPv6) messages including the Mobility header. According to the standard [170], various forms of identifiers can be used to identify a Mobile Node (MN). The Network Access Identifier (NAI) [3] and the IEEE MAC address are two examples of such namespaces used for identification. Figure 3.13 illustrates the mapping of the MNID option and the content of its fields. This option does not have any alignment requirements. Depending on the implementation and the chosen identifier space (NAI or MAC for instance), the identifiers can be mapped from the ASCII to the binary or directly mapped as binary digits in the MNID option before being sent. When used with MIPv6 (resp. PMIPv6), this option will then carry the identity of the mobile node and thus be part of all the binding updates (resp. proxy binding updates) and binding acknowledgements (resp. proxy binding acknowledgements).

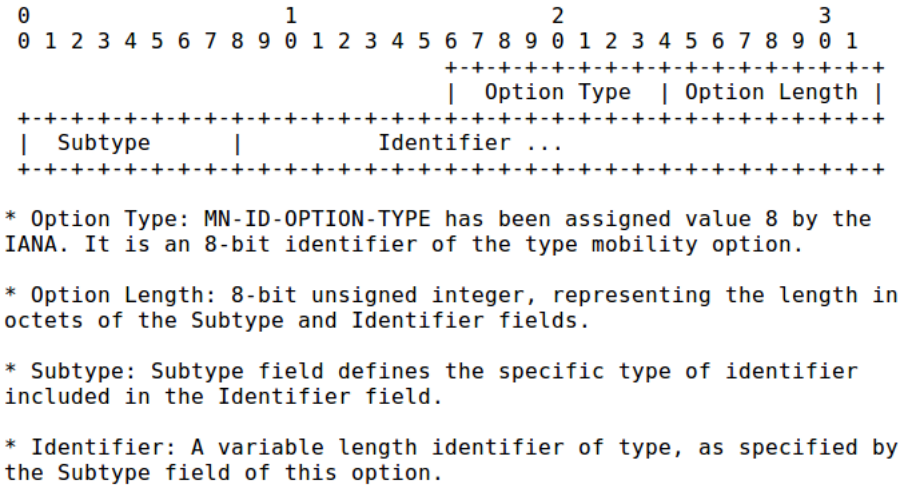


Figure 3.13: RFC 4283 Mobile Node Identifier option for MIPv6.

As explained in section 3.3.3, due to its multiple heterogeneous communication interfaces and the centralized nature f the PMIPv6 architecture, interface-specific MAC addresses should not be used to represent the whole vehicle with all of its connected hosts/machines. For this purpose, we propose the use of the ISO-3780 Vehicle Identifier Numbers (VIN) as RFC-4283 MNID option. Similar to the other namespaces mapping, VIN to MNID mapping will preserve the uniqueness of the VIN (distinct VINs are mapped to distinct MNIDs).

The VIN (more details in Chapter 5) is a 17 characters alphanumeric hierarchical code that uniquely identifies a vehicle worldwide. The VIN can be broken down to the World Manufacturer Identifier section (WMI), Vehicle Description Section (VDS), and Vehicle Identification Section (VIS). We propose the use of VIN in the MNID option for its great potential in being a vehicular-specific identification space which is:

- ISO-3779 and ISO-3780 standard
- Mandatory, unique, and present in every vehicle

- Hierarchical vehicular-specific endpoint identifier

3.4 Conclusion and future work

The infrastructure of the Internet is continuously evolving to support new services. Intelligent Transportation Systems will play a fundamental role in the future, helping to preserve lives and making transportation safer and efficient. eHealth, if supported by vehicular networks could be one of the applications improving vehicle passengers safety. On the other hand, the acceptance of Fully-Electric Vehicles in many big cities to improve transport efficiency and sustainability is an opportunity to provide more IPv6 infrastructure based services. This is to help accelerating the users' adoption of FEVs, by increasing their confidence in being able to reach an arbitrary destination and adapting their driving behavior to the specifics of electric mobility.

This chapter described the technical challenges of these two vehicle-to-Internet use cases: eHealth and FEV services. We presented our integrated eHealth platform and described the involved protocols. We also presented our mobility-supporting architecture in the context of FEV-related service. We reviewed the characteristics of both use cases and determined their common technical requirements for in-vehicle IP-based services. We also determined the importance of mobility-supporting IP-based protocols and mobility management architectures. We also described some similarities when it comes to the IPv6 communication requirements for both of these applications.

Next chapter focuses on the last use case (mobility management architectures for IP-based services) and presents the performance analysis of different mobility management protocols approaches.

Chapter 4

Performance study of network mobility management protocols

The IETF defines the IP locator/identifier split (also referred to as IP semantic overload), mobility management and multihoming as the challenges to overcome for a scalable and reliable Future Internet [48][146]. This chapter reviews the IETF network mobility techniques for an IP-based platform composed of backend servers, networks of fixed charging stations and of mobile FEVs. This is to allow further services for ensuring driver's confidence in reaching arbitrary destinations, despite well-known limitations such as battery technologies, and mitigating the risks involved by the use of inherently insecure basic IP datagram exchanges. In particular, this chapter is focused on the comparison study of Network Mobility (NEMO) extension as proposed in *host-based*, *network-based*, and *distributed* mobility management protocols.

While mobility is a feature that may be defined at different layers [63], we focus in this chapter on Network-layer mobility approaches for the host and the network. Network-layer mobility approaches have attracted a fair amount of contributions in the research and standards tracks [22] [52]. The main reason the IETF chose the Mobile IP approach as the de facto standard for Network-layer mobility approach is for interoperability reasons. Implemented using mechanisms at the layer 3 (the waist of the Internet Protocol), mobile and fixed users are oblivious to the presence of Mobile IP users and able to communicate with them without any upgrade to their stack [172]. Organizations that wish to implement the Mobile IP architecture (hosting the Home Agent) and support mobile IP-based services, benefit from the control and policies they install on their infrastructure[1].

This chapter first explains the importance of addressing architectures for mobility and the topological correctness, inherent to IP addressing. It then gives the overall picture that integrates the reviewed technologies before stressing the importance of IP network mobility in such scenarios (in particular those requiring Vehicle-to-Internet communications). Host-based, Network-based and Distributed addressing and mobility architectures are compared before focusing on the problem of session continuity for IP-based electric mobility related services. In particular, Mobile IPv6 (MIPv6), Proxy Mobile IPv6 (PMIPv6), and Distributed Mobility Management (DMM) standards are reviewed from a network mobility perspective. A qualitative feature characterization and an analytical model to compare the protocols are provided.

In detail, our contributions in this chapter are:

- The study of addressing topologies and the concept of topology correctness

[1]The effects of Home Agents introduced in the middle of an end-to-end source-to-destination path, can be considered disruptive to the original end-to-end argument that lead initial Internet Protocol developments. So are the effects of NATs, Firewalls and other middles boxes introduced in the markets [50].

- Mobility management schemes and their taxonomy
- IETF standards and research landscape of main approaches
- Extending the existing DMM architecture with our NEMO extension
- Features summary and comparison of the proposals
- Performance evaluation of the proposed techniques through a exhaustive parameterized analytical model

4.1 Addressing architectures

The scalability of the Internet routing system suffers from an increasing demand for provider-independent non-aggregatable IP addresses. Some approaches tried to alleviate the core network scaling issue through novel routing architectures based mainly on indirection between provider-independent addresses at the edge and aggregatable, provider-allocated addresses in the core of the Internet [143] [145].

4.1.1 Topology correctness

Mobility and multihoming management challenges are usually solved using indirection [145]. For instance, MIPv6/NEMO and PMIPv6 use the concept of indirection (through address translation) at fixed points of the network (respectively, Home Agent for MIPv6 and Local Mobility Anchor for PMIPv6) [52]. Usually, the home addresses are derived from Provider Independent Addressing (PIA) pool and translated to temporary care of addresses that belong to the Provider Allocated Addressing (PAA) pool [32]. The mobile users are *permanently identified* in their domain's PIA pool and *temporarily located* in the PAA pool announced in their current point of attachment.

In the PIA scheme, the home domain where the MR belongs is responsible of the *home prefix's uniqueness*. Eventually, the MR is able to generate a *collision-free* addressing scheme by combining the announced unique prefix to a local identifier, also globally unique (EUI-48 and EUI-64 are often used). *The MR is identified and located in two distinct topologies: in the IP realm (at the provider infrastructure and the home domain) and in the IEEE EUI realm through the Interface Identifier (at the interface manufacturer domain)* [49].

While PIA/PAA are used for Autonomous Systems as large as an ISP, when the routing domain shrinks, so does the addressing scope. The IETF originally defined three scopes for the IPv6 address to be used as appropriate: Link-local, Site-local and Global. While Link-local and Global are still used, the site-local scope has been deprecated [105]. The main criticism was the *ambiguity* of site local addresses. Indeed, the absence of a unique identifier for each domain/site, kept the developers into ambiguity as to which host belongs to which site if every site-local scoped address is of the format "FEC0::1234:5678:9ABC" ?

The immediate consequence for site-local scoped networks is the absence of a proper addressing mechanism allowing local communications without any connected gateway relaying an infrastructure-delegated prefix [2]. The consequence for our in-vehicle network (the network inside the vehicle, connected to the MR) is the dependency on the presence of an infrastructure that would announce a guaranteed unique IPv6 prefix. When the MR is disconnected, the in-vehicle network devices must uninstall the previous IPv6 addresses to be topologically correct. It follows

[2] The prefix can be obtained through DHCPv6-prefix delegation as explained in Chapter 3.

that devices on separate networks cannot communicate[3]. Unique IPv6 Local Addresses (ULA) have been defined as a replacement for site-local scoped addresses with modifications, among which the presence of a site identifier (Figure 4.1).

With regards to the topology correctness, the IPv6 addressing architecture can be infrastructure-based or infrastructure-less. Table 4.1 summarizes the main characteristics of the two approaches.

4.1.2 Infrastructure-based addressing

IP addressing is strongly tied to the notion of topology[4] and remains meaningful as long as it belongs to its domain of definition [52]. From the perspective of an IP-based services providers (for example, traffic management centers), the IP addressing used to reach the in-vehicle attached hosts must be global and topologically correct. Here, the topology can either reflect the network organization of the service provider or the internal topology of the network provider (operator/ISP). The autonomous sites that are not network operators/ISPs, generally prefer to have PIA space. Doing so gives them additional agility in selecting ISPs and helps them avoid the need to renumber when changing their ISP.

The sites (Autonomous Systems) that wish to have their own topologies request a pool of Provider Independent addresses. The RIR policies allow them to request such a pool. These addresses are usually not aggregated with the network provider's addresses (who actually routes and transfers the packets, such as Internet Service Providers) who uses its own pool of addresses. Therefore, this practice requires additional entries in the Default Free Zone routing and forwarding tables (tier-1 ISPs)[146]. The actual cost of this Traffic Engineering (TE) practice is expressed in terms of additional routing entries, routing overhead, and further BGP update churns in the core network leading the system as a whole to suffer from a lack of scalability in a large scale [64].

The benefits for a service provider are an independent addressing scheme that avoids renumbering when changing ISPs, support of multi-homing, and better management of network mobility for its hosts [52]. The privacy when using either infrastructure-based addressing architecture is not guaranteed. Users of such providers are highly exposed to eavesdropping and other information collectors' practices. Current best practices recommend the use of temporary addresses generated using forged Interface Identifiers (not IEEE)[154].

4.1.3 Infrastructure-less addressing

Regardless of the nature of an IPv6 addressing (PIA or PAA), from a vehicle's perspective, the addressing is *infrastructure-based*: the MR needs to be connected to the infrastructure to configure a proper network prefix for its connected interfaces. In an infrastructure-less scenario, in particular for the local in-vehicle communication needs, a Mobile Router may use locally generated addressing that is independent of the infrastructure. For IPv4, RFC 1918 specifies the use and scope of private addresses with prefixes permanently allocated at the IANA [107]. In the case of IPv6, RFC 4193 defines an alternative method for the generation and the use of unicast local IPv6 addressing (ULA) within a determined site's scope [135]. Such locally generated prefixes cannot be mobile as the network operator is not supposed to be aware of them. It is noteworthy that Network Address Translation (NAT) techniques, which are compatible with RFC 1918, are not recommended for RFC 4193 compliant addresses [216].

The address planning needed to perform in-vehicle inter-machine communications includes PIA and ULA Addressing [36]. As mentioned earlier, the AS that uses PIA pool decides for

[3]As a reminder, the 2001:db8::/32 prefix is defined for documentation and must not be used for isolated

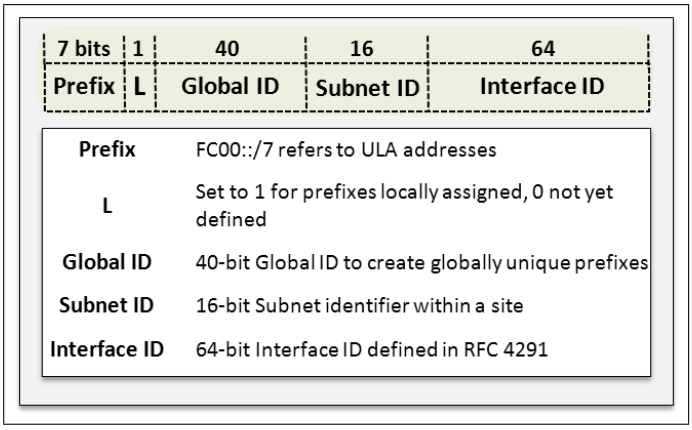


Figure 4.1: Unique Local IPv6 Address format.

the in-vehicle addressing architecture. In this scenario, the in-vehicle embedded machines are topologically connected to their AS. The AS is then considered the Home Network, and the PI prefix, the Home Network Prefix (HNP).

Alternative addressing is based on RFC 4193 to generate Unique Local IPv6 Addresses. Figure 4.1 illustrates the content and format of the ULA address. The standard specifies a pseudo-random generation method that uses a unique system identifier. In our case, this identifier could be the MR ingress MAC address, or any other identification number such as the Vehicle Identification Numbers (VIN). The RFC 4193 recommended ULA generation algorithm is illustrated in Algorithm 1.

Algorithm 1 IPv6 Unique Local Addresses generation

1) Get the current NTP format time on 64bits.
2) Get the EUI-64 of the system. If not available, convert the MAC (48bits) into EUI-64 using RFC 4291. If not available, use a unique system identifier (e.g. VIN).
3) Concatenate values 1 and 2 into a 128bits key.
4) Compute the SHA-1 of this key into a 160bits result.
5) Use the least significant 40bits as a Global ID.
6) Concatenate: FC00::/7, L, and the 40bits Global ID to create a /48 ULA prefix.

Unique local addresses allow for the in-vehicle network to be deployed independently of whatever provider assigned or provider independent address space is used and to be operational during any global re-addressing event [135]. When it comes to FEV mobility, the drawback of ULA has to do with its limited scope: ULA is for internal use only and not intended to be used across the Internet. Thus, notifying service providers globally with this addressing is not possible [36]. Nonetheless, it is possible to extend the use of ULA addressing across collaborating interconnected domains through certain approaches that are out of scope for this chapter [138].

networks configuration.

[4]The literature often states "Yakov Rekhter's Law" as the fundamental assumption for the scalability of routing systems "Addressing can follow topology or topology can follow addressing. Choose one." [146]

Table 4.1: Addressing architecture features comparison

	Type	Scope	Privacy	Generation method	Mobility support
PAA	Infrastructure-based	Global	Not guaranteed	Prefix announced after network association	Depends on the provider domain
PIA	Infrastructure-based	Global after AS announcement	Not guaranteed	Administrative request to the RIR	Compatible with host, network and distributed approaches
ULA	Infrastructure-less	Global with the scope of a site	Guaranteed if the generation method is pseudo-random	Pseudo-random algorithm (RFC 4086)	Not default. Possible if anchored in the infrastructure

4.2 Mobility management schemes

4.2.1 Mobility as viewed from the network layer

Starting from the legacy IP addressing and naming conventions originally developed for stationary hosts, mobility can be seen at the network-layer as an address translation problem [22]. At the network layer, we need to distinguish between the concepts of name and address (best discussed in [193], [187] and [160]). Basically, a host's name is a location-independent identifier whereas its address reflects its current point of attachment to the network. Hence, a static host can use both names and addresses interchangeably; but a mobile host will have a different address each time it attaches to a different domain. The name is then the only location-independent identifier that can be used to refer to mobile hosts.

At the network layer, only the IP namespace can be used to derive both names and addresses. A host that belongs to a domain (home domain) with its own addressing architecture (ideally, a provider independent addressing) will derive an address. The host will be *reached* at this address and it will *initiate* sessions with arbitrary hosts using this address. This home address identifies the host (name) and locates it inside its home domain (current point of attachment).

If this host is static, this name-to-address binding will not change: the home address reflects the name and the location of the host. But if the host moves and attaches to a foreign network (with its proper addressing architecture), the name-to-location becomes a function of time and changes following the mobility pattern of the host. The highlight can be then put over the name-to-location function and what it implies in terms of architecture components and functionalities.

4.2.1.1 Architecture components

Existing network-layer mobility management protocols have primarily employed a mobility anchor (that handles the name-to-location function) to ensure connectivity of a mobile node by

forwarding packets destined to, or sent from, the mobile node after the node has moved to a different network. Initially, the mobility anchor has been centrally deployed. MIPv6, PMIPv6, and HMIPv6 are such examples of centralized mobility management schemes. Hence, the traffic of (potentially) millions of mobile nodes in an operator network is typically managed by the same anchor (such as in LTE with PMIPv6). Recent proposals investigate the feasibility of distributed mobility management, by affecting certain centralized functionalities into different network components [34].

Important mobility management functions resulting from the research, development and standardization of these mobility management protocols are:

1. The **Anchoring** function allocates and IP address/prefix to a mobile node. Since the mobility anchor belongs to the host's home domain, the IP is called Home Address (HoA) and the prefix a Home Network Prefix (HNP). These are topologically anchored at the home domain and need to be advertised globally to be routed (cf. Section 4.1). The *Address/Prefix delegation* function is generally co-located with the anchoring function, but can be separated in certain cases (for example for NEMO where a DHCPv6 server can take charge of this function).

2. The **Location Information/Directory** function manages the location information of host and tracks its IP addresses changes. The accuracy of the IP address on the current point of attachment is essential for the relevance of name-to-address binding function. The binding ties the HoA/HNP to the foreign host address. The location update protocol is responsible for the accuracy of this directory information. If this protocol involves the host in the control plane, the protocol is *host-based*. If the protocol includes a mechanism to detect the host's movement and does not involve it in the signaling, the protocol is *network-based*.

3. The **Forwarding Agent/Management** function is responsible of the data forwarding to/from the Home IP address/prefix assigned to the host, based on the location directory (current location information). The translation from HoA/HNP to the foreign address/prefix happens using an *address translation mechanism*. Usually, two mechanisms are known at the network-layer: address rewriting or encapsulation. MIPv6, PMIPv6 and HMPIv6 use the latter approach for performance reasons.

In Mobile IPv6, the home agent handles the anchoring function, the location information management and the forwarding function. It is also part of the location update protocol executed in interaction with the mobile host. In Proxy Mobile IPv6, the Local Mobility Anchor provides for the anchoring function and the location information but distributes the location update protocol and the forwarding management between the LMA and the Mobile Access Gateway (MAG).

We can also distinguish between the macro-mobility and the micro-mobility management (Figure 4.2), when a mobile host roams between different administrative domains. In terms of network functionalities, if the host is anchored at the same point when it moves, then the mobility is of the *micro or local* type. If the anchoring point changes, the mobility is of the *macro or global* type. In the latter, depending on the policies, current communication sessions might be lost [139].

4.2.2 Standards landscape

As mentioned briefly above, initial standard IP mobility management solutions proposed a *centralized* anchoring functionality hosted at a unique network component. MIPv6's HA, PMIPv6's

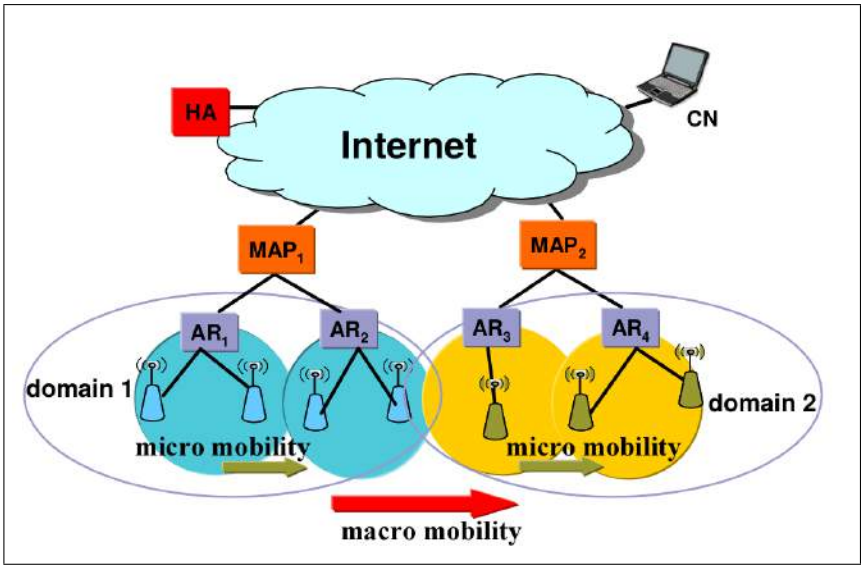


Figure 4.2: Intra-domain (micro) and inter-domain (macro) mobility of nodes.

LMA are such examples of centralized approaches. The current activities at the IETF's Distributed Mobility Management (DMM) working group aim at the distribution of the anchoring and mobility management functions [139]. The main arguments in favor of the distributed mobility advent revolve around provisioning the network with more capacity to avoid single point of failures/attack and an appropriate *flattened* mobility architecture to face nodes' mobility patterns and needs [34].

Another important part of the mobility management at the network layer is the location update protocol. Indeed, the forwarding function to properly transmit/deliver a packet, relies on the accuracy of the location directory entry that concerns a given mobile host. In order to update the location information properly, the host can directly interact with its directory and updates it with the current network point of attachment (Foreign IP address). In this case, regardless of centrality of the anchoring function, the mobility protocol is said to be host-based. MIP, HMIP, FMIP, HIP, LISP-Mobility [223] are such approaches. On the other hand, if the location update protocol does not interact with the host, the mobility protocol is network-based. The cellular networks typically make use of such protocols, notably the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) and Proxy Mobile IPv6 for LTE.

In order to classify the mobility management solutions, we can take two point of views (Table 4.2):

- The anchoring perspective. We then distinguish between the centralized and the distributed approaches.
- The host involvement into the location update protocol. We then distinguish the host-based and the network-based approaches.

		Anchoring function	
		Centralized	Distributed
L.U.	Host-based	Mobile IP, HMIP, NEMO, HIP, LISP-MN	Client-DMM
	Network-based	PMIP, PMIP-NEMO, GTP	Network-DMM

Table 4.2: Mobility management approaches taxonomy.

4.2.3 Centralized mobility management schemes

With regards to the anchoring functionality in a mobility management protocol, a centralized approach accumulates control and data path in the same architectural point (the anchor).

4.2.3.1 Host-based approaches

These approaches chose to centralize the anchoring point and to involve the mobile entity into the process of location update. When a host (or Mobile Node, MN) moves and changes its point of attachment it needs to be relocated from an addressing perspective. In order to be reachable, an association of the past and current address is then necessary (name-to-location binding). When using a mobility management protocol to handle these associations, the host makes use of location-independent addresses (such as PIA).

In a Host-based mobility management protocol, the host is part of the exchange that guarantees the reachability during topology changes. As illustrated in Figure 4.3, location update, IP packets decapsulation, and address association are handled by the host whereas location directory, forwarding algorithm, and address translation are handled in the anchor (at the Home Agent level). These protocols that split the responsibility of mobility management between the host and network are called Host-based. Mobile IPv6 at the network layer, Mobile TCP and Mobile SCTP at the transport layer, and SIP at the session layer of OSI reference model are all instances of mobility management through Host-based mechanisms [52].

4.2.3.2 Network-based approaches

These approaches chose to centralize the anchoring point and to not involve the mobile entity into the process of location update. The Host-based approach to solve the mobility management problem requires frequent updates to host software stacks and complex security transactions with the network [128]. Consequently, by limiting the mobility management to closed domains (micro mobility), Network-based mechanisms emerged.

Network-based Localized Mobility Management (NETLMM) approaches emphasize the distinction between name and address. Indeed, the host that roams through the attachment points of the same mobility domain is associated with a set of IPv6 prefixes (Home Network Prefixes, HNPs). These prefixes no longer refer to the topology of the network but to the host that owns them. The Local Mobility Anchor (Figure 4.4) maintains these associations on a per-node granularity basis and updates the Location Directory and Forwarding routes according to the current attachment point. Subject to correct credentials (Mobile Node Identifier) these prefixes are advertised by the Access Routers and installed by the hosts.

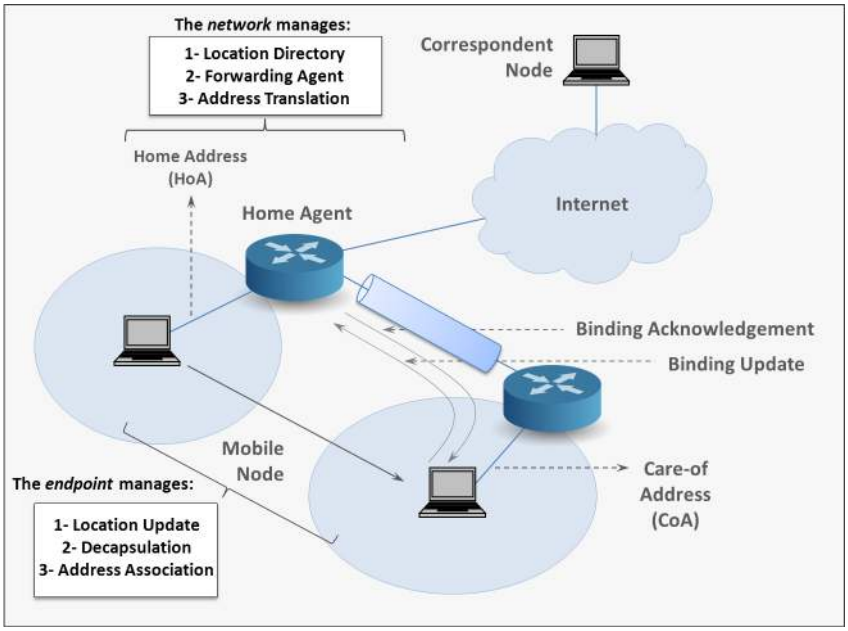


Figure 4.3: Centralized Host-based mobility management.

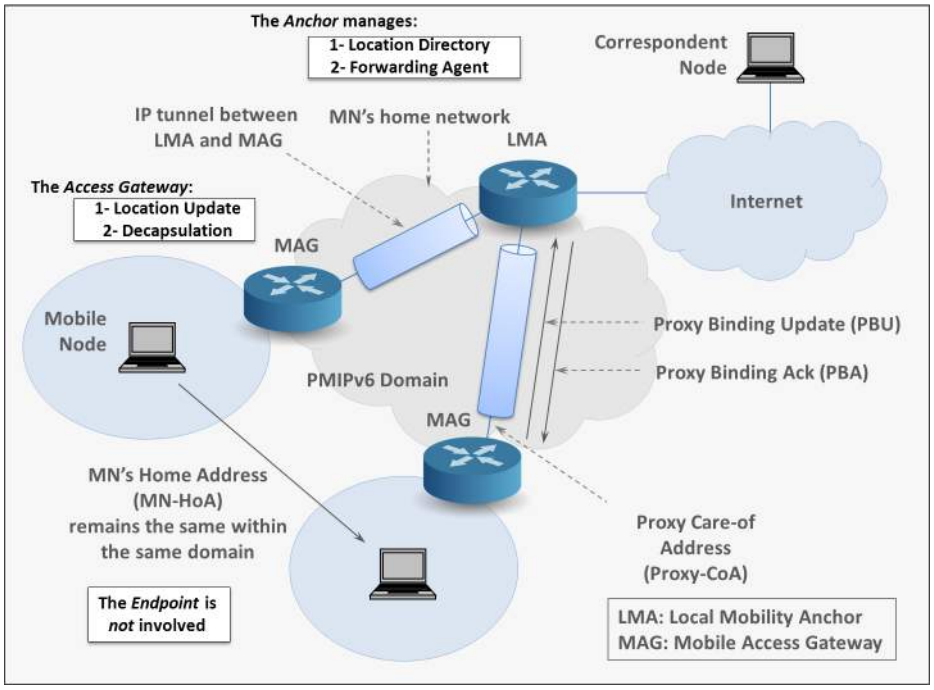


Figure 4.4: Centralized Network-based mobility management.

In terms of reachability, the Correspondent Nodes are oblivious to the host's movements as long as it roams in the same NETLMM domain. The difference with regards to Host-based approach is the reduction in handover-related signaling overhead, as it is handled in the core and does not involve interactions from the host in the Edge.

NETLMM approach is mainly defined at the Network layer of the OSI-model. In this context, PMIPv6 is the NETLMM de-facto standard for IP-based management in the 3GPP architecture for LTE/LTE-A [45].

4.2.3.3 Known limitations of centralized mobility management approaches

Mobility management with centralized mobility anchoring in existing hierarchical mobile networks, as inspired by early cellular networks deployment models, are prone to some known limitations [33]. Suboptimal routing, scalability, and reliability are the main concerns that lead to distributed mobility management working groups within 3GPP and IETF [224]. Some of these cons may be summarized as follows:

- Sub-optimal and triangular routing problems due to anchoring functionality that centralizes the routing and control paths. However, routing optimization solutions exist in the literature for different centralized approaches [156].
- Difficult dimensioning of the anchoring point performance and risks of scalability issues. Encapsulation and tunnel management for the forwarding entity in the architecture is easy to deploy but difficult to maintain to avoid bottlenecks [21].
- Potential single point of failure and attack for a network operator size wide number of users.
- Need to fine-grain the user's needs in terms of applications. Not all the users require session continuity and mobility management for all their applications.
- Incompatibility with recent CDN trends. Due to the success of mobile Internet and its important data traffic, more operators are deploying Content Delivery Network (CDNs) closer to the edge. This is to host the data that the user wants (popular applications) closer to him. This is incompatible with the concept of centralized core network entities to anchor all of the client's traffic.

4.2.4 Distributed mobility management schemes

In order to tackle the issues related to centralized mobility management, several proposals from industry and academia converge towards distributed mobility management architectures [21]. The basic idea is to distribute the anchoring functionality among several network entities to flatten the architecture resulting in a shorter data paths. In terms of location update, the solutions can here also be split into host-based approaches and network-based ones. The DMM WG at the IETF proposes to reuse existing mechanisms of previous centralized approaches (namely MIPv6 and PMIPv6) in the new approaches [123]. At the time of writing, current results of the WG do not show any consensus reached on the standard DMM approach to adopt.

4.2.4.1 Host-based approaches

These approaches chose to distribute the anchoring functionality in several network components and involve the client/host into the location update protocol. For instance, authors of [122]

(we will refer to this approach as H-DMM) and [88] (we will refer to this approach as C-DMM) propose such approaches.

Basically, the mobility anchor is distributed and its role redefined. H-DMM refers to this newly defined entity as Access Mobility Anchor (AMA) which is co-located with the access router (first hop from the attachment point of the user). This router allocates the network prefix (Pr-1) and announces it with a Router Advertisement message. The AMA maintains a coherent name-to-location binding by interacting with the user (after handovers). The difference with centralized approach occurs when the user has to perform a handover. Where as the forwarding tunnel is established between the user and the HA, in H-DMM the tunnel is established between the previous AMA (p-AMA) and the new AMA (n-AMA).

The location update phase is performed as follows. (1) The user attaches to the n-AMA and receives a new prefix Pr-2. The user will use Pr-2 for his new sessions. (2) The user registers Pr-1 to continue the ongoing communications. The user sends a Binding Update message (BU) to the n-AMA containing: the new address (Pr-2), the previous (Pr-1) and the p-AMA's address. (3) At the reception of this message, the n-AMA will send an Access Binding Update message (ABU) to notify the p-AMA with the new mobility context of the user. The p-AMA responds with an Access Binding Acknowledgment message (ABA) and both entities now set a bidirectional tunnel to encapsulate all of the user's traffic that is destined or originated from the Pr-1 prefix. (4) The user is notified by the n-AMA with a Binding Acknowledgment message (BA) that the mobility of his previous prefix is taken into consideration. This operations (BU/BA and ABU/ABA) have to be performed as long as the Pr-1 is used.

The C-DMM approach is similar in terms of architecture and mobility procedure, but differs in terms of authentication needs. In this approach, C-DMM makes use of Cryptographically Generated Addresses [12] in order to guarantee the identity of the mobile client after a handover. Basically, the CGA is generated the first time the mobile user attaches to a Distributed Anchor Router (DAR, which an AMA equivalent). The CGA are then maintained if the mobile user requires to (depending on the needs of the application). In this addressing architecture, the CGA are the Home addresses.

Figure 4.5 illustrates the distrbuted mobility management solutions, their addressing anchoring ad forwarding plane.

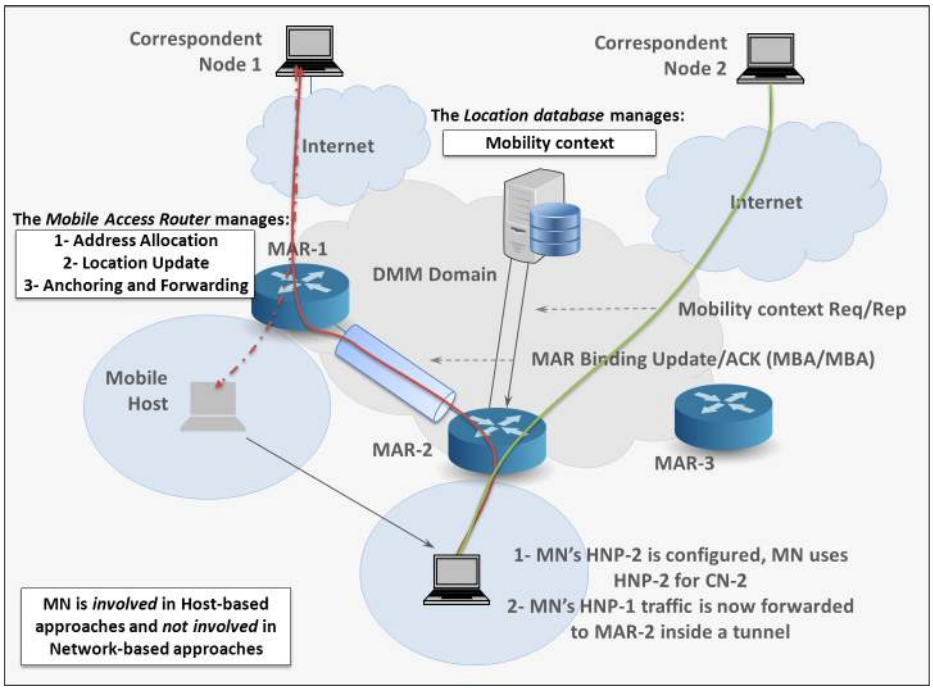
4.2.4.2 Network-based approaches

These approaches chose to distribute the anchoring functionality in several network components and do not involve the client/host into the location update protocol. As for the host-based DMM solution is based upon existing MIPv6 concepts, the network-based DMM solution is also based on the PMIPv6 standard. For instance authors of [87] and [123] both adopt this approach. Basically, the network-based DMM (N-DMM) approach is obtained by reducing the responsibilities of the LMA in PMIPv6 and allocating some or all of them to the MAG, to obtain a flat architecture. We can further differentiate between partially and fully N-DMM approach based on the *location directory/database* of the solution.

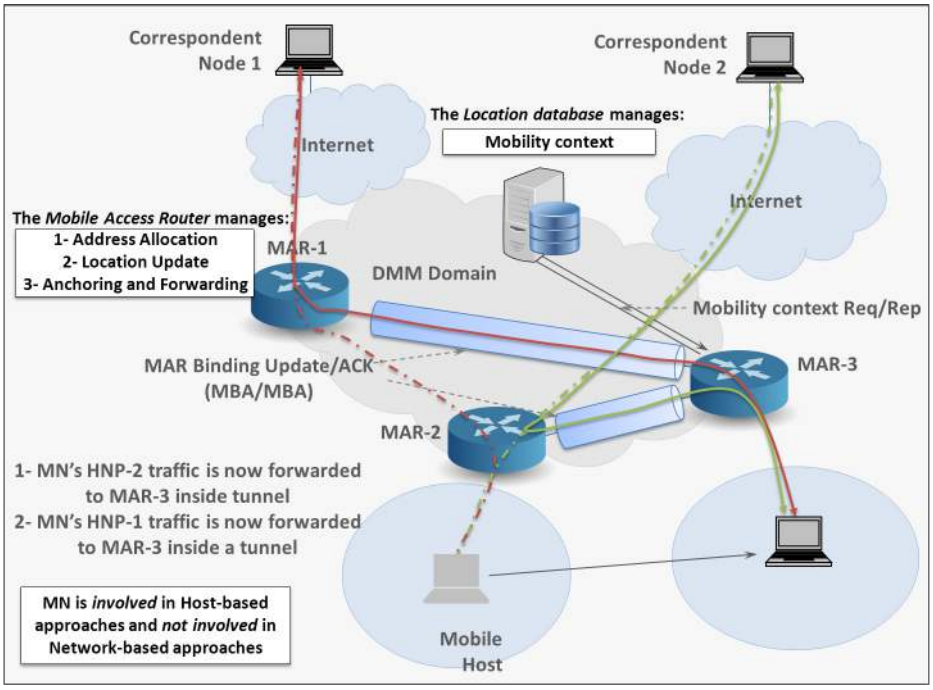
In this solution, the mobile host will attach to the Mobile Access Router (MAR). Being at the first hop from the host's network attachment point, the MAR will deliver the host with its HNP (HNP-1). When the host moves and attaches to a new MAR (n-MAR), it will receive a second HNP (HNP-2). In order to handle the mobility of the host, the n-MAR needs to know whether the it is the first point of attachment of the host (HNP-2 being the only prefix that the host has configured) or it there was previous MARs to notify.

If the N-DMM solution is partially distributed [123] (N-DMM-P), the architecture need to have a separate global location database that gathers and updates the mobility context of the

Figure 4.5: Distributed Mobility Management approaches and network functionalities distribution.



(a) HNP-1 is anchored at MAR-1 and forwarded to MAR-2 where the MN is now attached



(b) Both HNP-1 and HNP-2 related traffic are now forwarded to MAR-3 while anchored at their origin MARs

hosts. In this case, right after the host attaches to n-MAR, the n-MAR requests the mobility context of the host at the location database. The p-MAR would have already registered the

previous association (HNP-1 and the p-MAR's address). The n-MAR and p-MAR will then install a bidirectional tunnel to handle the traffic issued/destined to HNP-1. New sessions of the host must bear the HNP-2 prefix as the source address, and the host continues to receive the traffic related to HNP-1.

In a fully distributed N-DMM solution (N-DMM-F) the location database would also be deleted from the architecture. After the attachment, the n-MAR needs to figure out whether the host has a previous prefix that needs to be portable. In this case, authors of [87] propose to multicast a PBU message to all of the MARs in the domain to know if the host has already been registered elsewhere. In this case, the delay between the request and the decision may be significant and the previous session dropped. Another solution would be to interact with the host, similarly to the host-based DMM approach. In this (hybrid) case, the host still needs to have a stack update with the proper control plane, which goes against the PMIPv6 approach to support all of the devices with little to no update. Other solutions for the location update in the fully distributed case can be proposed [87].

When compared to PMIPv6, the N-DMM architecture changes the data routing path by affecting the forwarding functionality to the MAR. The signaling and data still traverses the same points (no separation of data and control paths) but the MAR being located in the access network, makes it closer to the host (first hop).

4.2.5 Centralized vs. Distributed mobility management

Table 4.3 summarizes and compares the features of both centralized and distributed mobility management approaches. The solutions that we described can either be host-based or network-based and might introduce different network components and extended control plane for different mobility granularity.

4.3 Network Mobility extensions

In order to support multiple hosts moving together as a whole, the NEMO basic support concept relies on the association of Network Prefixes with current attachment points rather than single addresses [32]. In this context, at least one Mobile Router is present in the network. The MR connects to a fixed infrastructure and guarantees the roaming of the moving network on behalf of the nodes connected to it.

In terms of mobility architecture, the vehicle can be considered as a mobile network that transports a set of mobile hosts sometimes called Locally Fixed Nodes (LFNs) [57]. Basically, mobile networks and mobile hosts need the same network functionalities (anchoring, locating, and forwarding). In fact, if we consider the mobile router only from its outgoing network interface (one CoA only), they are identical. The fundamental difference arises when we consider the case of IPv6 embedded in-vehicle networks that are connected to the MR. While in IPv4 the addressing architecture would have been simplified by the use of RFC 1918 addresses (the reachability problem apart), the IETF advises against using ULA addressing as equivalent to RFC 1918 addresses [216]. We discuss the Network Mobility (NEMO) extensions of the standard mobility management protocols in this section. One might consider the case of network mobility as a generalization of the host mobility use case.

NEMO Basic Support protocol can be defined as an extension to Mobile IPv6 protocol for the support of moving networks. Recently, the NEMO principle has also been proposed to integrate the PMIPv6 protocol and it is also expected to be defined within the DMM paradigm. In this section, we present the NEMO extension as proposed for MIPv6 and explain the current trends

Table 4.3: Features summary comparison of Centralized and Distributed mobility management schemes

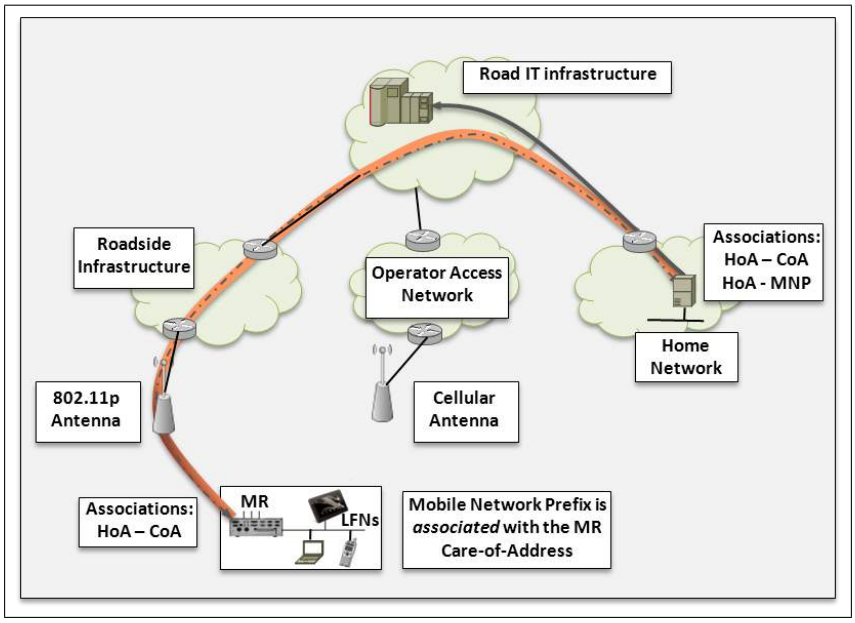
	MIPv6	PMIPv6	H-DMM	C-DMM	N-DMM-F	N-DMM-P
Category	Centralized, Host based	Centralized, Network-based	Distributed, Host-based	Distributed, Host-based	Fully Distributed, Network-based	Partially Distributed, Network-based
Granularity	Macro mobility	Micro mobility	Micro mobility	Micro mobility	Micro mobility	Micro mobility
Network compo-nents	HA	LMA, MAG	AMA	DAR	MAAR	MAR, Location database
Stack upgrade	Yes	No	Yes	Yes	Depends	No
Addr. arch.	PIA, Prefixes shared between hosts of the domain	PIA/PAA, HNP per host	PIA/PAA, Prefixes shared between hosts of the domain	PIA, CGA for hosts	PIA/PAA, HNP per host	PIA/PAA, HNP per host
Addresses per Host	2 (HoA, CoA)	1 (HNP)	1 Preffred, n-1 Deprecated (if the host traversed n AMAs)	1 CGA as HoA, n-1 CoA (if the host traversed n DARs)	1 Preffred, n-1 Deprecated (if the host traversed n MAARs)	1 Preffred, n-1 Deprecated (if the host traversed n MARs)
Control plane	BU/BA from host to HA	PBU/PBA for MAG and LMA	BU/BA for Host-AMA, ABU/ABA for AMAs	BU/BA for Host-DAR, CGA-related signaling for Host-DAR	PBU/PBA between MAARs, Possible involvement of Host	PBU/PBA between MARs, Request/Up-date for MAR-Location DB
Tunnel overhead	From Host to HA	MAG to LMA	Host to AMA, p-AMA to n-AMA	Host to DAR, p-DAR to n-DAR	p-MAAR to n-MAAR	p-MAR to n-MAR

to extend PMIPv6 and DMM with NEMO Basic Support. The reader is referred to the existing literature surveys for a more comprehensive overview on these concepts, e.g., [129] [24].

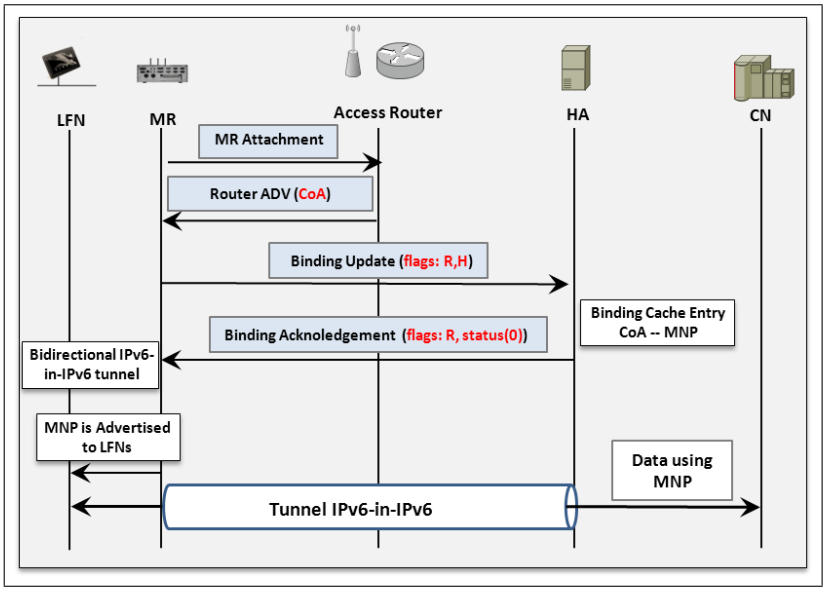
4.3.1 MIPv6 NEMO

Mobile IPv6 (MIPv6) [172] is IETF's host-based mobility management solution, which provides mobile hosts the ability to retain their home address while changing their point of attachment to the Internet. IPv6 packets addressed to the mobile node through its home address are transparently directed to its current care-of address (CoA), which is a temporary address associated to the node every time it is served by a network attachment point away from its home network.

Figure 4.6: NEMO Basic Support in Mobile IPv6.



(a) General architecture



(b) Message exchange diagram

NEMO is IETF's network-based mobility management solution. As mentioned previously, this extension to MIPv6 enables the association of a CoA to a pool of IPv6 home prefixes (the Mobile Nodes Prefixes - MNP). The basic idea behind NEMO concept is to handle the mobility

of a set of moving hosts through a unique entity, namely the MR, instead of managing each mobile host separately (i.e. deploying MIPv6 on each of them).

Figures 4.7(a) and 4.7(b) depict NEMO basic functionality. The MR connects to an access router (the 802.11p antenna in Figure 4.7(a)) that provides it with a CoA. The MR then sends a Binding Update (BU) message to its Home Agent (HA) to inform it about its new CoA. The 'R' flag in the BU is set in order to inform the HA that the BU comes from a MR. Upon reception of such BU, the HA updates its cache entries by binding the new CoA with the MNP that are owned by the MR and sends back a Binding Acknowledgment (BA) to the MR: the IPv6-to-IPv6 tunnel between the MR and the HA is created.

Now let us consider that a Correspondent Node (CN) located somewhere in the Internet wants to exchange data with a LFN. As the IPv6 address of the LFN belongs to the home network, data packets are routed to the home network. Knowing the binding between the MNP and the CoA, the HA forwards the packets to the MR through the IPv6-to-IPv6 tunnel. Upon reception, the MR decapsulates the packets and forward them to the LFN. The same steps apply in the other direction: packets sent by a LFN to a CN are encapsulated by the MR and routed to the HA that decapsulates and forward them to the CN. The encapsulation is necessary to avoid the ingress filtering of the access router that may lead to packets drop as the IPv6 source address is not topologically correct.

4.3.2 PMIPv6 NEMO

Proxy Mobile IPv6 (PMIPv6) [92] is IETF's network-based mobility management solution, where the mobile node is unaware of IP mobility. Based on MIPv6, PMIPv6 introduces a proxy that performs mobility signaling on behalf of the host. PMIP defines two new functional elements:

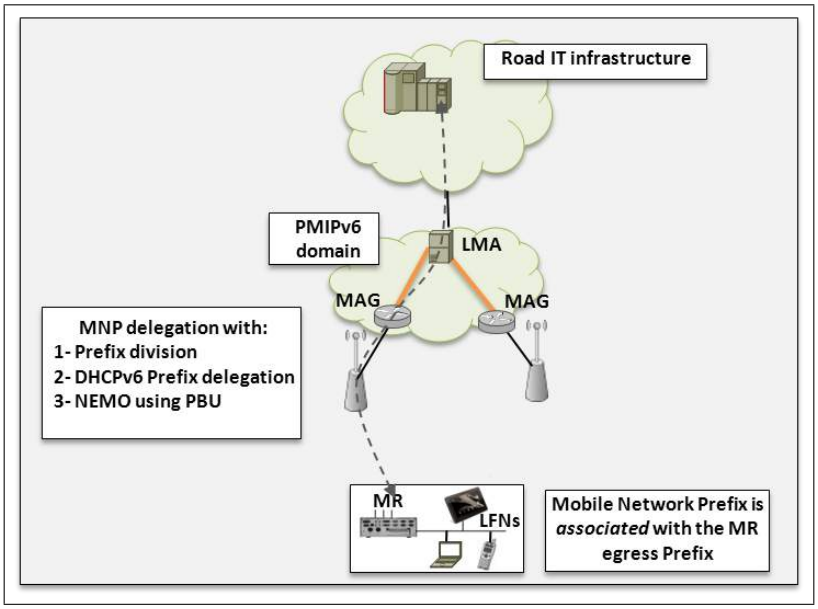
- **LMA (Local Mobility Anchor)** performs the Home Agent function of MIPv6, which provides the topological anchor point for the CoA.
- **MAG (Mobile Access Gateway)** is an access router responsible for the mobility signaling.

While in MIPv6 the fundamental mobility functionalities (anchoring, locating, and forwarding) are centralized in the HA, they are distributed in PMIPv6. The LMA handles the anchoring and manages the location database, the MAG detects the host's movements and participates in the location update operations. The forwarding is split between the LMA and the MAG. LMA and MAG build a bidirectional tunnel for the traffic of the host. When the host changes its point of attachment, the LMA and the new MAG build a new tunnel while retaining the IP connectivity for the host. The operation of PMIPv6 and the involved entities are illustrated in Figure 4.8(a).

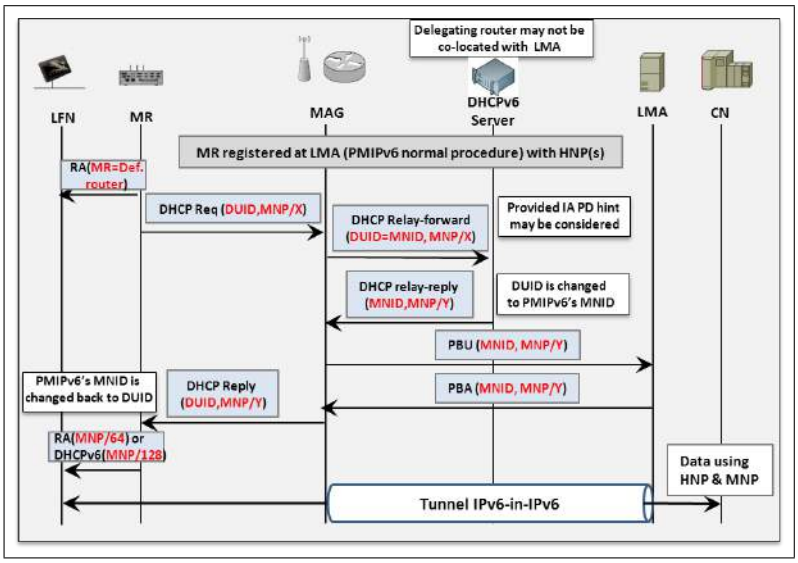
Proxy Mobile IPv6 is a protocol that was designed initially with the goal of supporting mobile nodes like end-user terminals, handsets, and smartphones. The goal was to allow such an MN to dynamically change its point of attachment by performing a hand-over between different access points. Upon attachment to a new access point, a new IPv6 address would be attributed to the MN; changing the address of the terminal would pose a significant threat to the good behavior of ongoing applications - hence a mechanism was needed that would allow MN handovers without a change in the IP address. PMIPv6 offers this feature, by dynamically changing the network routing (with tunnels) corresponding to one particular address, which moves itself together with MH.

On another hand, the protocol PMIPv6 was not designed to support groups of hosts moving together as a whole (as for the vehicle). Although PMIPv6 assigns an entire prefix to the MH

Figure 4.7: NEMO Basic Support in Proxy Mobile IPv6.



(a) General architecture



(b) Message exchange diagram

(i.e. the leftmost common 64bits of an address, the HNP "Home Network Prefix") this prefix cannot be used by nodes in the moving network to attribute an address for themselves. This HNP can be used by MH to self-configure one single address.

The lack of NEMO extension for PMIPv6 has negative implications in the case of moving networks. If we consider the typical topology of a moving network (several LFNs attached to a MR moving together), IP applications between LFN and an arbitrary CN in the Internet are not possible.

First, the LFNs do not have globally routable addresses, because only one address is delivered by PMIPv6 to MR's egress interface. Second, even if a LFN had a statically configured globally routable IP address, it would not be reachable: a CN sending a packet to that address would

be dropped at LMA, because the routing path is not set up between CN, LMA, MAG, MR and LFN. Trivial solutions to address this problem may have several problems. for example, if we consider IPv4, a NAT and DHCP may be implemented in the MR; this would offer unidirectional access from LFNs to arbitrary CNs; however, this would not offer reverse reachability from CN to LFN. Note that NAT concept is proper to IPv4 and is not defined in IPv6.

For use cases of Chapter 3, the embedded network mobility and reachability needs to be guaranteed. PMIPv6's initial design did not provide for network mobility extension. Although NEMO Basic Support and PMIPv6 could be combined, the use of two different addressing pools (Home Network and NETLMM domain) may cause unexpected service interruptions and an unnecessary control plane overhead [128].

Figure 4.8(b) illustrates a proposal for NEMO to support moving networks in PMIPv6 [175]. In detail, the proposal includes two possible and potential solutions for the lack of network mobility to PMIPv6:

- **HNP Division**: The mechanism divides the Home Network Prefix into two or more Mobile Network Prefixes (MNPs). It is assumed that in a domain running PMIPv6 the LMA assigns a Home Network Prefix (HNP) to the Mobile Host. Simply using HNP to form addresses for LFNs, without modifying MR behavior with respect to its routing table, is not sufficient. HNP division requires that the MNP be part of the HNP (e.g. MNP must have the leftmost n bits the same as the prefix length of HNP), and its length be longer. In case of an HNP/64 and the use of Ethernet for LFNs, only DHCPv6 can be used by LFNs, and not SLAAC (not possible for MNPs longer than 64, the Interface ID being of length precisely 64 for Ethernet).
- **Enhancing DHCPv6-PD and PMIPv6**: A second mechanism, alternative to HNP Division, considers the use of MNP different than HNP. With HNP Division, the HNP and MNP necessarily have a common set of leftmost leading bits. But with this method, HNP and MNP may differ at the leftmost bit. This has an immediate advantageous consequence: it allows the use of SLAAC with Ethernet LFNs even when the HNP is of length 64. The inconvenient is that the PMIPv6 must be modified; this mechanism involves also the use of the DHCPv6 Prefix Delegation protocol, which may be considered as an additional burden. In our proposal, we make use of the RFC 3633 Prefix Delegation option of DHCPv6 (Figure 4.8(b)). The MAG is then a DHCPv6-relay that intercepts the request of the MR, changes its DUID by the MR's MNID and forwards the request to the DHCPv6 Server. Upon receiving the requested prefix the LMA is notified (PBU/PBA exchange) of the allocated prefix. This newly allocated prefix is then associated with the MR's MNID and its mobility managed.

A similar proposal is now standardized by the IETF within the NETEXT Working Group [222].

4.3.3 DMM NEMO

At the time of writing, the IETF's within its DMM WG has not reached a consensus on the approach to adopt for a standardized distributed mobility management solution (client- or network-based). Some of the proposals we described earlier, C-DMM [88], H-DMM [122], N-DMM-F [123], and N-DMM-P [87] are discussed within the DMM WG and other similar Internet-drafts can be found [19] [20]. It is then expected not to find any standard candidate for NEMO in DMM, as usually it is proposed as an extensions for an existing standard (MIPv6 or PMIPv6, for instance). However, the literature proposes two non-standard approaches to solve network mobility for mobile networks. Figure 4.10(a) illustrates the architecture behind NEMO in DMM.

4.3.3.1 Recent trends for DMM NEMO

Very recently, authors of [66] proposed a network-based nemo extension in DMM. The proposed Network-based DMM architecture reuses functionalities existing within PMIPv6 and similar to N-DMM-P approach. The noticeable difference resides within the distribution of the location database over the network, with each anchor having a local location database (quid of the mobility information coherence). In this proposal, the HNP allocation is the responsibility of the Location Management (LM) servers. The NEMO prefixes are also delegated through LMs (delegating function) when the MR requests an HNP for its attached devices. This is a major difference when compared to previous DMM approaches (host-based and network-based alike) as they rely solely on MAR for the prefix allocation and the location database to handle the mobility context only; i.e. which Mobile Node has been given which HNP at which anchoring point. Also, in this approach, the authors rely on the routing management entity (a gateway, the forwarding entity in their model) to associate the MR with the serving MAG (responsible of detecting the moving network and forward the data, similarly to PMIPv6). Figure 4.8 summarizes the control plane of NEMO when the MR performs a handover from p-RM to n-RM, as proposed by the authors.

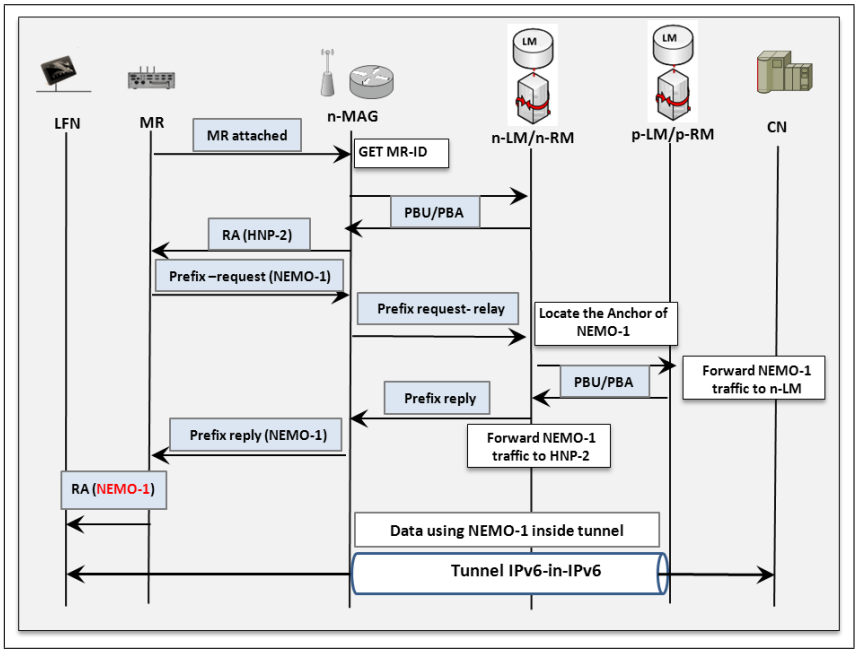


Figure 4.8: NEMO handover signaling flow for non-nested MR.

When the MR makes a handover from p-MAG to n-MAG, it is configured with a new HNP (HNP-2) for its egress interface (PBU/PBA exchange with n-RM, bidirectional tunnel established). The MR then sends a request to the n-MAG to maintain the mobility of prefix NEMO-1 obtained at p-MAG for its attached devices. The n-MAG forwards this request to the n-RM (Prefix-request). The n-LM indicates to the n-RM that the NEMO-1 prefix was delegated through p-LM. The n-RM will then perform a PBU/PBA exchange with the p-RM (and establish a bidirectional tunnel) to register this new status for the NEMO-1 prefix. The Prefix-reply is then sent from the n-RM to n-MAG, and eventually to the MR. The network mobility is now maintained for NEMO-1. The data path is anchored at p-RM, n-RM and n-MAG. The data encapsulation ends at the MAG (no tunnel over the MR's wireless link). The authors do not specify how the n-LM knows that p-LM was the one delivering NEMO-1 and p-RM the previous

anchor for this prefix.

Another recent non-standard proposal for DMM NEMO is currently ongoing at the IETF [53]. This approach differs from the previous as the authors assume a flattened distributed architecture with one location database, whereas the first architecture assumed a hierarchical architecture with distributed location database function. This difference has an impact on the control plane. Indeed, when the MR changes its point of attachment from p-MAR to n-MAR, the n-MAR allocates a new HNP (HNP-2) and a new mobile prefix (NEMO-2). The n-MAR when updating the mobility context at Location database, will extract the address of p-MAR. The n-MAR exchanges PBU/PBA messages with p-MAR to update the forwarding plane for HNP-1 and NEMO-1 prefixes. The data flow to NEMO-1 will now go to p-MAR, tunneled to n-MAR, tunneled to MR and then decapsulated before reaching the mobile nodes. Another difference with the previous approach, the MR in this draft (called Proxy Router - PR) declares the identities of his attaches nodes (RFC 4283 MNID option) to its serving MAR. This has the advantage of letting the mobile nodes independent from their MR and capable of continuing their data traffic if they perform a handover from the PR to their serving MAR. The Location database in this case tracks the status of the MNs as individual hosts and the PR as a group of hosts and associates then with their respective HNP and NEMO prefixes.

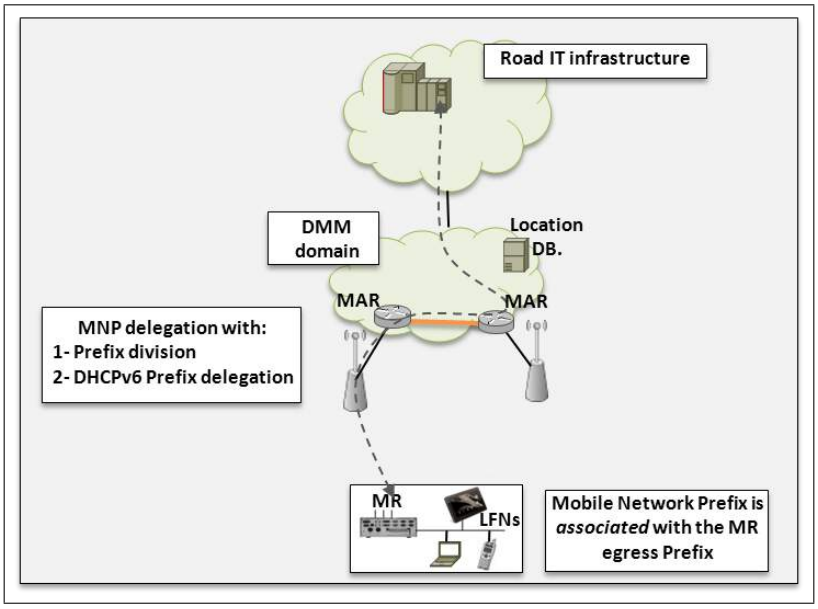
4.3.3.2 Proposal for DMM NEMO

In this section we reuse the two techniques proposed for PMIPv6 in the context of DMM: HNP division and enhanced DHCPv6-PD. As for the reference architecture, we take the Network-based DMM partially distributed (N-DMM-P) architecture. Four actors exist in this architecture. (1) The MAR has similar responsibilities as in the original N-DMM-P architecture. In addition to anchoring and handling the mobility on the behalf of the MNs and MRs, it handles also the addresses and the prefixes allocation. It is then natural to involve the AR into the NEMO delegation. (2) The Location database maintains a coherent state of the mobility context for each MN and MR in the network. It must be updated if any change to the anchoring or the delegation occurs to any of the nodes in the domain. (3) The Mobile Router (MR) is a generalization of the Mobile Node entity. It requests along its usual HNP (for the outgoing traffic) an additional prefix (MNP) for its attached devices. The mobility of this prefix must be guaranteed when the MR makes a handover from one attachment point to another. (4) Locally Fixed Nodes (LFNs) are attached to the MR and fixed in the network. In a vehicle for instance, the LFNs would be the machines and devices inside the vehicle connecting through the MR to the network. Our proposal based on DHCPv6 is illustrated in Figure 4.10(b).

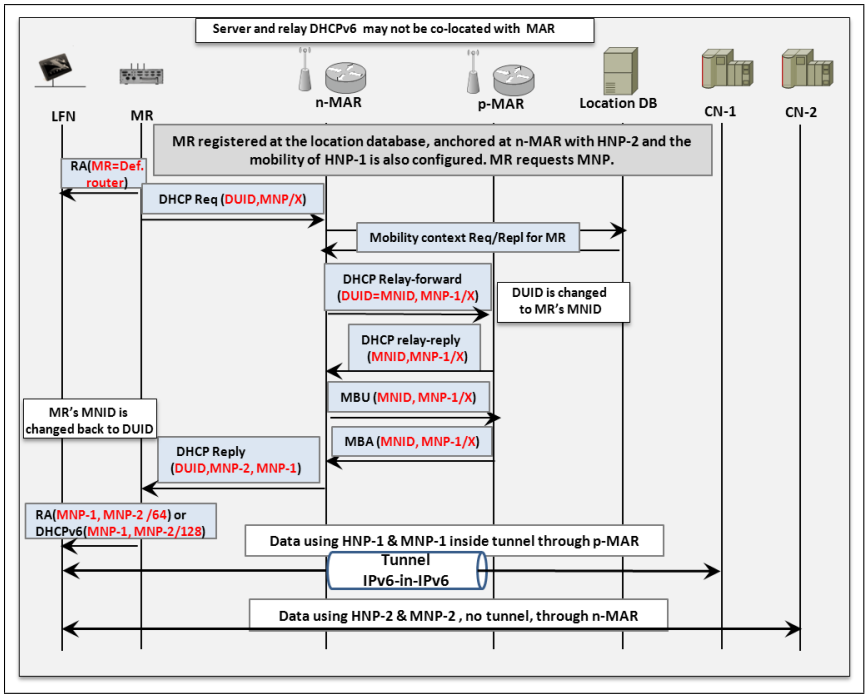
Using this architecture, the four actors behave as described in the following in our proposals:

- **HNP Division**: The mechanism divides the Home Network Prefix into two or more Mobile Network Prefixes. As described in the PMIPv6 case, this approach requires that the MNP is an extract of the announced HNP (MNP must have the leftmost n bits the same as the prefix length of HNP), and its length be longer. The MR by setting a flag in the RS message sent to the MAR in the first attachment, warns it that the delegated HNP prefix should be longer (48 bits, for example). At the reception of this message, the MAR fetches the MR's mobility context at the location database using its MNID option. In a moving vehicle, the MR can use the VIN as its MNID as explained in Chapter 3. If the MR has not already attached to the network, the location database will not deliver any previous HNP at other locations. The MAR will then allocate a new HNP (HNP-1) of the desired length and announce it to the MR (RA message). The MAR will then notify the location database of this change. At the reception of this HNP, the MR will extract a

Figure 4.9: NEMO Basic Support in Network-based Distributed Mobility Management.



(a) General architecture



(b) Message exchange diagram

HNP-1/64 prefix for its egress interface and announces the other 64bit long prefixes inside the vehicle. LFNs are now capable of auto-configuring their home addresses using SLAAC.

When the vehicle moves and the MR attaches to a new MAR, a handover must occur. The MR will warn the n-MAR of being a router through a flag put in the RS message. The n-MAR will query the location database for the mobility context of the MR and will receive information about p-MAR and HNP-1. The n-MAR will then perform a

MBU/MBA messages exchange with p-MAR to install a bidirectional tunnel for HNP-1 related traffic session continuity. The n-MAR will now allocate a new prefix, HNP-2 of the desired length, and announce the prefixes HNP-2 (with status preferred) and HNP-1 (with status deprecated) to the MR in a RA message. The MR will now divide the HNP-2 and HNP-1 for his egress interface and attached LFNs needs. The HNP-1 related traffic will now flow through p-MAR to n-MAR (tunneled traffic) and then decapsulated before being delivered to the MR and its LFNs. No tunnel over the wireless link is required in this approach. The location database is also notified of this mobility context change for the MR.

- **Enhancing DHCPv6-PD and N-DMM-P**: As an alternative to HNP Division, let us consider the use of an MNP which is different from the HNP. This has an immediate advantageous consequence: it allows the use of SLAAC with Ethernet LFNs even when the HNP is of length 64. The inconvenient is that the N-DMM-P must be modified to include a control plane which is compatible with DHPCv6-PD. In our proposal, we make use of the RFC 3633 Prefix Delegation option of DHCPv6. The MAR has now two additional functionalities: DHCPv6-relay and DHCPv6-server. As supposed earlier, the delegation functionality is co-located with the anchoring point (the MAR), but our proposal works the same if the DHCPv6 server is a separate network entity.

  In our approach, after the MR is configured with its HNP, it send a DHCPv6-PD request message for an MNP of length X to its serving MAR. If the location database record that describes the mobility context of the MR does not contain a previous MNP, the serving MAR sends a DHCPv6-PD reply with a MNP (MNP-1) to announce inside the MR's network for the LFNs. If the MR has already been attached to a previous MAR with a MNP anchored there, the n-MAR has to relay its DHCPv6-PD request to the p-MAR. The n-MAR retrieves the p-MAR's address from the mobility context of the location database. If the DHCPv6-PD reply is positive, the n-MAR sends an MBU message and receives an MBA to confirm the bidirectional tunnel configuration to handle the data flow for this MNP (MNP-1). The n-MAR will now send a DHCPv6-PD reply containing both MNP-2 (with status preferred) and MNP-1 (with status deprecated). The location database is also notified to track these changes. It worthy of mention that the HNP portability from p-MAR to n-MAR for this MR is handled in the same way as described for simple hosts and happen before the NEMO phase. Also, during the DHCPv6-PD control plane, the requests/replies are intercepted by the MARs and the contained DUID changed accordingly.

Our approaches differ from the first DMM NEMO proposal by the architecture. When we chose a centralized location database and a flattened mobility architecture, the authors of the first proposal provide a hierarchical mobility management approach with a distributed location database. We also co-locate our address/prefix delegating entity with the MAR rather than the location database, and thus cleanly separate the network functionalities. In comparison to the second proposal (draft), our architectures are similar, but our approaches are not proposed by the authors of the draft. Also, our MR is not a proxy router, meaning that the LFNs attached to the MR are not "declared" to the location database. If a MN chose to make a handover from the MR to its serving MAR, the MN would not be able to request for the portability of its prefix (MNP), as this prefix belongs (associated) to the MR.

Table 4.4: Features summary comparison of NEMO BS in MIPv6, PMIPv6 and DMM

	Control plane	NEMO support method	Standard	Addressing	Routing optimization
NEMO in MIPv6	Signaling messages involve the MR	MNP association to the HoA of the MR, MNP included in th BA	Mature and experimented on deployments	Implicit (HA associates the MR with its MNP) and Explicit (MNP sent in the BU)	Experimental, solutions exist [32]
NEMO in PMIPv6	Transparent to the MR, handled in the core	HNP division, DHCPv6-PD and PBU/PBA extensions	Recently standardized, not yet deployed	HNP division and Explicit DHCPv6 requests	Not yet addressed
NEMO in DMM	Network-based, transparent to the MR	HNP division, DHCPv6-PD and MBU/MBA extensions, other	Not standard, not deployed	HNP division and Explicit DHCPv6 requests, other	Not yet addressed

4.4 Analysis of the solutions

In this section, we analyze the use of NEMO in Centralized and Distributed mobility management proposals. In particular, MIPv6, PMIPv6, and N-DMM-P with their NEMO extensions are compared. Note that no Routing Optimization schemes are considered in our study. Table 4.5 sums up the notations used in our model.

4.4.1 Considered scenarios

To compare the efficiency of MIPv6-NEMO, with the proposed NEMO techniques (prefix division and Prefix delegation) in PMIPv6 and N-DMM-P, we consider the network topologies illustrated in figures 4.7(a) 4.8(a), and 4.10(a) respectively. We suppose that the MR attaches to the network through a wireless antenna and attempts to configure its internal network (embedded LFNs) with each of the compared configuration techniques. To make the comparison fair, we make the following assumptions:

- $H^{CN}_{LMA} = H^{CN}_{HA} = H^{CN}_{MAR}$. The CN is at the same distance from the LMA, HA, and the first MAR the MR attaches to.
- T_{L2} and T_{AU} are the same in the proposed protocols. That is; the link-layer processing and the authentication process are of the same duration (reasonable assumption regarding the standards).
- M^{d}_{LFN} the LFN data packet size is the same in the proposed scenarios. Note that an additional IPv6-in-IPv6 encapsulation tunnel may be added depending on the proposal.

Note that for the Router Advertisement messages, we took into consideration the recommendations of High Mobility scenarios when deciding of the minimum and maximum advertisement timers of RFC 6275.

4.4.2 Performance metrics

In this analytical study, we are interested in the following performance metrics:

1. Signaling cost: It is the cost of location update signaling as well address configuration when traversing new cells and obtaining new addressing configurations.
2. Addressing configuration delay: It is the time that starts from MR doing a Layer 2 handover and finishes when this MR receives its MNP configuration.
3. End-to-end delay: It is the time for a user packet (sent by the LFN) to reach the other end (CN).
4. Tunnel usage: It is the ratio of sessions making use of tunnels to the total number of sessions. This is to highlight the importance of prefix anchoring and dynamic tunnel establishment in DMM.

4.4.3 Host mobility model

In order to measure the above metrics, we need to take into account the handover frequency, which is the main cause of signaling in the mobility architectures[5]. Based on the model in [142], for this purpose, we make use of the Session-to-Mobility Ratio (SMR) defined as the relative ratio of sessions arrival rate (new applications/packets) to the user mobility rate. The user mobility rate can be quantified using the *subnet border crossing rate* (μ_{cr}) or the *subnet residence time* ($\eta = 1/\mu_{cr}$). We also take these additional assumptions to simplify the calculations later [86]:

- The subnet residence time (in the MIPv6's AR, PMIPv6's MAG, or DMM's MAR) follows an exponential distribution with parameter η.
- The data session duration (at the MR's connected network) also follows an exponential distribution with parameter λ.
- The subnets (or coverage cells) have a circular coverage defined with Radius R_{SN}.
- The vehicle travels with a subnet (or cell) with a direction uniformly distributed in $[0, 2\pi)$ and average speed $\overline{v}$.

Using these notations, we define:

$$\mu_{cr} = \frac{2\overline{v}}{\pi R_{SN}}, \eta = \frac{1}{\mu_{cr}} \tag{4.1a}$$

$$SMR = \rho = \frac{\lambda}{\eta} \tag{4.1b}$$

[5]Note that in the PMIPv6 standard [92], before the expiry of the lifetime associated to the binding cache of a Mobile Node, the MAG checks whether the mobile node is still present on the link. On possible procedure is the use of Neighbor solicitation/Neighbor advertisement messages. This of course introduces additional control plane messages.

Assuming the mobility domains have N cells, intra-domain cell crossing triggers an intra-domain handover procedure and inter-domain cell crossing triggers an inter-domain handover procedure. We have the intra-domain and inter-domain handover probability and expected numbers of handovers as:

$$P_{intra} = \frac{1}{1+\rho}, P_{inter} = \frac{1}{1+\rho\sqrt{N}} \tag{4.2a}$$

$$E_{intra} = \frac{1}{\rho}, E_{inter} = \frac{1}{\rho\sqrt{N}} \tag{4.2b}$$

4.4.4 Modeling for total signaling cost

Maintaining an up-to-date binding at the Location database is of paramount importance for Mobile Hosts in any mobility solution. Throughout its journey across the mobility domain, the MR will trigger configuration and mobility related control messages. In order to assess the cost of the configuration and maintaining the MR's mobility session up to date, we analyze the cost of the solutions of which the message exchange diagram is illustrated in Figures 4.7(b), 4.8(b), and 4.10(b). This signaling load can be expressed as:

$$C^{total} = (E_{intra} - E_{inter}) \times C_{intra} + E_{inter} \times C_{inter} \tag{4.3}$$

Where C_{intra} and C_{inter} are the costs of signaling update for handovers occurring inside and outside the mobility domain. We now define the costs in Equation 4.3 in each use case.

4.4.4.1 MIPv6 NEMO

In the MIPv6-NEMO solution, the messages exchanged between the MR and the HA are the same if the MR is in one of HA's controlled cells or the MR is registered at another domain: the MR needs to get its global CoA then registers its binding at its HA in its origin domain. The configuration of a CoA needs a movement detection at layer 2, and authentication of the MR's interface, a Router Advertisement message reception and sending Neighbor Solicitation message in the Duplicate Address Detection process. After configuring a proper global CoA, the MR needs to register its new binding at the HA in order to map it to its HoA and MNP prefix. The HA supports N_{MR} vehicles in its domain and stores their binding in a tree-based data structure with O(Log n) update, lookup, and delete operations complexity. This leads to the below equations 4.4. We suppose that the movement detection at layer 2, and authentication of the MR's interface are the same for every protocol, and thus ignored in our cost analysis here.

$$C_{intra}^{MIPv6-NEMO} = C_{inter}^{MIPv6-NEMO} = C_{AC} + C_{reg} \tag{4.4a}$$

$$C_{AC} = M_{RA}^{c} + M_{NS}^{c} \tag{4.4b}$$

$$C_{reg} = 2 \times (M_{BU}^{c} \times H_{AR}^{HA}) + C_u \tag{4.4c}$$

$$C_u = \alpha \times \log(N_{MR}) \tag{4.4d}$$

4.4.4.2 PMIPv6 NEMO with Prefix division

In the PMIPv6 NEMO through Prefix division solution, the messages exchanged between the MR and the MAG in the address configuration part are the same as in MIPv6-NEMO, except the MR configures the Home Network Prefix instead of a temporary address. The MR's binding at the LMA is also updated through PBU/PBA messages exchanged between the MAG and the

LMA. The LMA supports N_{MR} vehicles in its domain and stores their binding in a tree-based data structure with O(Log n) update, lookup, and delete operations complexity. In the inter-domain handover, we assume an control plane between the p-LMA and the n-LMA consisting in 2 PBU/PBA messages to notify the previous LMA of the presence of MR in a new domain. This leads to the below equations 4.5.

$$C_{intra}^{PMIPv6-NEMO} = C_{AC} + C_{reg} \tag{4.5a}$$
$$C_{inter}^{PMIPv6-NEMO} = C_{AC} + C_{reg} + C_{reg}^{inter} \tag{4.5b}$$
$$C_{AC} = M_{RA}^{c} + M_{NS}^{c} \tag{4.5c}$$
$$C_{reg} = 2 \times (M_{PBU}^{c} \times H_{MAG}^{LMA}) + C_u \tag{4.5d}$$
$$C_{reg}^{inter} = 2 \times (M_{PBU}^{c} \times H_{LMA-2}^{LMA-1}) + C_u \tag{4.5e}$$
$$C_u = \alpha \times \log(N_{MR}) \tag{4.5f}$$

4.4.4.3 PMIPv6 NEMO with Prefix delegation

In the PMIPv6 NEMO through Prefix delegation solution, the MR has to explicitly ask for a new MNP prefix to its LFNs from the MAG. While the configuration and registration is the same as in the Prefix division based solution, the prefix delegation involves a DHCPv6 server that we suppose architecturally co-located with the LMA. Here also, the location database and the DHCPv6 delegated prefixes database are handled with an O(Log n) operation cost based data structure (with different factors). The inter-domain handover needs a PBU/PBA registration from n-LMA to p-LMA and the MNP portability (prefix delegation) is also forwarded from n-LMA to p-LMA to preserve the session continuity of the MR's LFNs.

$$C_{intra}^{PMIPv6-NEMO} = C_{AC} + C_{reg} + C_{pdel} \tag{4.6a}$$
$$C_{inter}^{PMIPv6-NEMO} = C_{AC} + C_{reg} + C_{reg}^{inter} + C_{pdel}^{inter} \tag{4.6b}$$

$$C_{AC} = M_{RA}^{c} + M_{NS}^{c} \tag{4.6c}$$
$$C_{reg} = 2 \times (M_{PBU}^{c} \times H_{MAG}^{LMA}) + C_u \tag{4.6d}$$

$$C_{pdel} = 2 \times M_{DHCPv6-PD}^{c} + 2 \times (M_{DHCPv6-PD}^{c} \times H_{MAG}^{LMA}) + 2 \times (M_{PBU}^{c} \times H_{MAG}^{LMA}) + C_{pdel} \tag{4.6e}$$

$$C_{reg}^{inter} = 2 \times (M_{PBU}^{c} \times H_{LMA-2}^{LMA-1}) + C_u \tag{4.6f}$$

$$C_{pdel}^{inter} = 2 \times M_{DHCPv6-PD}^{c} + 2 \times (M_{DHCPv6-PD}^{c} \times H_{MAG}^{LMA}) + 2 \times (M_{DHCPv6-PD}^{c} \times H_{LMA-2}^{LMA-1}) + 2 \times (M_{PBU}^{c} \times H_{MAG}^{LMA}) + C_{pdel} \tag{4.6g}$$

$$C_u = \alpha \times \log(N_{MR}) \tag{4.6h}$$
$$C_{pdel} = \beta \times \log(N_{MR}) \tag{4.6i}$$

4.4.4.4 N-DMM-P NEMO with Prefix division

Similarly to the PMIPv6 NEMO through Prefix division solution, the messages exchanged between the MR and the MAR in the address configuration part consists in Router advertisement and Neighbor solicitation messages. The MR also configures a Home Network Prefix anchored at the MAR it just entered. The MAR updates the MR's binding at the Location database that handles $N_{MD} \times N_{MR}$ vehicles binding in a tree-based data structure with O(Log n) operations cost. In the inter-domain handover, the n-MAR assures the portability of MR's previous prefix by contacting the p-MAR. This leads to the below equations 4.7.

$$C_{intra}^{DMM-NEMO} = C_{AC} + C_{Update} \tag{4.7a}$$
$$C_{inter}^{DMM-NEMO} = C_{AC} + C_{Update} + C_{reg}^{inter} \tag{4.7b}$$
$$C_{AC} = M_{RA}^{c} + M_{NS}^{c} \tag{4.7c}$$
$$C_{Update} = 2 \times (M_{MOB}^{c} \times H_{LDB}^{MAR}) + C_u \tag{4.7d}$$
$$C_{reg}^{inter} = 2 \times (M_{MBU}^{c} \times H_{n-MAR}^{p-MAR}) \tag{4.7e}$$
$$C_u = \alpha \times \log(N_{MD} \times N_{MR}) \tag{4.7f}$$

4.4.4.5 N-DMM-P NEMO with Prefix delegation

The address configuration, Location database registration and session continuity for the MR's HNP is similar to previous DMM-NEMO scheme. The prefix delegation based on DHCPv6 prefix delegation messages involves interactions with the DHCPv6 server co-located with the MAR. Same assumptions about data structure operations cost are valid in this approach.

$$C_{intra}^{DMM-NEMO} = C_{AC} + C_{Update} + C_{pdel} \tag{4.8a}$$
$$C_{inter}^{DMM-NEMO} = C_{AC} + C_{Update} + C_{reg}^{inter} + C_{pdel}^{inter} \tag{4.8b}$$

$$C_{AC} = M_{RA}^{c} + M_{NS}^{c} \tag{4.8c}$$
$$C_{Update} = 2 \times (M_{MOB}^{c} \times H_{LDB}^{MAR}) + C_u \tag{4.8d}$$
$$C_{pdel} = 2 \times M_{DHCPv6-PD}^{c} + 2 \times (M_{MOB}^{c} \times H_{LDB}^{MAR}) + C_{pdel} \tag{4.8e}$$
$$C_{reg}^{inter} = 2 \times (M_{MBU}^{c} \times H_{n-MAR}^{p-MAR}) \tag{4.8f}$$

$$\begin{aligned} C_{pdel}^{inter} = {} & 2 \times M_{DHCPv6-PD}^{c} + \\ & 2 \times (M_{MOB}^{c} \times H_{LDB}^{MAR}) + 2 \times (M_{DHCPv6-PD}^{c} \times H_{n-MAR}^{p-MAR}) + \\ & 2 \times (M_{MBU}^{c} \times H_{n-MAR}^{p-MAR}) + C_{pdel} \end{aligned} \tag{4.8g}$$

$$C_u = \alpha \times \log(N_{MD} \times N_{MR}) \tag{4.8h}$$
$$C_{pdel} = \beta \times \log(N_{MD} \times N_{MR}) \tag{4.8i}$$

Figure 4.10 shows the overall signaling cost as function of the session-to-mobility ratio (SMR or ρ). When the SMR is small, the mobility rate is larger than the session arrival (actual communications). In this case, the signaling due to the MR changing its point of attachment (i.e.

the binding updates) is higher. However, when the $SMR > 1$; that is, the session arrival rate is larger than the mobility rate, the overall mobility-related signaling decreases as the consequence of the less frequent subnet changes of the MR. The approach which induces the most signaling overhead in our comparison is PMIPv6-NEMO through prefix delegation, and the lowest is the DMM-NEMO through prefix division. For instance, when the $SMR = 1$ (mobility-related signaling is the highest), the PMIPv6-NEMO PD approach induces 42.73% higher signaling load than MIPv6-NEMO, 53.12% higher load than DMM-NEMO PD, 74.68% higher load than PMIPv6-NEMO Div, and 79.46% higher than DMM-NEMO Div. This tendency remains accurate when the $SMR > 1$; that is the previous order is the same. The PMIPv6-NEMO PD and DMM-NEMO PD use the DHCPv6 prefix delegation control plane, which induces higher latency and more message exchanges between the entities involved. The MIPv6-NEMO in our proposal is comparable to PMIPv6-NEMO Div and DMM-NEMO Div in terms of message exchanges (no DHCPv6 server involved). Still, MIPv6-NEMO has higher signaling load than the latter two approaches due to its central anchor (the HA) even in case of domain change. The DMM-NEMO Div has the lowest signaling which is due to a flattened architecture when compared to PMIP-NEMO Div.

Noteworthy of mention, those results are closely tied to our solutions, in particular to the messages exchanged between entities and the entities location. For example, the results can differ if the MIPv6-NEMO requires a DHCPv6 server (hence more control overhead), or if the DHCPv6 server is not co-located with the LMA and MAR respectively.

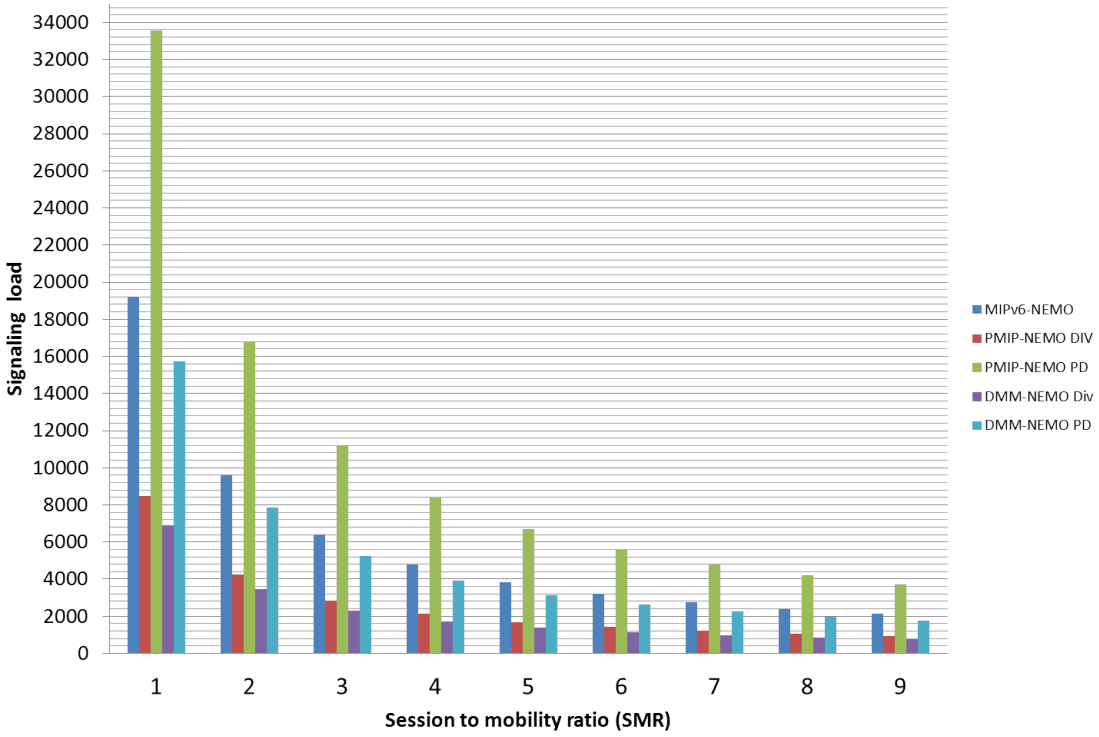


Figure 4.10: Impact of the session-to-mobility ratio on the total signaling cost for MIPv6-NEMO, PMIPv6-NEMO, and DMM-NEMO.

4.4.5 Modeling for addressing configuration delay

Using the border crossing probabilities in Equations 4.2, we define the total address configuration delay as:

$$T^{total} = (P_{intra} - P_{inter}) \times T_{intra} + P_{inter} \times T_{inter} \tag{4.9}$$

The configuration delay depends on the bandwidth, the propagation delay, the distance between and the control messages involving the MR and its mobility architecture components.

4.4.5.1 MIPv6 NEMO

Figure 4.11 shows the time diagram for address configuration in the case of MIPv6-NEMO. The process starts with a Link-layer handover and ends with the MR receiving its MNP from the HA. The process is decomposed into a CoA configuration and a Binding at the HA as follows:

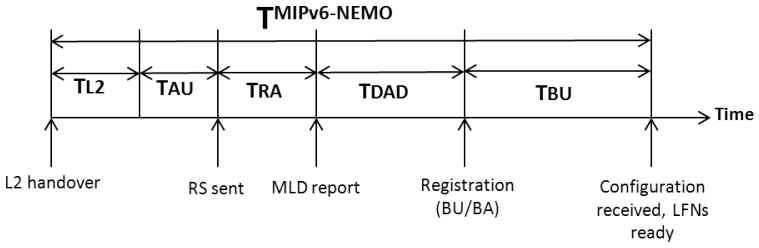


Figure 4.11: Time diagram for the Addressing Configuration Delay in MIPv6-NEMO.

$$T_{intra}^{MIPv6-NEMO} = T_{inter}^{MIPv6-NEMO} = T_{CoA} + T_{BU} + T_{BA} \tag{4.10}$$

In order to express T_{CoA}, we need to find T_{RA}: the average duration spent between the moment an MR enters a new area and the moment it receives the Router Advertisement to configure its CoA. An expression of the average T_{RA} is [95]:

$$T_{RA} = \frac{T_{RA_{max}}^2 + T_{RA_{min}}^2 + T_{RA_{max}} \times T_{RA_{min}}}{3 \times (T_{RA_{max}} + T_{RA_{min}})} \tag{4.11}$$

The CoA configuration time is then defined as:

$$T_{CoA} = T_{L2} + T_{AU} + T_{RA} + T_{DAD} \tag{4.12}$$

The Binding update on the other hand depends on the size of the control message and the bandwidth and is expressed as follows:

$$T_{BU} = T_{BA} = (\frac{M_{BU}^C}{B_{V2I}} + R_{V2I}) + H_{AR}^{HA} \times (\frac{M_{BU}^C}{B_f} + R_f) + T_u \tag{4.13}$$

Equations of 4.10 are now fully defined using equations 4.11, 4.12, and 4.13

4.4.5.2 PMIPv6 NEMO

Figure 4.12 shows the timeline for address configuration in PMIPv6. We have the Equations in 4.14. The control plane to obtain an HNP for a MR in PMIPv6 is the same as obtaining a CoA in MIPv6, in addition to a PBU/PBA exchange between the MAG and the LMA. If the PMIPv6 NEMO-Div scheme is used, the NEMO process stops here. If the PMIPv6 NEMO-PD

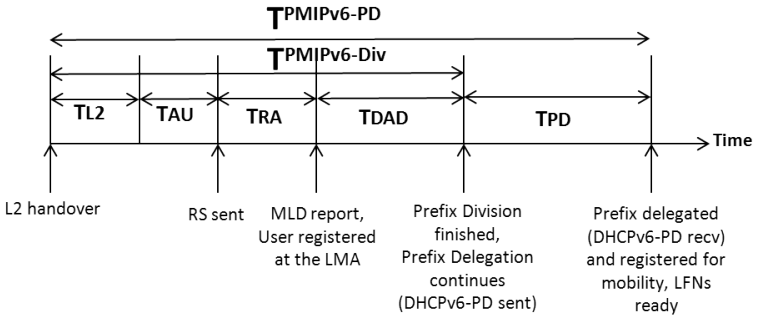


Figure 4.12: Time diagram for the Addressing Configuration Delay in PMIPv6-NEMO.

is used additional DHCPv6 messages have to be exchanged between the MR, MAG and LMA as detailed in Figure 4.8(b). If the MR roams to a new PMIPv6 domain, the new LMA and the previous LMA exchange also PBU/PBA messages to retrieve the mobility context for this MR.

$$T_{intra}^{PMIPv6-NEMO} = T_{HNP} + T_{PD} \tag{4.14a}$$

$$T_{inter}^{PMIPv6-NEMO} = T_{HNP} + T_{reg}^{inter} + T_{PD}^{inter} \tag{4.14b}$$

Where:

$$T_{HNP} = T_{L2} + T_{AU} + T_{RA} + T_{DAD} + 2 \times H_{MAG}^{LMA} \times (\frac{M_{PBU}^{C}}{B_f} + R_f) + T_u \tag{4.15a}$$

$$T_{PD} = 0, \text{ For the PMIPv6 NEMO-Div scheme} \tag{4.15b}$$

$$T_{PD} = 2 \times (\frac{M_{DHCPv6}^{C}}{B_{V2I}} + R_{V2I}) + 2 \times H_{MAG}^{LMA} \times ((\frac{M_{DHCPv6}^{C}}{B_f} + R_f) + (\frac{M_{PBU}^{C}}{B_f} + R_f)) + T_u, \text{ For the PMIPv6 NEMO-PD scheme} \tag{4.15c}$$

And:

$$T_{reg}^{inter} = 2 \times H_{LMA-2}^{LMA-1} \times (\frac{M_{PBU}^{C}}{B_f} + R_f) + T_u \tag{4.16a}$$

$$T_{PD}^{inter} = 0, \text{ For the PMIPv6 NEMO-Div scheme} \tag{4.16b}$$

$$T_{PD}^{inter} = T_{PD} + 2 \times H_{LMA-2}^{LMA-1} \times (\frac{M_{DHCPv6}^{C}}{B_f} + R_f) + T_u, \text{ For the PMIPv6 NEMO-PD scheme} \tag{4.16c}$$

4.4.5.3 N-DMM-P NEMO

Figure 4.13 shows the timeline for address configuration and prefix delegation in N-DMM-P. We have the Equations in 4.17. The control plane to obtain an HNP for a MR in N-DMM-P is the same as obtaining a CoA in MIPv6, in addition to a the exchange between the MAR and the Location DB to store this new binding. If the DMM NEMO-Div scheme is used, the

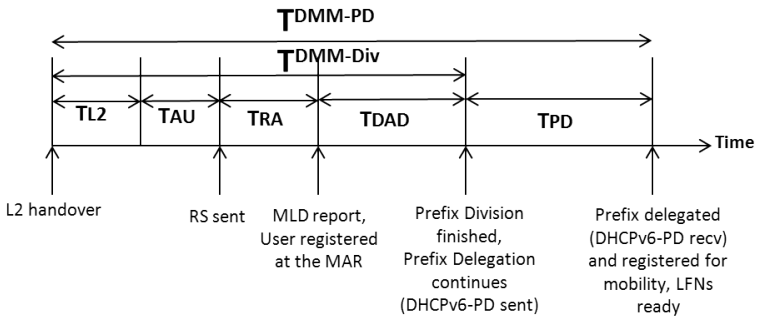


Figure 4.13: Time diagram for the Addressing Configuration Delay in DMM-NEMO.

NEMO process stops here. If the DMM NEMO-PD is used additional DHCPv6 messages have to be exchanged between the MR and n-MAR (and possibly p-MAR) and LMA as detailed in Figure 4.10(b). If the MR roams to a new DMM domain, the new MAR and the previous MAR exchange also MBU/MBA messages to anchor the mobile prefixes. The mobility context for this MR is stored at the Location DB and has to be updated when changes occur.

$$T_{intra}^{DMM-NEMO} = T_{AC} + T_{Update} + T_{PD} \tag{4.17a}$$

$$T_{inter}^{DMM-NEMO} = T_{AC} + T_{Update} + T_{reg}^{inter} + T_{PD}^{inter} \tag{4.17b}$$

Where:

$$T_{AC} = T_{L2} + T_{AU} + T_{RA} + T_{DAD} \tag{4.18a}$$

$$T_{Update} = 2 \times H_{MAR}^{LDB} \times (\frac{M_{MOB}^{C}}{B_f} + R_f) + T_u \tag{4.18b}$$

$$T_{PD} = 0, \text{ For the DMM NEMO-Div scheme} \tag{4.18c}$$

$$T_{PD} = 2 \times (\frac{M_{DHCPv6}^{C}}{B_{V2I}} + R_{V2I}) + 2 \times H_{MAR}^{LDB} \times (\frac{M_{MOB}^{C}}{B_f} + R_f) + T_u, \text{ For the DMM NEMO-PD scheme} \tag{4.18d}$$

And:

$$T_{reg}^{inter} = 2 \times H_{p-MAR}^{n-MAR} \times (\frac{M_{MBU}^{C}}{B_f} + R_f) \tag{4.19a}$$

$$T_{PD}^{inter} = 0, \text{ For the DMM NEMO-Div scheme} \tag{4.19b}$$

$$T_{PD}^{inter} = 2 \times (\frac{M_{DHCPv6}^{C}}{B_{V2I}} + R_{V2I}) + 2 \times H_{p-MAR}^{n-MAR} \times ((\frac{M_{DHCPv6}^{C}}{B_f} + R_f) + (\frac{M_{MBU}^{C}}{B_f} + R_f)) + 2 \times H_{n-MAR}^{LDB} \times (\frac{M_{MOB}^{C}}{B_f} + R_f) + T_u, \text{, For the DMM NEMO-PD scheme} \tag{4.19c}$$

Figure 4.14 shows the address configuration as function of the session-to-mobility ratio. When the SMR is small, address configuration delay is higher due to the signaling induced by the MR as it changes its point of attachment more frequently. However, as the SMR increases; that is, the session arrival rate is larger than the mobility rate, the time spent in address configuration is shorter. The hierarchy of the approaches from address configuration delay perspective is the same as for the control signaling overhead: PMIPv6-NEMO through prefix delegation induces the longest configuration time, and the lowest is the DMM-NEMO through prefix division. For instance, when the $SMR = 0.2$ (configuration time is the highest), the PMIPv6-NEMO PD approach induces 7.13% longer time delay in address configuration than MIPv6-NEMO (in the figure MIPv6-NEMO and DMM-NEMO PD overlap), 7.4% longer delay than DMM-NEMO PD, 16.34% longer delay than PMIPv6-NEMO Div, and 19.95% higher than DMM-NEMO Div. This tendency remains accurate when the SMR is higher; that is the previous order is the same. This configuration delay is a consequence of the signaling overhead. The PMIPv6-NEMO PD and DMM-NEMO PD use an additional protocol, DHCPv6, to have the prefix delegation functionality. This induces higher latency as more message exchanges are required. The MIPv6-NEMO although induces less exchanges to the first two protocols, but suffer from longer delays to the central anchor distance from the MR even in case of domain change. The DMM-NEMO Div has lower configuration delay due to a flattened architecture when compared to PMIP-NEMO Div. These delays can be lowered by changing the access technologies and the distance between the network entities.

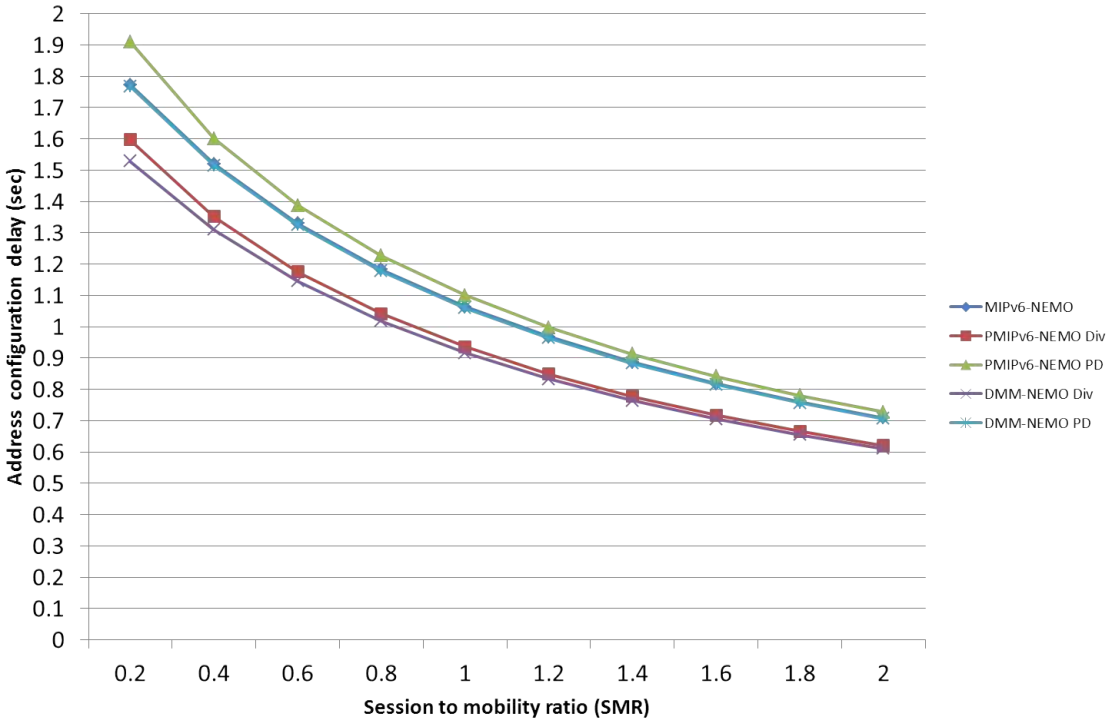


Figure 4.14: Impact of the session-to-mobility ratio on the total address configuration delay for MIPv6-NEMO, PMIPv6-NEMO, and DMM-NEMO.

4.4.6 Modeling for the end-to-end delay

Using the border crossing probabilities in Equations 4.2, we define the total end-to-end delay as:

$$T^{E2E} = (P_{intra} - P_{inter}) \times T^{E2E}_{intra} + P_{inter} \times T^{E2E}_{inter} \tag{4.20}$$

The e2e delay depends on the bandwidth, the propagation delay, and the distance between the MR and its mobility architecture components.

4.4.6.1 MIPv6 architecture

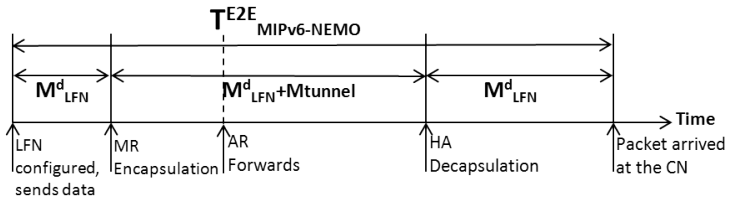


Figure 4.15: Time diagram for the end-to-end delay in MIPv6.

Figure 4.15 illustrates the time diagram for the end-to-end delay in the MIPv6 architecture. The data sent from the LFN to the CN is first encapsulated at the MR before it is transferred to the HA through the AR. The HA tears off the tunnel header when the packet arrives, before transferring the message to the CN (end of the data path). The e2e delay for this packet is then:

$$T^{MIPv6}_{intra} = T^{MIPv6}_{inter} = (\frac{M^d_{LFN} + M_{ENC}}{B_{V2I}} + R_{V2I}) + H^{HA}_{AR} \times (\frac{M^d_{LFN} + M_{ENC}}{B_f} + R_f) + H^{CN}_{HA} \times (\frac{M^d_{LFN}}{B_f} + R_f) \tag{4.21a}$$

4.4.6.2 PMIPv6 architecture

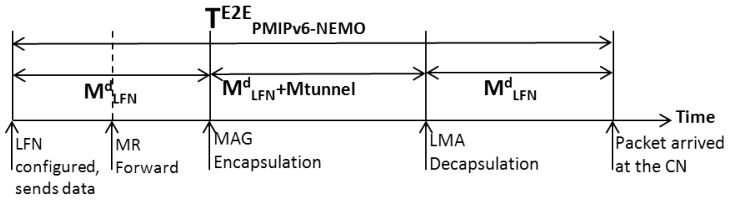


Figure 4.16: Time diagram for the end-to-end delay in PMIPv6.

Figure 4.16 illustrates the time diagram for the end-to-end delay in the PMIPv6 architecture. The data path follows the control path to reach the CN through the LMA. In addition, the PMIPv6 addressing pool anchored at the LMA avoids the triangular routing problem of MIPv6, given that the MR roams in the same PMIPv6 domain. Note that the encapsulation starts at the MAG (not the MR) and terminates at the LMA, before the data reaches its destination. When the MR roams from the first PMIPv6 domain (anchor point LMA-1) to the second domain

(anchor point LMA-2), the address remains anchored at the LMA-1 and the packets traverse a tunnel between both LMAs. The e2e delay for this packet is then:

$$T_{intra}^{PMIPv6} = (\frac{M_{LFN}^{d}}{B_{V2I}} + R_{V2I}) + H_{MAG}^{LMA} \times (\frac{M_{LFN}^{d} + M_{ENC}}{B_f} + R_f) + H_{LMA}^{CN} \times (\frac{M_{LFN}^{d}}{B_f} + R_f) \quad (4.22a)$$

$$T_{inter}^{PMIPv6} = (\frac{M_{LFN}^{d}}{B_{V2I}} + R_{V2I}) + H_{MAG-2}^{LMA-2} \times (\frac{M_{LFN}^{d} + M_{ENC}}{B_f} + R_f) + H_{LMA-1}^{LMA-2} \times (\frac{M_{LFN}^{d} + M_{ENC}}{B_f} + R_f) + H_{LMA-1}^{CN} \times (\frac{M_{LFN}^{d}}{B_f} + R_f) \quad (4.22b)$$

4.4.6.3 N-DMM-P architecture

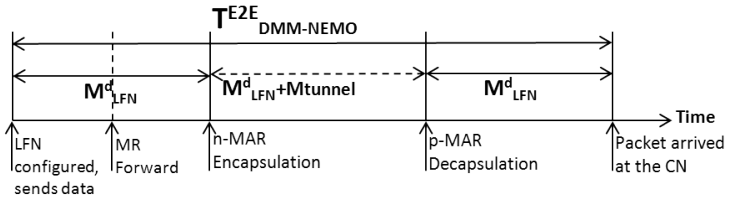


Figure 4.17: Time diagram for the end-to-end delay in DMM.

Figure 4.17 illustrates the time diagram for the end-to-end delay in N-DMM-P architecture. When the LFN uses the HNP advertised in the domain, the data path traverses the MR, MAR to the CN with no encapsulation. If the MR maintains the mobility of a previous HNP at n-MAR, then the data path is incremented by the distance separating the n-MAR and the p-MAR; distance which the data packets traverse encapsulated in a bidirectional tunnel.

$$T_{intra}^{DMM} = (\frac{M_{LFN}^{d}}{B_{V2I}} + R_{V2I}) + H_{MAR}^{CN} \times (\frac{M_{LFN}^{d}}{B_f} + R_f) \quad (4.23a)$$

$$T_{inter}^{DMM} = (\frac{M_{LFN}^{d}}{B_{V2I}} + R_{V2I}) + H_{p-MAR}^{n-MAR} \times (\frac{M_{LFN}^{d} + M_{ENC}}{B_f} + R_f) + H_{p-MAR}^{CN} \times (\frac{M_{LFN}^{d}}{B_f} + R_f) \quad (4.23b)$$

Figure 4.18 shows the end-to-end delay between a CN and a LFN in the vehicle as function of the session-to-mobility ratio. The end-to-end delay decreases as the SMR increases; That is the end-to-end delay is shorter when the MR does not change its original point of attachment frequently. We can here appreciate the effect of the centrality vs. distribution of anchors in mobility architectures. As the data plane (or the routing path) follows the addressing architecture, the CN's packets have to reach the mobility anchor before reaching the final destination.

In MIPv6, if the MR is attached in a distant topological location, the data path is longer, and has to pass the HA. In PMIPv6, the addressing is still anchored at a central location (LMA) but the distance between the MAG and an LMA in a single domain is shorter. In DMM, due to a flattened architecture and a combined LMA/MAG roles at the MAR, the routing path is the shortest. When the MR moves from its original point of attachment, the packets in MIPv6 still join the HA before the MR. Same in PMIPv6 where the packets join the LMA, the MAG then the MR. In DMM, the packets have to join their original anchoring point and then are tunneled back to the current point of attachment of the MR, until the end of this session. In Figure 4.18 this tendency is respected and the end-to-end delays decreases gradually and seems to converge when the SMR is higher due to a fair initial choice of the initial numerical system parameters. This end-to-end delay can be decreased in each situation by shortening the routing path thus separating the control plane from the data plane. Routing optimization approaches can be applied to these mobility management protocols in this case.

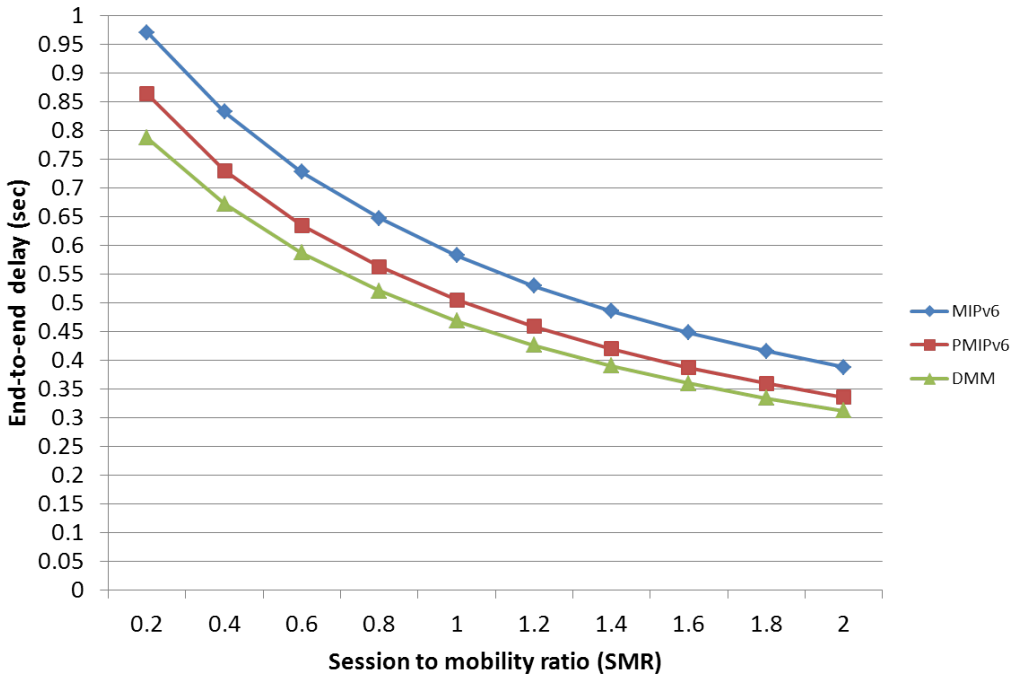


Figure 4.18: Impact of the session-to-mobility ratio on the end-to-end delay for MIPv6-NEMO, PMIPv6-NEMO, and DMM-NEMO.

4.4.7 Tunnel usage

The DMM approach takes into consideration the fact that hosts use heterogeneous applications with different mobility requirements. In DMM , the mobility of a prefix is maintained if the host after the handover is still running an application requiring the use of a previous HNP. This feature is the *dynamic anchoring*. MIPv6 and PMIPv6 maintain the mobility of their hosts all the time. This has an overhead cost that we established earlier in Metric 1. We try here to quantify the ratio between the number of sessions using tunnels to the total number of sessions (TU).

As described for MIPv6 and PMIPv6, $TU = 1$. This is due to the absence of the dynamic anchoring feature in these mobility architectures. In DMM, tunnels are used for sessions after

the handover. At the time t, let us define $N_n(t)$ and $N_h(t)$ as the number of new sessions and handover sessions. If we suppose that these are Poisson processes with parameters λ_n and λ_h, we find:

$$TU = \frac{N_h(t)}{N_n(t) + N_h(t)} \tag{4.24}$$

Also [142]:

$$\lambda_h = E_{inter} \times \lambda_n \quad and \quad E_{inter} = \frac{1}{\rho\sqrt{N}} \tag{4.25}$$

We finally obtain:

$$TU = \frac{1}{1 + \rho\sqrt{N}} \tag{4.26}$$

Figure 4.19 illustrates the use tunnel encapsulation in the proposed protocols in function of the session-to-mobility ratio. As described above, this metric highlights the dynamic anchoring in DMM to only support mobility for applications that requires it. The impact is a higher use of tunnels when the mobility is higher (low SMR) and a lower use of tunnel in case of low mobility and high number of new sessions (higher SMR). Lower tunnel usage means lower complexity in implementation, deployment and maintenance at the network components involved.

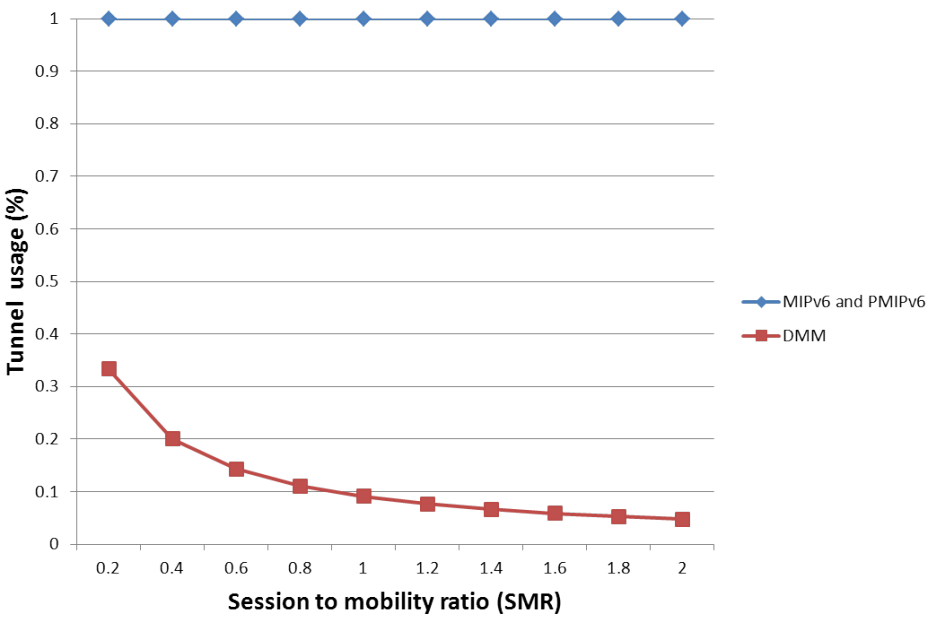


Figure 4.19: Impact of the session-to-mobility ratio on the tunnel usage for DMM-NEMO.

4.5 Conclusion and future work

Mobility management has always been a key issue for network operators and of great value for users and application developers. Several IPv6-based mobility schemes have been proposed in the literature and by IETF. In order to understand the core problem of mobility in IP-based architectures, we first proposed to study the addressing architectures and to understand the importance of topology correctness. The addressing architecture is a core issue for the current

Internet architecture scalability. Network operators expressed their concerns for the scalability of their routing systems as the use of Provider Independent addressing grew in interest among other Internet players. PIA are used for easier mobility and multihoming management and tailored traffic engineering practices. The consequence is the use of non-aggregatable addressing architectures that increase the size of the BGP routing tables in the core network. We also explained the difference between infrastructure-based and infrastructure-less addressing architectures and their possible uses in vehicle-to-Internet communications.

In order to understand the current state of the art of mobility management protocols, we first proposed to classify them into centralized and distributed approaches. Initially, the Mobile IP centralized architecture was the de facto solution for IP-based mobility. Mobile IP introduced the concept of IP addresses used as locators to reach the mobile node, and as names/labels to identify the mobile node. We explained how the accurate binding between those two objects decides of the network functionalities and their deployment in a mobility architecture. The DMM paradigm pushed by network operators, aims at flattening those centralized mobility architectures and to relocate the anchors closer to the user and the edge network to avoid traversing and overloading the core. The mobility of hosts and networks are different in terms of requirements. The main mobility management solutions propose Network Mobility extensions to support the mobility of moving networks, such as vehicles. We also reviewed the solutions proposed in this field and proposed two possible extensions to existing DMM paradigm, not existing in the literature at the time of writing.

In order to understand the performance of these proposals, we conducted an analytical evaluation using a parameterized analytical model. Obtained results showed that the partially distributed mobility approaches can lower the signaling load and the address configuration delay for the users. In terms of data plane, the end-to-end delay can also be decreased in DMM. Finally, we also showed that the DMM scheme through its dynamic anchoring feature can save resources in the network by using tunnels and re-routing only if required, for example, if the LFNs in the vehicle are running long lasting applications.

As a perspective, the use of simulation to approach real-life network conditions with high load is promising. Other perspectives can be the use of routing optimization extensions in our model and the evaluation of other metrics such as the packet loss after a handover.

Table 4.5: Model parameters and notations.

Parameter	Description	Default values
$T_{RA_{min}}$, $T_{RA_{max}}$, T_{RA}	The (min, max) delay between 2 consecutive Router Advertisements	40ms, 70ms (High mobility scenarios of RFC 6275)
T_{RA}	The average delay between 2 consecutive Router Advertisements	
T_{DAD}	The delay required to perform a Duplicate Address Detection check	1 sec
T_{L2}, T_{AU}	Link-layer and Authentication latency	50, 550 ms
M^c_{RA}, M^c_{NS}, M^c_{PBU}, M^c_{MBU}, M^c_{DHCPv6}, M^c_{MOB}, M^c_{BU}	The size of the control message of ICMPv6 Router Advertisement, Neighbor Solicitation, , PBU/PBA (PMIPv6), MBU/MBA (N-DMM-p), DHCPv6 (Prefix delegation), Request/Reply towards the Location database, BU/BA (MIPv6) messages	80bytes, 80bytes, 75bytes, 66bytes, 170bytes, 66bytes, 56bytes
M^d_{LFN}	The size of a data packet sent by an LFN	1KBytes
M_{ENC}	The size of the encapsulating tunnel	40 bytes
B_{V2I}, B_F	Bandwidth for V2I and Fixed Infrastructure links	11Mbps, 100Mbps
R_{V2I}, R_F	Propagation for V2I and Fixed Infrastructure links	40ms, 0.5ms
$\overline{v}$, R_{SN}, $\mathbf{N}$	Vehicle's average speed, Radius of cell's circular coverage, Total number of cells (subnets)	45km/h, 500m, 100
T_u	The latency of processing a binding update or a prefix delegation	200 msec [44]
C_u, C_{pdel}	The cost of processing a binding update (resp. a prefix delegation)	–
α, β	Unit cost (factor) of processing a binding update (resp. a prefix delegation) with the Location Database (resp. the DHCPv6 server)	2, 3
N_{MR}, N_{MD}	Number of active MR per Mobility Domain (resp. Number of Mobility Domains)	2^{16}, 64
H^D_S, H^{HA}_{AR}, H^{CN}_{HA}, H^{LMA}_{MAG}, H^{LMA}_{CN}, H^{LMA-1}_{LMA-2}, H^{MAR}_{MAR}, H^{LDB}_{MAR}, H^{CN}_{MAR}	Average number of hops from Source to Destination	-, 20, 10, 5, 10, 10, 3, 5, 10

Chapter 5

VIN6: A VIN-based namespace for Evolutionary Future Vehicular Internet

When considering IP multi-homing and mobility management issues in a fixed infrastructure, it is common to assume at least one indirection level for addressing and routing [48][145]. For example, Mobile IP and Network Mobility (MIP/NEMO), instances of Network-Layer routing and addressing indirection at the Home Agent [32], are often referred to as two-tier addressing architectures.

Indirection increases hugely the entropy and size of inter-routing tables required to reach end systems [146][10]. The Internet Architecture Board (IAB) considers this problem as the consequence of IP semantics overload and proposed recently to tackle this issue by splitting Locator and Identifier functions of the IP numbering space [146].

Name to location indirection with IP is achieved with Provider Independent (PI), as opposed to Provider Allocated (PA), addresses [146]. Multi-homed or mobile sites use fixed PI addressing (names). PI addressing is not topological (labels) and is stable even if the network operator (Internet Service Provider) changes. However, unlike PA addressing, PI prefixes cannot be aggregated in the core network which leads to unbound growth of inter-domain routing tables [10].

Multi-homing and mobility management are of paramount importance for vehicular networks. Only recently, standard development bodies proposed protocol stacks supporting IP-based communications along with safety and emergency time-critical protocols [32]. Infotainment, fleet management, remote diagnostic, traffic offload or distributed games are implemented on Vehicle-to-Infrastructure (V2I) or Vehicle-to-Vehicle (V2V) settings [127]. Operation and performance of IPv6 over WAVE/802.11p standard must be enhanced [13].

Indeed, in-vehicle network mobility management is usually solved with MIPv6/NEMO. Embedded Mobile Router (MR) may use several wireless egress interfaces (802.11p, LTE, and more) which makes the MR multi-homed [32]. For IP-based vehicular networking scenarios (of interest in this paper), one instance of PI addressing could be based on ISO-3779 VIN codes that are unique and mandatory identities of each vehicle worldwide [114]. These wireless technologies now enable recent research initiatives to consider naming and addressing challenges for vehicular networks [214] [65].

Solving the vehicular networking challenges by simply adapting the legacy indirection infrastructure may not be sustainable [127]. Indeed, some VIN databases for developers [213] claim including up to 2^{31} *distinct VIN codes of vehicles* in North America *only* since 1996 (regularly updated). VIN is provisioned to uniquely identify up to 2^{78} vehicles worldwide *every 30 years* which is already several orders of magnitude bigger than IPv4's 2^{32} numbering space. Futuristic

scenarios forecasting vehicles integration to the Internet may *not be scalable* with this networking model.

We propose to dig further in the VIN semantics and present our algorithm to build a scalable and hierarchical Future Internet (FI) IPv6 PI addressing space that identifies up to 2^{51} distinct vehicles. We also present an original approach to create vehicular-specific endpoint identifiers and integrate vehicular communications in an evolutionary and sustainable manner in FI. Our addressing architecture is compatible with a subset of evolutionary network-based approaches (such as LISP and GSE). Our large vehicle identification space (2^{35}) per manufacturer allows using pseudonyms in local and global communications.

In detail, our contributions in this chapter are:

- Using VIN codes as hierarchical vehicular identifiers.
- Mapping VIN to IPv6 numbering space with an algorithm that achieves uniqueness conservation.
- Discussing the benefits of the IPv6 vehicular-specific prefixes and addresses for end-to-end (E2E) services
- Maintaining E2E reachability while using pseudonym codes with an architectural indirection element
- Integration of our VIN-based architecture with the LISP-MN protocol
- Performance evaluation of the proposed techniques

5.1 Network-based Future Internet architectures

The IAB considers IP semantics overload as the problem to be solved today in order to narrow the explosion of inter-routing tables in the core network [146]. Indeed, the unique IP numbering space principle lead to consider the same IP address as a label (name) for the Internet graph vertices and a locator guiding the global routing operations [48].

Despite different design objectives, recent FI proposals consider Locator/Identifier split realm as a fundamental building block [168]. *Host-based* solutions propose a new stack-layer between transport and network for E2E identification, when other *network-based* approaches specify two separate spaces for identification and location [189]. We focus on this chapter solely on network-based approaches. The full taxonomy of Future Internet approaches are detailed in our second chapter dedicated to this matter (Chapter 2).

Network-based approaches use functional elements in the network to provide the desired level of indirection with less mandatory changes to hosts and applications. Evolving without breaking the infrastructure comes as a result of the use of legacy IP addresses.

For instance, Locator/ID Separation Protocol (LISP) defines two addressing elements: Routing locators (RLOCs) and Endpoint Identifiers (EIDs) on the IP numbering space [189]. The evolution of the infrastructure is achieved with the separation of the EIDs as hosts identities and RLOCs used to route the packets in the core network with encapsulation. Authors of [143] follow a similar architecture design approach. This subset of network-based evolutionary FI proposals using IP tunneling and location services in the core network, can be grouped into the map-and-encap category [145]. These approaches share the common property of encapsulation overhead and must provide for an efficient and scalable EID to RLOC mapping system.

The other category is based on address rewrite and represented by GSE $(8 + 8)$ [163]. GSE uses address translation to achieve indirection and provide aggressive topological aggregation to

narrow routing tables growth. In this approach, the IPv6 address bears new semantics: locator part (called Routing Goop), a local site information (called Site Topology Partition), and an endpoint identifier (End System Designator). This addressing architecture guarantees a clear and distinction of public and private topology while assuring interoperability and E2E principle conservation. Similar and recent addressing rewrite architectures can be found within ILNP [10] to mention a few. Despite IPv6 addressing architecture compatibility, these approaches may seem having a disruptive impact on the current architecture [145].

5.2 VIN-based IPv6 networking

With regards to this related work, we specify a *scalable network-based architecture with Provider Independent subset of the IPv6 space that bears the semantics of the VIN hierarchy.* Along with the supporting architecture, our numbering space integrate both evolutionary Internet approaches: map-and-encap or address rewrite, and enhance them to efficiently support vehicular IP-based communications.

In order to support a large set of vehicle-to-Internet use cases through an evolutionary FI solution space, we need this initial non-exhaustive set of basic functional requirements:

- The addressing must be provider independent and support the Locator/ID split for scalability.
- Localization service should be introduced as a flexible functional architectural element
- Interoperability with network-based evolutionary FI approaches .

5.2.1 VIN numbering space overview

Let us first define one possible instance of vehicular specific identifiers. The Vehicle Identification Numbers are possible candidates. Indeed, VIN space is:

- ISO-3779 and ISO-3780 standard
- Mandatory, unique, and present in every vehicle
- Hierarchical vehicular-specific endpoint identifiers

Our objective is to preserve these characteristics while mapping VIN onto usable IPv6 networking objects (addresses, prefixes, and Mobile Node Identifiers).

VIN (Figure 5.1) is a 17 characters alphanumeric hierarchical code that uniquely identifies a vehicle worldwide. The VIN code contains 3 sections: WMI, VDS, and VIS.

The WMI is 3 digits long and uniquely designates the manufacturer's continent, country, and the unique national identifier. The VDS is 6 characters long and describes the vehicle: weight, model, engine type or body style. ISO-3779 allows filling it with "dummy" information if not used. *This section is not included in the unique vehicle identifier.*

The VIS is 8 digits long. Combined with VDS, they uniquely identify a vehicle within a car manufacturer for 30 years. Combined with WMI, they uniquely identify a vehicle worldwide. VIS ranges from the 10th digit to the 17th. Digits (10-13) are alphanumeric and (14-17) numeric.

For the sake of concreteness, "VF1", "VF3", and "VF7" are examples of WMI codes in the region "VF" (V is allocated to Europe and F to France) belonging to the manufacturers Renault, Peugeot, and Citreon respectively. One car manufacturer may have several WMI codes depending on the number of manufactured cars per year.

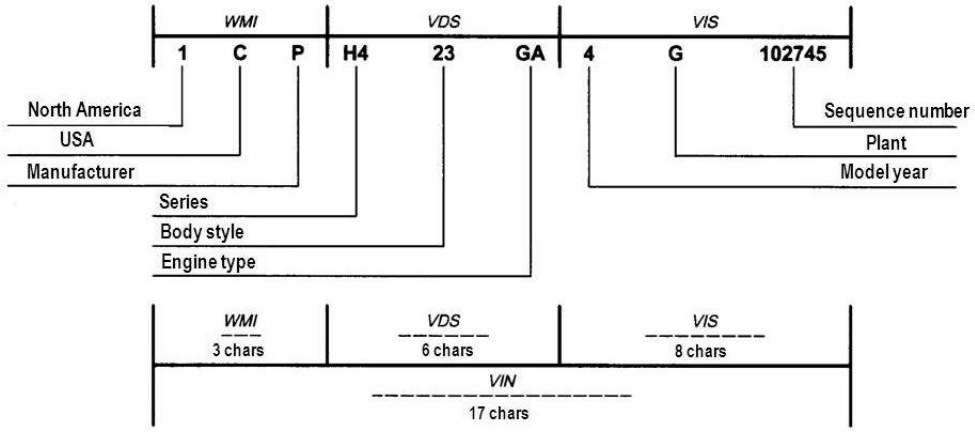


Figure 5.1: Vehicle Identification Number

Our work is not the first that considers VIN as a valuable information for IPv6 addresses. Authors of [131], use some VIN fields to map them into decimal numbers *separately*, before binary conversion to Extended Unique Identifiers (EUI-64). *One* IPv6 address is generated. This method is inefficient in terms of compression and uniqueness of the EUI-64 is also debatable (some included values are from VDS which is non-standard). Finally, one generated IPv6 address is not enough for the solution space described above.

Authors of [130] provides a method to determine the IPv6 address of a component inside the vehicle. This proposal uses only the VIS section of the VIN as part of the generated prefix along with a non-standard method to set a global prefixes. In order to assure global scope for generated prefixes, an administrative check *must* be performed.

In other areas, as discussed in our Chapter 3, VIN can be used as an ID for the vehicle and its components in Vehicle-to-Grid communications as suggested by this technical report [177].

In the following, we present an algorithm to perform conversion of the VIN into IPv6 network prefix and address while preserving its uniqueness.

5.2.2 Initial assumption

To identify a vehicle, WMI (digits 1 to 3) and VIS (digits 10 to 17) must be used [114]. The VDS section can be inferred knowing the two other sections. A multi-key query on a local database by the original manufacturer is a possible method.

Assumption *VIN codes being hierarchical, WMI and VIS sections uniquely identify a vehicle.*

This assumption (based on ISO-3779 and ISO-3780 documents) allows to create vehicular-specific identification space of 2^{35} codes per manufacturer (2^{16} manufacturers).

5.2.3 Detailed algorithm

In [131] mapping (transliterating) and numeral conversion are used. To include a VIN digit in EUI-64, 33 decimal values are possible (6 binary positions for conversion).

We propose to build a VIN-specific numeral system using allowed values of ISO-3780; that is Arabic numerals (0 to 9) and Latin letters (A to Z) excluding the exceptions (I, O, and Q), in order to generate Base-VIN numbers. We show that compression gain can be achieved in the conversion operation when mapping *grouped* digits.

Base-36 is another candidate for our model. It contains all alphanumeric characters and uses 36 as the radix. Conversion to other numeral systems needs simple arithmetic operations (multiplication/division). Digits of this system are ordered as follows: $0 < 1 < 2... < 9 < A < B... < Y < Z$.

Basically, our mapping proposal can further be summarized as: *VIN identifier can be considered as a whole and read as a number written in Base-VIN.*

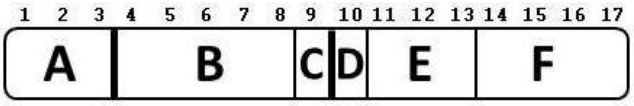


Figure 5.2: VIN Identifier broken down to its basic semantic components to form hierarchical unique identifiers

The compression is achieved by *reading* a value in Base-VIN rather than mapping *separately* to Base-2. The number of bits after conversion is:

$n \leftarrow Log_2(X) + 1$ {X is the maximum of the set}

The *restricted set of allowed values* (Figure 5.2) for selected VIN sections, helps reducing the amount of necessary bits with an objective of preserving *VIN uniqueness*. Algorithm 4 summarizes the high level details of this approach. Note that alternative compression algorithms using information theory techniques may also be possible. The algorithm may run only once (engine ignition, for example) but can also be run each time a new pseudonym needs to be created.

Algorithm 2 VIN to IPv6 conversion algorithm

X is a Binary vector, Y is the bitmap to fill

$X_1 \leftarrow f$(A,VIN), $X_2 \leftarrow f$(D,VIN), $X_3 \leftarrow f$(E,VIN), $X_4 \leftarrow f$(F,10). {f arguments are the selected fields and the numeral base to use (radix) when reading}

for $i = 1$ to 4 **do**

$Y_i \leftarrow g(X_i, type)$ {g arguments are the binary value to map and the bitmap type. The bitmap type defines the bits placement (prefix, endpoint ID).}

end for

5.3 VIN-based Network-Layer architecture

This paper focuses on describing the VIN-based IPv6 addressing and the presentation of the *uniqueness conservation* algorithm. However, to complete our Network-Layer architecture design, a quick glance at necessary high-level architecture functional elements and their roles is given.

5.3.1 Architecture functional elements and roles

WMI identifies the car manufacturer. Its validity is maintained by the Society of Automotive Engineers (SAE) along with national automotive authorities. VIS is the vehicle sequential identifier and unique by definition. By hierarchical design of our VIN numbering space (WMI, VIS), a new network and services domain emerge: the vehicle manufacturer domain (MD). *The addressing is operator independent but permanently correct at the MD.* The fundamental roles at this level are three fold.

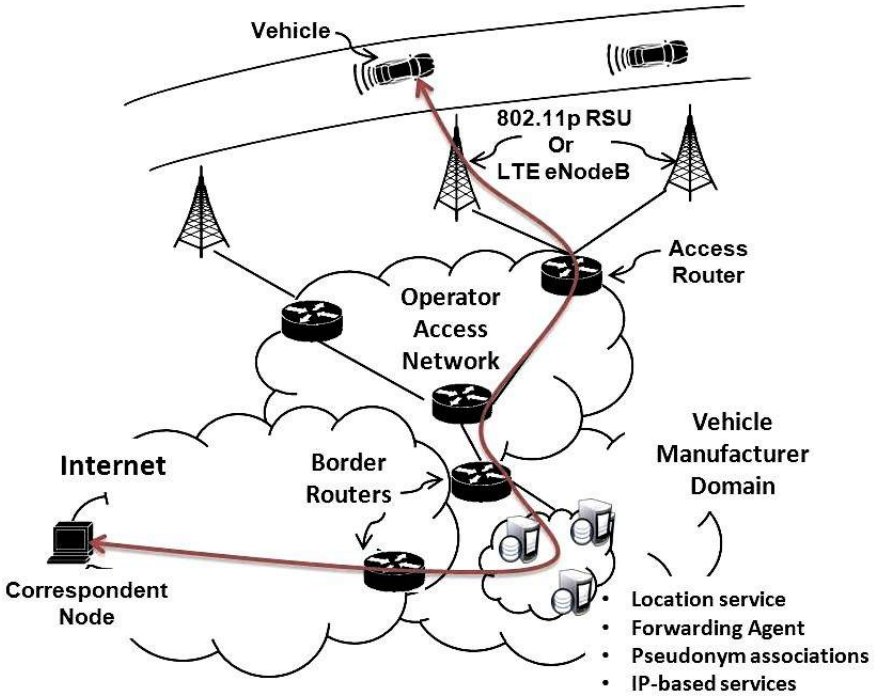


Figure 5.3: VIN6 architecture and functional elements. Regardless of the current location of the vehicle, a correspondent node can issue a packet with VIN-based addressing to the vehicle. Indirection occurs at the manufacturer domain and the packet is forwarded to the current topological location

The E2E principle conservation. The VIN-based identification calls for trusted end-to-end relationship establishment based on these identifiers and guaranteed authentic (even when pseudonyms are in use) by a central trusted authority. The E2E principle is conserved regardless of the translation strategy (map-and-encap or address rewrite).

The IP Location and Forwarding Service. The MD records the associations of identifiers (VIS) and current topological address. The correspondence of (PI, PA) addressing is performed at this level. This control plane is compatible with EID-to-Locator mapping system in LISP [145]. The forwarding depends on the address translation strategy (encapsulation or rewrite). The IP traffic could be handled by different techniques (including the cloud computing).

The VIS pseudonym associations. The tussle between mobility (stable global ID) and privacy (random and temporary ID) is detailed in [26]. Our architecture comprises two scopes (CN, MD) and (MD, Vehicle). It is then possible to change VIS pseudonyms in each scope and yet conserve E2E reachability (two-tier addressing). The large VIS identifier space (2^{35} per manufacturer) provides for the use of several temporary VIS codes by vehicle (at each handover for example) to generate pseudo-random IPv6 prefixes/addresses. *Its original and unique VIS code attributed at manufacturing time could never be used globally by our design.*

5.3.2 VIN6 enhancements for IPv6

The VIN6 addressing is compatible with IPv6. Base-VIN along with our conversion algorithm, allows to create unique vehicular IDs shorter than 64 bits. Figure 5.4 illustrates the Locator part and Endpoint ID. The first 8 bits designate the scope of the prefixes formed. Two global scopes

are possible (V1 or V2). V1 is routed through the global infrastructure and V2 is used locally (multi-hop) but does not leak to global Infrastructure (filtered at some architecture level).

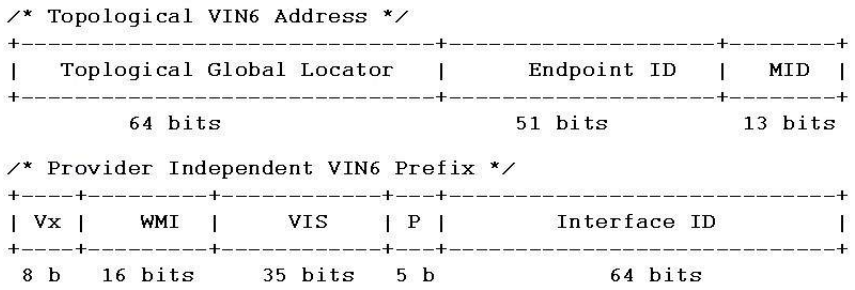


Figure 5.4: VIN-based IPv6 addressing architecture. The compression gain achieved with our algorithm helps defining additional parts that enables more end-to-end services. Top figure illustrates current topological address. Bottom figure represent provider independent address format

V1 prefixes are announced in the infrastructure and routed globally to the indirection point. The routing decision is made by Longest-prefix match on the tuple (V1, WMI). This WMI-only based routing, completes initial assumption to assure that routing operations of the network are deterministic.

On the other hand, WMI codes preceded with the V2 value are used locally to the vehicle and should not leak to the infrastructure. These prefixes can then be generated with an infrastructure-less algorithm (for vehicular scenarios with regular infrastructure disruptions) at the vehicle level.

The 24 bits long part (V1, WMI) allows an aggressive aggregation of prefixes in the core network. Indeed, for the core network routers, the next 35 bits are not considered for routing decisions. This design choice allows us to anchor 2^{35} prefixes with one routing table entry. The next 35 bits long VIS part, are left up to the manufacturer domain to localize the owner (Location) and route accordingly (Forwarding).

The VIN-based Endpoint Identifier completes our design and replaces the Interface Identifier of IPv6. Using this vehicular specific identifier on several interfaces is now possible as its origins are not tied to the interface (as would MAC addresses be) but represents the identity (permanent or temporary) of the vehicle. This design choice creates a multi-homed site (the vehicle) addressable on several interfaces. The Machine ID (MID) part (13 bits) of this Endpoint ID allows for flexible addressing and Traffic Engineering. Table 5.1 details the sections included in the VIN-based addressing architecture of Figure 5.4. In Chapter 6 we propose the use of these sections to create IP-based clusters.

5.3.3 Making the best of VIN6 addressing

VIN6 addressing architecture propose a new type of provider independent addressing through VIN derivation. The provider here is the Internet Service Provider who actually routes the network packets. The manufacturer domain will then be in charge of his vehicle fleet. Based on the concepts of Chapter 2, VIN6 is also a *location independent name*. Location here means the *actual point off attachment* of the vehicle.

The network location concept has been exploited and defined accurately by (all) Mobile IP architectures as the Care-of-Address (CoA). LISP has also made use of the exact same concept in its Routing Locator (RLOC). Now, depending on the network technologies used, the manufacturer domain's VIN6 addressing pool can be announced inside BGP-Update message to

Table 5.1: Parameters of VIN-based addressing architecture

Parameter	Definition	Values
Vx	Addressing scope	V_1 for global and V_2 for VULA
PID	Prefix ID used for internal devices (fixed or mobile) and neighboring vehicles	P_k^f for internal fixed devices, P_k^m for internal mobile devices, and P_k^e P e for external prefixes
MID	Machine ID assigned sequentially, randomly, or permanently	M_k^f for internal fixed devices, M_k^t for temporary connections

the neighbors (Home Addresses, HoA) or installed as EIDs inside LISP mapping systems to be resolved to one of the domain's RLOCs.

5.3.3.1 VIN6 as home addressing pool

In this approach, the manufacturer domain (also an Autonomous System) has to advertise its VIN6 pool, along other PIA that he obtained, to its peers through BGP-Update messages. The vehicles identified by their VIN have a VIN6 prefix dedicated to them, obtained through Algorithm 4. The corresponding nodes would then join any of the in-vehicle or the MR hosts through one VIN6-based address. These addresses are anchored at the manufacturer domain. The mobility architecture can be any architecture of Chapter 4. The vehicle can then update the Anchor Point inside his manufacturer domain with the new location as it changes its point of attachment. The Anchor Point will forward any VIN6 addressed packet to its destination based on the latest location (CoA) registered within its location database.

This approach is not different from legacy PIA combined to mobility architectures already proposed in the literature. The advantage of using VIN6 addressing comes from its *compact size* and its *aggregation capacity*. Indeed, VIN6 PI addressing space that identifies up to 2^{51} distinct vehicles (cf. Figure 5.4), but the prefixes announced in BGP-Update messages are only 24bits long ($V_x + WMI$ sections). The rest of the 35 bits VIS section is used at the Anchor Point to identify the vehicle. This vehicle identification space (2^{35}) per manufacturer is already larger than the size of the IPv4's entire addressing pool, and is *not* present in the DFZ routing tables, but handled at the Anchor Point. The manufacturer has the choice of the technology and is capable of taking the decision on its own without affecting neighboring ASes. Of course, VIN6 is compatible with other addressing architectures and conserves the advantages of PIA, in particular, avoiding renumbering when the network operator is changed.

5.3.3.2 VIN6 as LISP EIDs

In this approach, we take advantage of the clean separation of locator and identifier in IP addressing as implemented by the LISP protocol. VIN6 addressing with its semantics derived from the VIN identifiers can be used as EIDs in LISP, EIDs being IP addresses (v4 or v6 alike). RLOCs on the other hand can be considered as care-of-addresses (using Mobile IP terminology). The LISP design splits location from identity in addressing in order to provide native mobility and multihoming. Mobile clients can therefore be provided with multiple network interfaces.

Routing in LISP is done through an additional Mapping System indirection level. Indeed, hostname lookups in DNS return EID(s) and a second lookup is required to find the current RLOC. The Mapping System here is a location management system, similar to the Location Directory functionality in Mobility architectures. One major difference to legacy mobility architectures, is the will of LISP's Mapping-System to remain distributed and federated by design [184].

The use of VIN6 as EIDs can be achieved by the use of a Mapping System hosting the manufacturer domain's RLOCs. LISP Mapping System (LMS) is used by the LISP border domain routers (Ingress/Egress Tunnel Routers, ITR/ETR, abbrev. xTR) to query the current location of a certain EID (for example, returned by a DNS server). The Mapping System returns the RLOC of the xTR to which the data packets should be tunneled in order to be delivered to the initial EID. In our case, to a VIN6 queried by the xTR, the LMS should return the RLOC of the manufacturer domain. This works for vehicles inside the manufacturer's domain; That is, the network point of attachment is topologically behind the xTR's RLOC. This is of course not always the case.

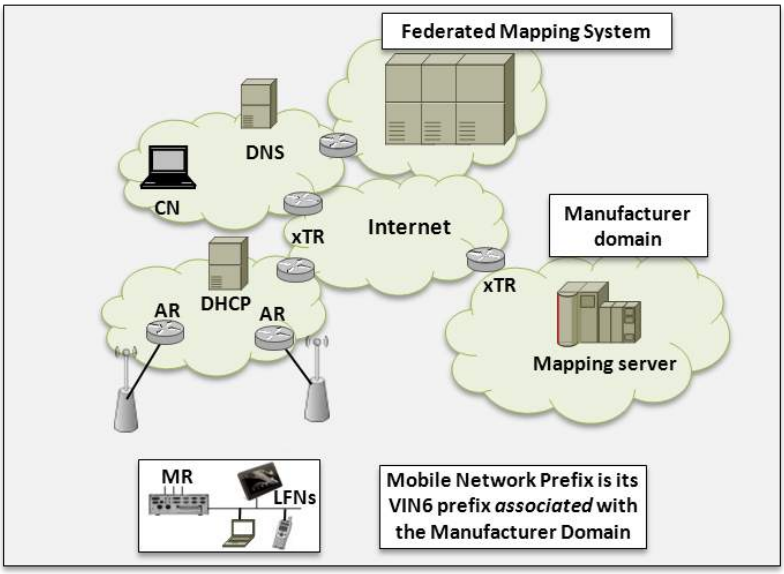


Figure 5.5: VIN6 addressing architecture as deployed in a LISP architecture

5.3.3.2.a LISP-MN protocol

LISP-MN [184] is a recent proposal to handle the mobility of nodes within LISP protocol[1]. Basically, the Mobile Node (MN) is provided with a lightweight version of the LISP xTR border routers functionalities. MNs in LISP-MN are capable of forming RLOCs in their current point of attachment and notify their Mapping Server of their current location. Given their fixed EID (each MN is provided with a permanent one), the LMS is then capable of replying with the current RLOC to requesters. Figure 5.6 illustrates the exchange diagram of the LISP-MN protocol in the case where the MN receives data and when the MN roams to obtain a new RLOC connected to a new Access Router.

The lightweight tunnel router implemented in LISP-MN encapsulates outgoing packets in a LISP header based on current RLOC(s) before leaving the mobile node. The LISP-MN also

[1]At the time of writing, authors of [89] and [221] are proposing advanced mobility architectures and network mobility extensions to LISP-MN protocols. It is basically the adaptation of the mobility architectures seen in Chapter 4 to LISP protocol.

removes the LISP header from incoming packets before sending them to upper layers. The LISP-MN protocol can be broken down to 3 basic operations (similar to Mobile IP): (1) Registering the EID and obtaining an RLOC (2) Updates EID-to-RLOC bindings and transmitting data-packets (3) Handover.

LISP-MN nodes are configured with at least one permanent unique EID: a regular (/32) IPv4 or (/128) IPv6 address. The DNS entry corresponding to the node's FQDN is reolved to this EID, for instance. This address is typically assigned by the *Map-Server provider*. The LISP-MN also needs at least an RLOC that reflects its current point of attachment in the Internet. RLOCs can be obtained through legacy mechanisms (DHCP or auto-configuration). LISP-MN obtain different RLOC in each point of attachment. It is the LISP-MN's responsibility to update its Mapping Server with the current RLOC using the Map-Register message. The node may include multiple RLOCs (multihoming). Once the Map-Server receives a valid Map-Register containing an EID-to-RLOC mapping it will it make it accessible throughout the Mapping-System.

In case a new RLOC is obtained by the LISP-MN while communicating with a CN, it is possible to ensure of the seamless traffic flow to the new location by notifying the xTRs of all the peers. This is to update the bindings stored in the Map-Cache of the peers. Solicit-Map-Request (SMR) messages can be used for example. Other mechanisms, such as versioning, have been proposed in [78] and [108].

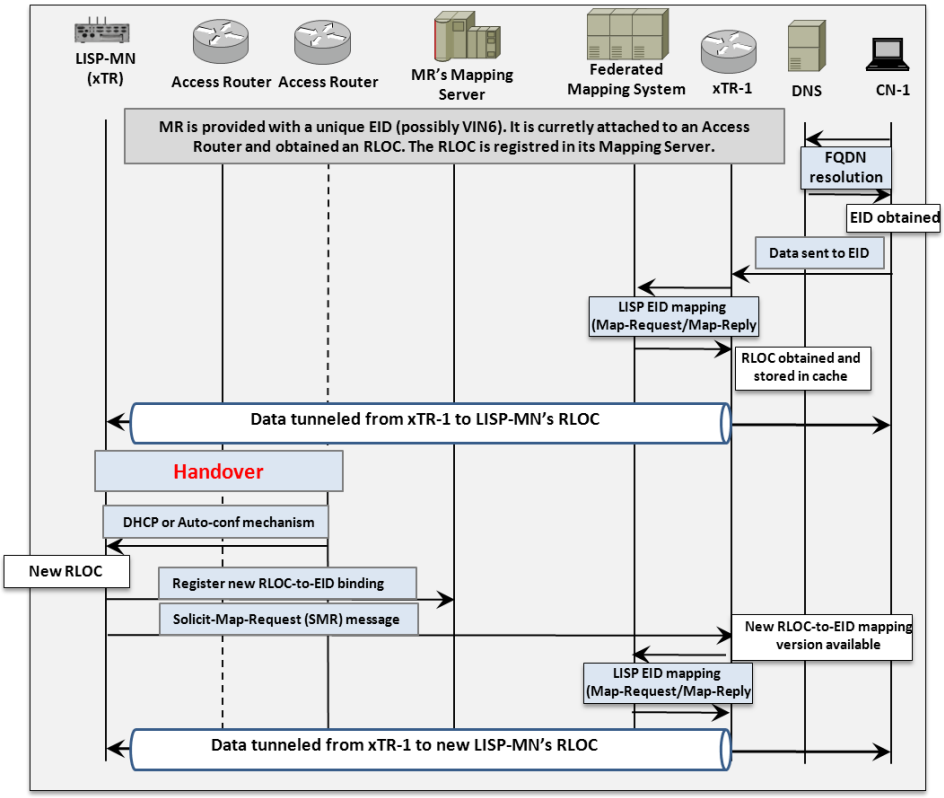


Figure 5.6: LISP-MN protocol message exchange diagram.

5.3.3.2.b VIN6 in LISP-MN

VIN6 addressing can be combined to LISP-MN protocol as follows:

1. The manufacturer domain owns its VIN6 addressing and uses it as EIDs for vehicles. The

Mapping server in the domain keeps track of VIN6 EIDs and shares a pre-configured key with the vehicle's Mobile Router to ensure authentication.

2. The vehicles are equipped with Mobile Routers where the EIDs are kept in a static configuration file. The VIN6 EID is also used to build an internal VULA prefix and announced to internal devices for auto-configuration.

3. The manufacturer domain opens a set of globally accessible EIDs inside the vehicle, and publish their FQDNs in the DNS. A possible DNS entry format of a certain service inside a vehicle could be: *(SERVICEx.VINy.MANUFACTURER, VIN6-EIDx)*.

4. A Correspondent Node behind xTR-1, wishes to communicate with the vehicle. In particular, an application inside CN's host needs to interact with a machine inside the vehicle. Using the FQDN, the DNS returns VIN6-EID of the machine connected to the MR.

5. The xTR queries the Mapping System after the reception of the first packet from the CN destined to VIN6-EID. The xTR stores the returned RLOC. The RLOC is not necessarily one of the manufacturer domain's. RLOCs reflect current topologically correct point of attachment of the MR.

6. The xTR encapsulates the data packets issued by the CN and forwards them to one of the MR's RLOCs. The MR running the LISP-MN daemon decapsulates the packet and detect upon the destination EID whether it is for an internal devices or for its own system.

7. If the MR changes its location, it ensures that its Mapping System has a recent version of its VIN6-EID-to-RLOC binding. The MR can also notify its correspondent's xTR to retrieve a fresh version of its cache entry relative to this EID.

The journey of a VI6 packet in our LISP-based solution shows the that the main advantage of using VIN6 as EIDs whithin LISP-MN protocol is that a **prefix** can be bound to **one RLOC** and the *mobility of a network* maintained using *one mapping entry* in the mapping system. The vehicle's VIN is transformed to an internal prefix (V_2 scope) anchored with global VIN6 EID (V_1 scope) at the manufacturer's domain. The manufacturer can then announce services hosted at particular vehicles using FQDNs that include their VIN. Also, no new messages and no Network-Mobility extensions are here defined when compared to LISP-MN.

5.4 Validation

The evaluation of our VIN-based addressing model will be three fold. Preparing *VIN standard-compatible database* of random VINs to provide for experimentation, *uniqueness conservation* property, and measure the *bit compression gain* on VIN codes using our algorithm. A detailed discussion of privacy in our context is also provided.

5.4.1 Implementation

Linux kernel 3.0.0-27-generic version is used for implementation. VIN mapping/conversion is implemented using bash and C programs implemented for our experiments. The strict respect of system and kernel versions used in implementation are not mandatory.

A detailed database of about 20620000 VIN values is generated. The size of the database can be enlarged for future experiments (involving simulation traces). The database respects strictly the definitions of the two VIN related standards [114] for the format and the content.

The bash script (user space) for VIN conversion operates in two modes: batch or interactive. The batch mode is used in order to confirm *assumption 1*, and interactive mode allows to chose between MAC or VIN as input, in order to generate according IPv6 prefixes.

5.4.2 Uniqueness property conservation

To evaluate the VIN numbers' *uniqueness property conservation*, we present the formal uniqueness proof and highlight the reversibility of used functions (bijectiveness).

Figure 5.2 illustrates the VIN extracted parts: A (WMI), D, E, and F (VIS). According to our model, VIN codes are numbers in Base-VIN. *Assumption 1* can then be rewritten as follows (1):

$\forall$ (VIN_i,VIN_j)$\in$ Base-VIN:

$$\mathrm{VIN}_i \neq \mathrm{VIN}_j \Leftrightarrow (\mathrm{WMI}_i \wedge \mathrm{VIS}_i) \neq (\mathrm{WMI}_j \wedge \mathrm{VIS}_j) \quad (1.1)$$

$$\Leftrightarrow (\mathrm{A}_i \wedge \mathrm{D}_i \wedge \mathrm{E}_i \wedge \mathrm{F}_i) \neq (\mathrm{A}_j \wedge \mathrm{D}_j \wedge \mathrm{E}_j \wedge \mathrm{F}_j) \quad (1.2)$$

Let function f be the bijective conversion from Base-VIN to Base-10 (2):

$\forall$ (VIN_i,VIN_j)$\in$ Base-VIN:

$$\mathrm{VIN}_i \neq \mathrm{VIN}_j \Rightarrow f(\mathrm{VIN}_i) \neq f(\mathrm{VIN}_j) \quad (2.1)$$

Using equation (2.1) with (1.2):

$$f(\mathrm{A}_i \wedge \mathrm{D}_i \wedge \mathrm{E}_i \wedge \mathrm{F}_i) \neq f(\mathrm{A}_j \wedge \mathrm{D}_j \wedge \mathrm{E}_j \wedge \mathrm{F}_j) \quad (2.2)$$

Function g is the bijective mapping function. Function g sets a bitmap according to a binary input. With this definition and using result (2.2) we deduce:

$$g \circ f(\mathrm{A}_i \wedge \mathrm{D}_i \wedge \mathrm{E}_i \wedge \mathrm{F}_i) \neq g \circ f(\mathrm{A}_j \wedge \mathrm{D}_j \wedge \mathrm{E}_j \wedge \mathrm{F}_j) \quad (3)$$

Result (3) states that the result of composition of functions f and g ($g \circ f$) gives distinct results given distinct VIN numbers. Bijectiveness is also a consequence of compositing bijective functions f and g (another way to confirm uniqueness property conservation). Precautions about expired and forged VIN codes that may provoke duplicate VIN6 addresses are considered by defining the MID section (Figure 5.4) to solve possible duplicate addresses conflicts.

5.4.3 Bit compression gain

Compression gain using our Base-VIN is shown in comparison of Base-36 and No-Base, when considering VIN as numbers. The latter case reflects the approach of [131].

The resulting graphic is illustrated in figure 5.7. Using the algorithm defined in section *algorithm*, we consider VIN *numbers as a whole (no sections)* in Base-VIN, Base-36 and No-Base. Note that the limited number of digits in VIN (17) stops the compression calculations at 17 digits.

The graphic shows at position 17 that our model combined with Base-VIN performs 1.961% (2 bits) better than Base-36, and 15.687% better than (prior art) No-Base (16 bits).

5.4.4 Pseudonym VIS codes

Recent studies concerning privacy requirements include the use of pseudonyms [13] [191]. The IPv6-stack includes pseudo-random generation of Interface Identifiers as IETF RFC 4941 standard. On the other hand, some argue that pseudonyms usage in VANETs is not enough given the accurate data disclosed in the applications (position, velocity and identity) that could be correlated to a single user [217].

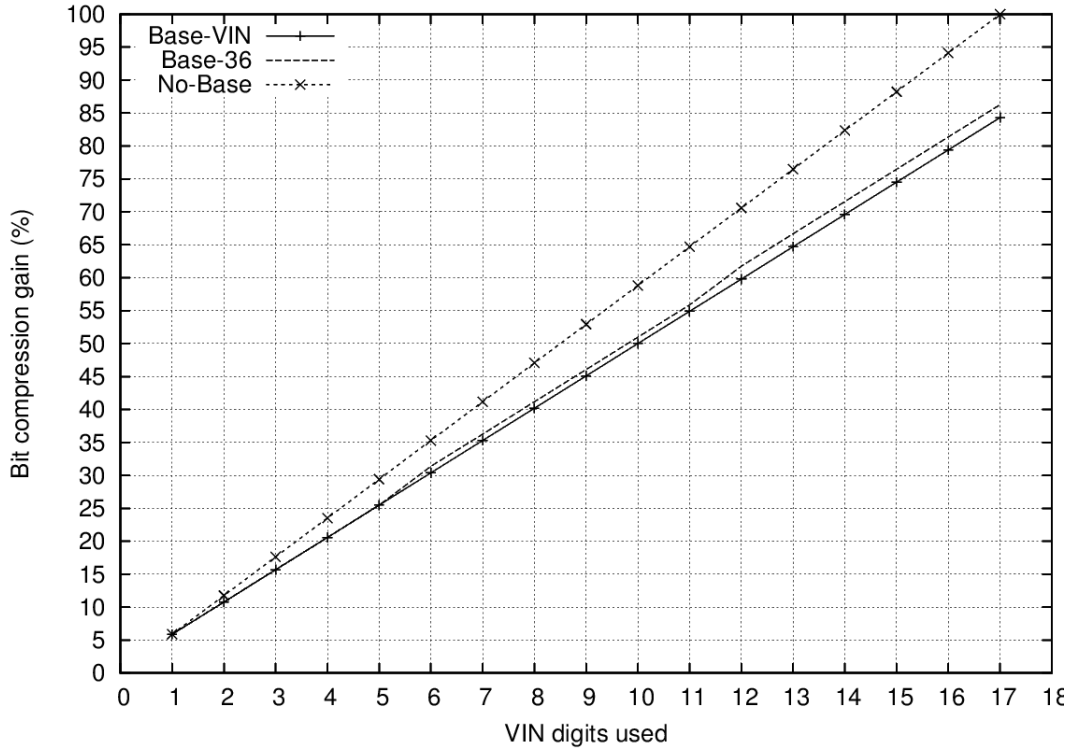


Figure 5.7: Compression bit gain with various numeral systems

Our contribution in this particular topic is *not* on how to use the pseudonyms efficiently but *providing* the possibility to create them. Different 35 bit pseudonym VIS (possibly pseudo-random) could be used on each scope of the global communications. The E2E session is maintained at the point of indirection. Our VIN-to-IPv6 conversion algorithm assures the selected VIS could map with no collisions, given the VIS generation method does not involve one.

If the communications involving the vehicle are global, it makes sense to leave it up to a central authority to select an appropriate pseudonym that does not provoke collisions (cf. Section 5.3). On the other hand, if communications are infrastructure-less (in-vehicle or V2V for instance), a one-way hash method could be a good approach to generate a low-collision probability prefix/address using a pseudonym VIS code (RFC 4941 gives an example using MAC).

5.4.5 Analysis of the solutions

We here compare the MIPv6-NEMO solution to LISP-MN as described in Section 5.3.3. The comparison considers configuration and overhead costs and the end-to-end delay from an arbitrary CN to the MR for both solutions. Note that only the original proposals are compared and therefore no Routing Optimization (RO) schemes are considered in our study.

5.4.5.1 Parameters and evaluation scenario

Table 5.2 sums up the notations used of our model. To compare both MIPv6-NEMO and LISP-MN solutions, we consider the network topologies depicted in Figures 4.7(a) and 5.5 respectively. We suppose that the MR attaches to the network through a wireless antenna and attempts to configure its internal network. We make the additional following assumptions:

- T_{L2} and T_{AU} are the same in the proposed protocols. That is; the link-layer processing and the authentication process are of the same duration.
- We consider that $H_{AR}^{MServ} = H_{AR}^{HA}$ for the sake of fairness in comparison.
- M_{LFN}^{d} the LFN data packet size is the same in the proposed scenarios.

Note that for the Router Advertisement messages, we took into consideration the recommendations of High Mobility scenarios when deciding of the minimum and maximum advertisement timers of RFC 6275.

5.4.5.2 Performance metrics

In this performance study, we are interested in the following:

1. Signaling overhead: It is one of the major considerations for mobility management due to the expensive wireless bandwidth consumed by signaling overhead and resulting delay. We will calculate the average overhead required for registration cost and the binding update with Map- Server and map updating after handover in both MIPv6-NEMO and LISP-MN based solutions.
2. Address configuration delay: It is the time that starts from MR doing a Layer 2 handover and finishes when this MR receives its MNP configuration.
3. End-to-end delay: It is the time for a user packet (sent by the LFN) to reach the other end (CN).

5.4.6 Host mobility model

The MIPv6 and LISP-MN based solutions are compared from the mobility perspective and their use of the VIN6 addressing architecture. To measure the performance of the LISP-MN solution and compare it to legacy MIPv6, we need to take into account the handover frequency, that is responsible for triggering the registration and mapping update process in LISP. Similarly to Chapter 4, we use the model in [142]. The Session-to-Mobility Ratio (SMR) is the relative ratio of sessions arrival rate (new applications/packets) to the user mobility rate. The user mobility rate can be quantified using the *subnet border crossing rate* (μ_{cr}) or the *subnet residence time* ($\eta = 1/\mu_{cr}$). We also the following assumptions to simplify the calculations:

- The subnet residence time (in the MIPv6's AR, or in a xTR's domain) follows an exponential distribution with parameter η.
- The data session duration (at the MR's connected network) also follows an exponential distribution with parameter λ.
- The subnets (or coverage cells) have a circular coverage defined with Radius R_{SN}.
- The vehicle travels with a subnet (or cell) with a direction uniformly distributed in $[0, 2\pi)$ and average speed $\overline{v}$.

Using these notations, we define:

$$\mu_{cr} = \frac{2\overline{v}}{\pi R_{SN}}, \eta = \frac{1}{\mu_{cr}} \tag{5.1a}$$

$$SMR = \rho = \frac{\lambda}{\eta} \tag{5.1b}$$

Table 5.2: Model parameters and notations.

Parameter	Description	Default values
$T_{RA_{min}}$, $T_{RA_{max}}$, T_{RA}	The (min, max) delay between 2 consecutive Router Advertisements	40ms, 70ms (High mobility scenarios of RFC 6275)
T_{RA}	The average delay between 2 consecutive Router Advertisements	
T_{DAD}	The delay required to perform a Duplicate Address Detection check	1 sec
T_{L2}, T_{AU}	Link-layer and Authentication latency	50, 550 ms
M^c_{RA}, M^c_{NS}, M^c_{Mreg}, M^c_{Mreq}, M^c_{Mrep}, M^c_{SMR}, M^c_{BU}	The size of the control message of ICMPv6 Router Advertisement, Neighbor Solicitation, LISP Map-Register, LISP Map-Request, LISP Map-Reply, LISP SMR, BU/BA (MIPv6) messages	80bytes, 80bytes, 96bytes, 96bytes, 96bytes, 96bytes, 56bytes
M^d_{LFN}	The size of a data packet sent by an LFN	1KBytes
M_{ENC}	The size of the encapsulating tunnel	40 bytes
B_{V2I}, B_F	Bandwidth for V2I and Fixed Infrastructure links	11Mbps, 100Mbps
R_{V2I}, R_F	Propagation for V2I and Fixed Infrastructure links	40ms, 0.5ms
$\overline{v}$, R_{SN}, $\mathbf{N}$	Vehicle's average speed, Radius of cell's circular coverage, Total number of cells (subnets)	45km/h, 500m, 100
T_u, T_l	The latency of processing a mapping update (resp. a mapping lookup)	500 msec [44]
C_u, C_l	The cost of processing a mapping update (resp. a mapping lookup)	–
α, β	Unit cost (factor) of processing a mapping update (resp. a mapping lookup) with the Mapping Server (resp. the Mapping System)	3, 2 [89]
N_{MR}, N_{MD}	Number of active MR per Manufacturer Domain (resp. Number of Manufacturer Domains in the LISP domain)	–
H^{HA}_{AR}, H^{MSrv}_{AR}, H^{xTR}_{AR}, , H^{MSrv}_{MS}, H^{CN}_{xTR}, H^{CN}_{HA}, H^{CN}_{AR}, H^{MS}_{xTR}	Average number of hops from AR to HA, AR to Mapping Server, AR to CN's xTR, Mapping Server to the Mapping System, CN to its xTR, xTR to the Mapping System (resp.)	15, 15, 12, 5, 5, 10, 17, 5

Assuming the domains have N cells, intra-domain cell crossing triggers an intra-domain handover procedure and inter-domain cell crossing triggers an inter-domain handover procedure. We also assume that the MR obtains an RLOC (in LISP-MN) or a CoA (in MIPv6) with Neighbor Discovery IPv6 auto-configuration procedure, and a new address is obtained at each intra-domain handover. We have the intra-domain and inter-domain handover probability and expected numbers of handovers as:

$$P_{intra} = \frac{1}{1+\rho}, P_{inter} = \frac{1}{1+\rho\sqrt{N}} \tag{5.2a}$$

$$E_{intra} = \frac{1}{\rho}, E_{inter} = \frac{1}{\rho\sqrt{N}} \tag{5.2b}$$

5.4.6.1 Modeling for signaling cost

Maintaining an up-to-date binding at the Mapping System is essential for the LISP protocol. An accurate up-to-date mapping allows the xTRs in the domain to locate and forward the packets to the destination MN regardless of its current location, just by querying its ID. Throughout its journey across the LISP domain, the MR will trigger configuration and mobility related control messages. Using the border crossing probabilities in Equations 5.2, we define the total signaling cost as:

$$C^{total} = (E_{intra} - E_{inter}) \times C_{intra} + E_{inter} \times C_{inter} \tag{5.3}$$

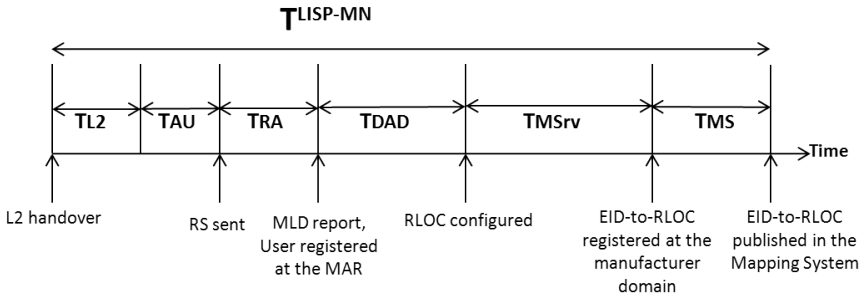


Figure 5.8: Time diagram for the Addressing Configuration Delay in LISP-MN.

Figure 5.8 shows the time diagram for address configuration in the LISP-MN solution. The figure also illustrates the sequence of control plane operations mandatory for the journey of one packet from the CN to reach the LFN inside the vehicle. Basically, the MR has to register into the LISP domain, then the CN's xTR to lookup for the proper RLOC to deliver the CN's packets destined to the VIN6 EID of the MR. In case of a handover, the MR needs to notify the xTR of the new mapping to retrieve in order for the communication to continue. The message exchange diagram is detailed in Figure 5.6. This leads to the equation 5.4

$$C_{intra}^{LISP-MN} = C_{inter}^{LISP-MN} = C_{AC} + C_{Reg} + C_{Pub} + C_{Update} + C_{Lookup} \tag{5.4}$$

Where C_{AC} is the cost of the address configuration as the MR registers itself in the domain for the first time after a roaming. This signaling overhead includes the size of a Router Advertisement message to auto-configure one topologically correct RLOC, and the size of Neighbor Solicitation message to ensure no other MR in this network formed the same RLOC (Duplicate Address Detection). Other control messages in the address configuration phase include the *registration* at the Mapping Server (C_{Reg}) and the *publishing* of this new mapping at the federated Mapping System (C_{Pub}).

As for the C_{Update}, it is the cost of updating one CN's xTR router of the current location of the MR in order for the xTR to update its binding cache (C_{Lookup}). The *recovery time* for an ongoing session in this case, is the time that separates the moment the SMR is sent from the MR to the CN's xTR and the moment the xTR receives an updated cache entry for this MR. The recovery time determines the amount of packets the xTR puts "on hold" (in a buffer) before forwarding them to the final destination. We here assume that the data structure used to store the mappings in the Mapping System uses a tree-based data structure, with a complexity of O(Log n) for lookup, insertion and deletion of data records. Several schemes have been proposed for LISP mapping systems in the literature, for example [119] uses such approach. Hence:

$$C_{AC} = M^c_{RA} + M^c_{NS} \tag{5.5a}$$

$$C_{Reg} = 2 \times (M^c_{Mreg} \times H^{MSrv}_{AR}) + C_u \tag{5.5b}$$

$$C_{Pub} = 2 \times (M^c_{Mreg} \times H^{MS}_{MSrv}) + C^{'}_u \tag{5.5c}$$

$$C_{Update} = M^c_{SMR} \times H^{MR}_{xTR} \tag{5.5d}$$

$$C_{Lookup} = 2 \times (M^c_{Mreq} \times H^{MS}_{xTR}) + C_l \tag{5.5e}$$

$$C_u = \alpha \times \log(N_{MR}) \tag{5.5f}$$

$$C^{'}_u = \alpha \times \log(N_{MD} \times N_{MR}) C_l = \beta \times \log(N_{MD} \times N_{MR}) \tag{5.5g}$$

As for the MIPv6-NEMO based solution, the MR has to configure a care-of-address before updating the binding at the Home Agent, in order to establish the forwarding plane from the VIN6 Home address (anchored at the Manufacturer Domain) to the current CoA. In case of a handover, with no routing optimization plane, the MR does not need to notify the CN. The study of MIPv6-NEMO with VIN6 addressing architecture signaling overhead is detailed in Chapter 4.

Figure 5.9 illustrates the result of varying the session to mobility ratio on the signaling overhead for both LISP-MN and MIPv6-NEMO based solutions. When the SMR is small, the mobility rate is larger than the session arrival (actual communications). In this case, the signaling due to the MR changing its point of attachment is higher. However, when the SMR is bigger, the overall mobility-related signaling decreases as the consequence of the less frequent subnet changes of the MR. The signaling overhead is 2.987 times (almost 3 times) higher in the case of the LISP-MN based solution than MIPv6 based solution when the $SMR = 0.2$. This is due to the control plain in the LISP protocol, in particular the Mapping System which introduces more exchanges between parties in order to maintain an up-to-date RLOC-to-VIN6 EID binding for the data path. This control plain can be reduced in part if the Mapping Server that is currently placed in the manufacturer domain (in our proposal) is moved to the federated domain. The advantage for the manufacturer domain to host a Mapping Server is to track its vehicle fleet and contact it if necessary without access to the federated Mapping System. In this model, we considered the federated mapping system to host the mappings of MRs only. In a realistic experiment, the mapping system would maintain heterogeneous entries for other Mobile and Fixed nodes, increasing the Update and Lookup operations cost. Hence the importance of choosing efficient data structures and advanced mapping approaches to reduce the cost of these operations [44]. Another effective solution to reduce the signaling cost is to re-locate some parts of the LISP system closer to the edge (sub-mapping system for instance). This optimization could be inspired from the earlier research on the DNS system.

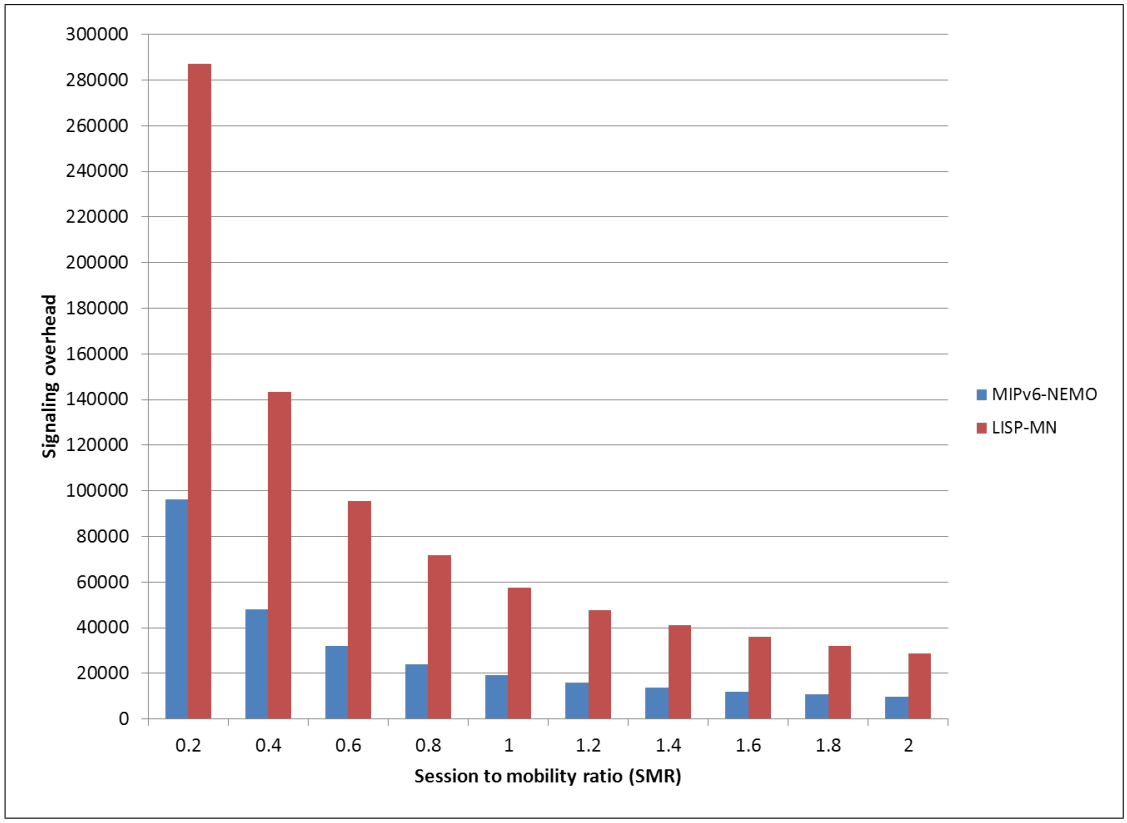


Figure 5.9: Signaling load for LISP-MN vs. MIPv6-NEMO based solutions as a function of SMR.

5.4.6.2 Modeling for configuration delay

Figure 5.8 shows the time diagram for address configuration in the case of LISP-MN solution. Using the border crossing probabilities in Equations 5.2, we define the total address configuration delay as:

$$T^{total} = (P_{intra} - P_{inter}) \times T_{intra} + P_{inter} \times T_{inter} \tag{5.6}$$

The configuration delay depends on the bandwidth, the propagation delay, the distance between and the control messages involving the MR and its mobility architecture components.

The total configuration delay can be formulated as:

$$T_{Intra}^{LISP-MN} = T_{Inter}^{LISP-MN} = T_{RLOC} + 2 \times T_{Reg} + 2 \times T_{Pub} + 2 \times T_u \tag{5.7}$$

Where T_{RLOC} is the delay to configure a topologically correct RLOC, T_{Reg} is the delay to register the EID-to-RLOC binding at the Mapping Server of the Manufacturer Domain (2 messages, Register and ACK), and T_{Pub} (2 messages, Register and ACK) the delay to "publish" this binding at the federated Mapping System. As for the RLOC delay:

$$T_{RLOC} = T_{L2} + T_{AU} + T_{RA} + T_{DAD} \tag{5.8a}$$

$$T_{RA} = \frac{T_{RA_{max}}^2 + T_{RA_{min}}^2 + T_{RA_{max}} \times T_{RA_{min}}}{3 \times (T_{RA_{max}} + T_{RA_{min}})} \tag{5.8b}$$

The Mapping Server registration is the next step. This operation depends on the size of the control message, the number of MRs handled at the manufacturer domain and also the

bandwidth.

$$T_{Reg} = (\frac{M^C_{Mreg}}{B_{V2I}} + R_{V2I}) + H^{MServ}_{AR} \times (\frac{M^C_{Mreg}}{B_f} + R_f) \tag{5.9a}$$

The last step, is to publish the new VIN6-EID-to-RLOC mapping and make globally accessible for the CNs to lookup. This step involves the Mapping Server at the manufacturer domain and the Mapping System.

$$T_{Pub} = H^{MS}_{MServ} \times (\frac{M^C_{Mreg}}{B_f} + R_f) \tag{5.10a}$$

Thanks to equations 5.8, 5.9, and 5.10 the configuration delay as defined in equation 5.7 in LISP-MN is now fully defined. Note that, T_u is counted twice, as the update occurs on two different mapping systems. As for the MIPv6-NEMO based solution, the configuration delay is as given in Chapter 4.

Figure 5.10 illustrates the evolution of address configuration delay in LISP-MN and MIPv6-NEMO through different mobility conditions. The addressing configuration delay in LISP-MN solution is 0.5 sec higher when compared to the MIPv6-NEMO solution if the $SMR = 0.2$ and the gap is reduced as the SMR increases. This corresponds to the phases where the control overhead is higher. The additional signaling observed in the first metric is mainly responsible for this difference. Indeed, as described before, the process of obtaining the RLOC in LISP is identical to obtaining the CoA in MIPv6 and both solutions make use of the VIN6 PIA to anchor the MR's internal network using one RLOC/CoA address. The difference in signaling occurs in the registration process (binding) and the handover. Indeed, 4 registration related messages are triggered by one MR after it changes the point of attachment,assuming the Mapping Server is at the manufacturer domain and the Mapping System in a federated common location. It is only 2 messages for the MIPv6 solution with the Home Agent placed at the manufacturer domain. Here also, the overall address configuration delay in LISP-MN based solution can benefit from an architectural co-location of the Mapping Server and Mapping System and an efficient data storage for the Update and Lookup operations.

5.4.6.3 Modeling for end-to-end delay

We define the total end-to-end delay as:

$$T^{E2E} = (P_{intra} - P_{inter}) \times T^{E2E}_{intra} + P_{inter} \times T^{E2E}_{inter} \tag{5.11}$$

The e2e delay depends on the bandwidth, the propagation delay, and the distance between the MR and its mobility architecture components.

Figure 5.11 illustrates the time diagram for Metric 3 in the case of LISP-MN. The data sent from the LFN to the CN arrives at the MR which runs the LISP-MN daemon (MR is light weight xTR). The MR performs a lookup of the CN's EID from the Mapping System in order to retrieve its xTR's RLOC. The packets can now be encapsulated directly to the destination xTR before being delivered to the final recipient, the CN. Note that the CN also communicate with the MR or one of its LFNs without traversing the Manufacturer Domain. This is not the case in the first solution based on MIPv6-NEMO, where the HA is also part of the data plane.

The E2E delay for this packet can now be expressed as follows:

$$T^{LISP-MN}_{Intra} = 2 \times T_{Map} + T_l + T_{For} \tag{5.12}$$

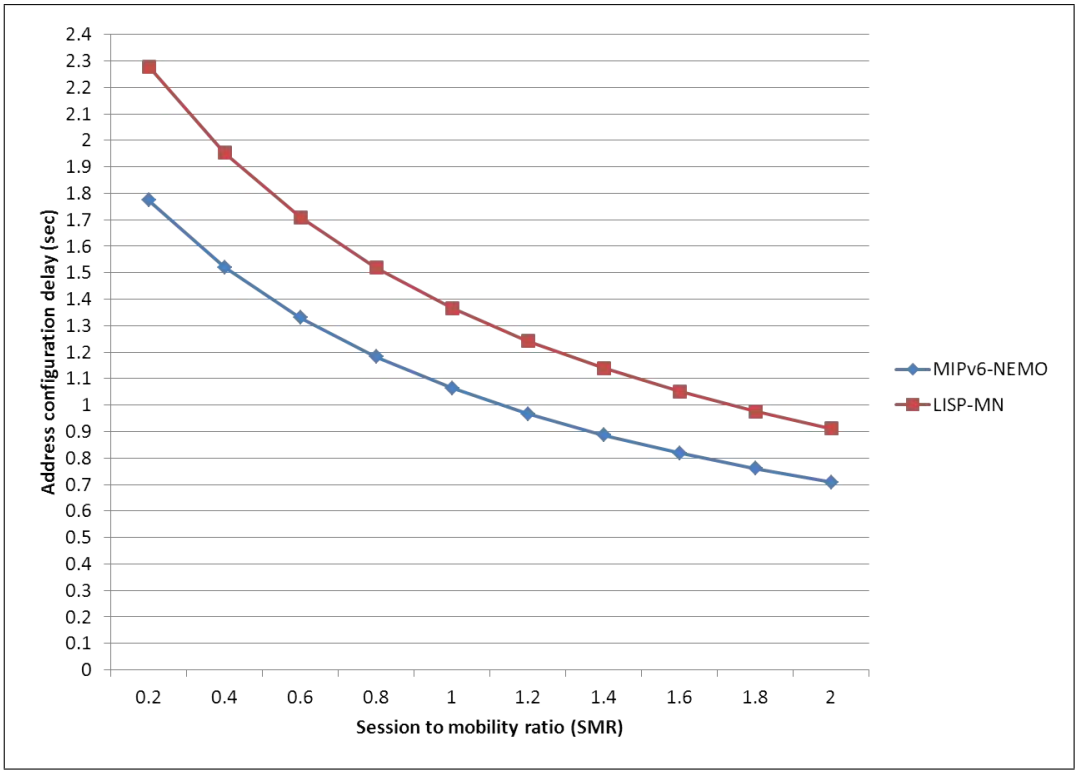


Figure 5.10: Address configuration delay for LISP-MN vs. MIPv6-NEMO based solutions as a function of the SMR.

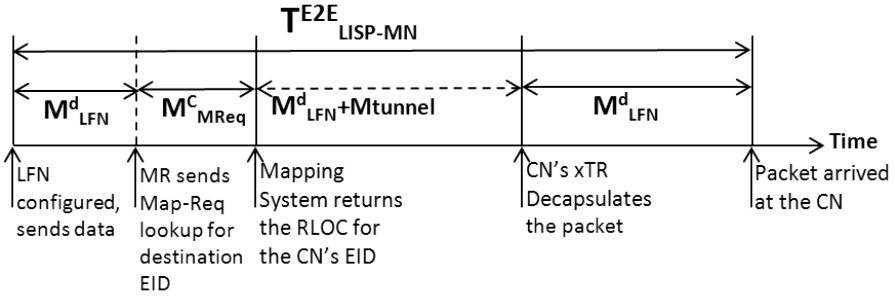


Figure 5.11: Time diagram for the end-to-end Delay in LISP-MN.

And:

$$T_{Inter}^{LISP-MN} = T_{SMR} + T_{Intra}^{LISP-MN} \tag{5.13}$$

Where:

$$T_{MAP} = (\frac{M_{Mreq}^{C}}{B_{V2I}} + R_{V2I}) + H_{AR}^{MS} \times (\frac{M_{Mreq}^{C}}{B_f} + R_f) \tag{5.14a}$$

And:

$$T_{For} = (\frac{M_{LFN}^{d} + M_{ENC}}{B_{V2I}} + R_{V2I}) + H_{AR}^{xTR} \times (\frac{M_{LFN}^{d} + M_{ENC}}{B_f} + R_f) + H_{CN}^{xTR} \times (\frac{M_{LFN}^{d}}{B_f} + R_f) \tag{5.15}$$

Finally:

$$T_{SMR} = (\frac{M^c_{SMR}}{B_{V2I}} + R_{V2I}) + H^{xTR}_{AR} \times (\frac{M^c_{SMR}}{B_f} + R_f) \quad (5.16)$$

This metric is also defined for MIPv6-NEMO in Chapter 4.

Figure 5.12 illustrates the evolution of end-to-end delay in LISP-MN and MIPv6-NEMO as a function of the SMR. The end-to-end delay for the data plane in LISP-MN solution is higher than the MIPv6-NEMO solution in higher mobility conditions. This is due to the additional EID-to-RLOC resolution operations that the xTR router must perform before *optimally* routing the packets to the *current* location of the MR. In comparison, The CN in the MIPv6 solution, regardless of the current location of the MR, routes the packets to the HA where the VIN6 PIA is topologically anchored. The gap between the two protocols closes slowly as the SMR is bigger, and therefore the MR less mobile.

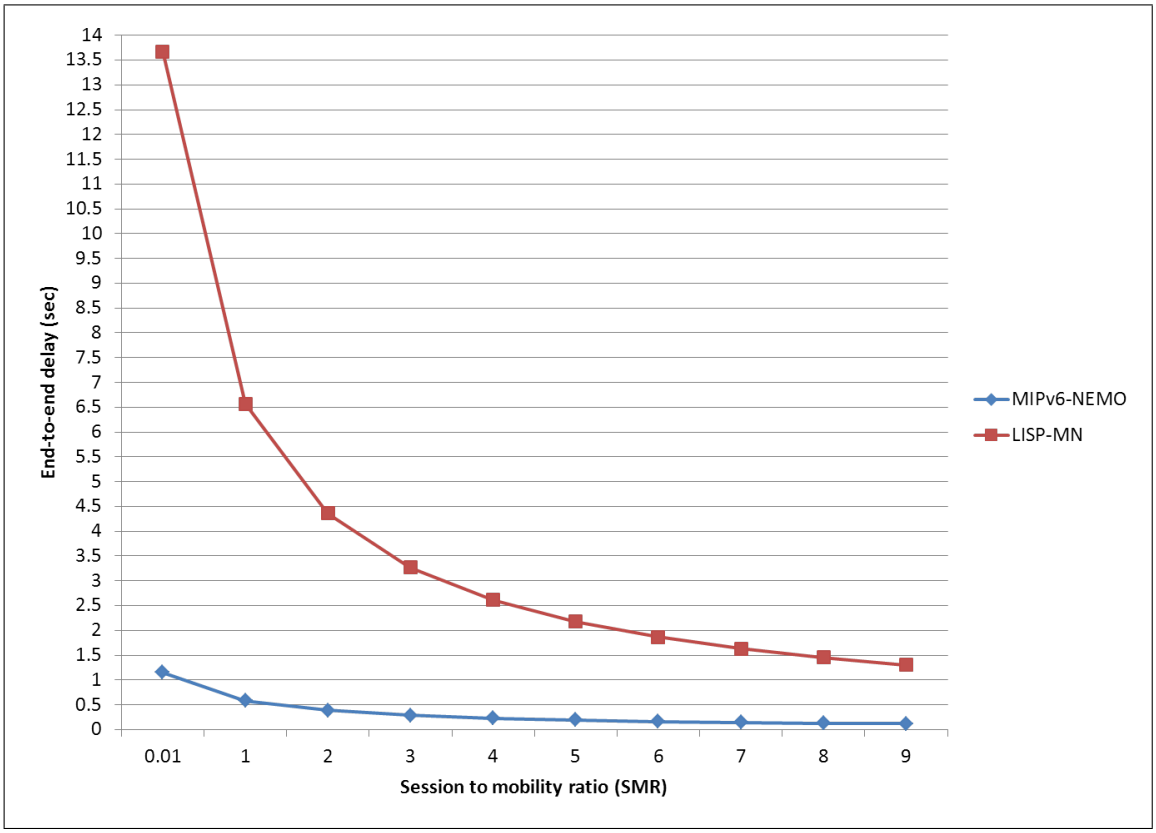


Figure 5.12: End-to-end delay delay for data plane in LISP-MN vs. MIPv6-NEMO based solutions as a function of SMR.

5.5 Conclusion and future work

Recent FI initiatives advocate to include new business entities and enhance market-penetration of IP-based applications (known as economics tussle space). The VIN-based architecture introduces the vehicle manufacturer as a new network and services domain. We propose through our VIN-based hierarchical PI addressing space to provide for the identification of up to 2^{51} distinct vehicles. The uniqueness conservation from VIN identifier to the VIN-based address, is of paramount importance when considering addressing collisions at large scale. We also show

that our addressing architecture is compatible with existing MIPv6 based solutions and also evolutionary network-based Future Internet architectures, namely LISP.

From an addressing/naming perspective, one major difference in using VIN6 with MIPv6-NEMO is that the VIN6 addressing was also used to route the packets and reach the destination. Indeed, by advertising the VIN6 PIA in a BGP message into the global routing system, correspondent nodes' packets routing is based upon the presence of such routes in the DFZ. The benefit of using VIN6 here is that the addressing can be aggressively aggregated. When used with the LISP architecture, VIN6 can only be used as Endpoint Identifiers and not Routing Locators. The VIN6 addressing only serves the purpose of identifying the vehicle and its inside network.

From a routing perspective, in the LISP based solution that we propose, the CN's packets can avoid the manufacturer domain and be routed optimally through shortest RLOC-based path, unless the vehicle is topologically present inside the manufacturer's domain. The manufacturer domain through its hosted Mapping Server follows the locations of the vehicle but not the content of the packets sent from the vehicle. This is different in MIPv6 based solution where the data path and the control path are the same and traverse the Home Agent hosted in the manufacturer domain.

The Endpoint Identifier is tied to the notion of pseudonym. While we do not specify how a pseudonym should be created, we provide for a VIS identification space that includes temporary VIS codes depending on the use case. For global communications, a central selection strategy of pseudonyms to avoid duplicates could be chosen, while local and random VIS codes could apply for local communications. In order to propose efficient and viable deployments, security and privacy threats need to be assessed for both solutions. Some studies already tackle some of these issues [97] [96].

In order to understand the effect of changing addressing architectures in Future Internet and mobility solutions, one perspective would be to compare VIN6 with other Future Internet host-based and network-based schemes. HIP and ILNP being present at the IETF and currently developed in the literature with existing prototypes are good candidates. In order to approach real-life deployments of these solutions, simulation is an important step after analytical analysis. For instance, authors of [54] recently proposed a LISP and LISP-MN implementation for OMNET++ simulator.

Chapter 6

Applying Locator/Identifier separation techniques for Group IP-Based Vehicular Communications

Recent years witnessed the advent of IP-based vehicular networking over several heterogeneous wireless transmission technologies: 802.11a/p, WAVE, UMTS and more recently LTE/LTE-A. However, the operation and performance of IP in those networks are still subject to improvement [10]. IP-based mobility management is of paramount importance in this context, especially for vehicular networks. Recently, standard development bodies proposed protocol stacks supporting IPv6 communications along with safety and emergency time-critical protocols [32]. Infotainment, fleet management, remote diagnostic, traffic offload or distributed games are implemented on Vehicle-to-Infrastructure (V2I) or Vehicle-to-Vehicle (V2V) settings [127]. More use cases, such as sharing of perception data, position information, vehicle tracking, and collision avoidance can profit from V2I and V2V communications and interact in meaningful ways [215]. Nonetheless, operation and performance of IPv6 over WAVE/802.11p standard must be enhanced [13].

In the context of Vehicle-to-Internet communications, the in-vehicle communications have also a revolution of their own: including IP as a way to reach embedded machines from a remote infrastructure location. Indeed, in-vehicle network is now provided with IPv6 supporting protocol stacks from all major SDOs (IEEE, ETSI, ISO, and C2C) and include mobility support at the network-layer through RFC 6275 Mobile IPv6 and RFC RFC 6276 Network mobility extension. An embedded Mobile Router (MR) may use several wireless egress interfaces (802.11p, LTE) which makes the MR multi-homed [32]. Mobility management approaches in the standards have evolved from centralized approaches (MIPv6 and PMIPv6) to distributed approaches (DMM) to meet the needs of operators and users. We observed in Chapter 4 how the Network Mobility extension is a requirement to meet for this mobility management protocol to support vehicular communications. In a related issue, recent Future Internet (FI) research initiatives consider naming and addressing challenges for vehicular networks as well [214] [65]. In the previous chapter, we discussed the importance of separating locator from the identifier in the IP addressing paradigm. In line with this approach, we then proposed to apply the LISP-MN protocol to vehicle-to-Internet communication through our proposal: VIN6 Provider Independent Addressing.

In this chapter, we consider another aspect of major concern for IP-based communications in quickly changing topologies: dynamic topological addressing auto-configuration mechanisms. We first review current trends in the topic: prefix delegation, neighbor discovery enhancement, and geonetworking. We then pose the problem Group Vehicular communications in Future

Vehicular Internet (FVI) by providing the motivations behind our approach. We then present our proposal for to extend LISP-MN with the support of group vehicle-to-Internet communications. In detail, our contributions in this chapter are:

- Review of IPv6 vehicle auto-configuration techniques.
- Using Future Internet paradigm through VIN codes as hierarchical vehicular identifiers.
- Mapping VIN to IPv6 numbering space with an algorithm that achieves uniqueness conservation, and allow quick vehicle cluster communications and reachability.
- Integration with LISP-MN protocol
- Comparison to existing techniques

6.1 Taxonomy and terminology of IPv6 configuration techniques for vehicular group communications

IP-based communications are key to leverage market penetration and deployment costs of the 802.11p architecture. To that end, the protocol stacks proposed by standardization bodies (IEEE, ETSI, ISO) include mandatory IPv6 support. From a networking standpoint, the connectivity problem of end-to-end IP-based applications is usually addressed by the use of Mobile IPv6 with NEtwork MObility extension (MIPv6/NEMO), in particular for V2I communications [31]. Nonetheless, as argued the authors of [28], the main functional requirement for the support of IP-based vehicular communications is the *uniqueness of the globally-scoped* address that the MR auto-configures on its egress interface. Therefore, MIPv6/NEMO guarantees this requirement at the expense of short-lived sessions due to its control plane overhead. Thus, the need for quick auto-configuration mechanisms that can exploit those short communication windows.

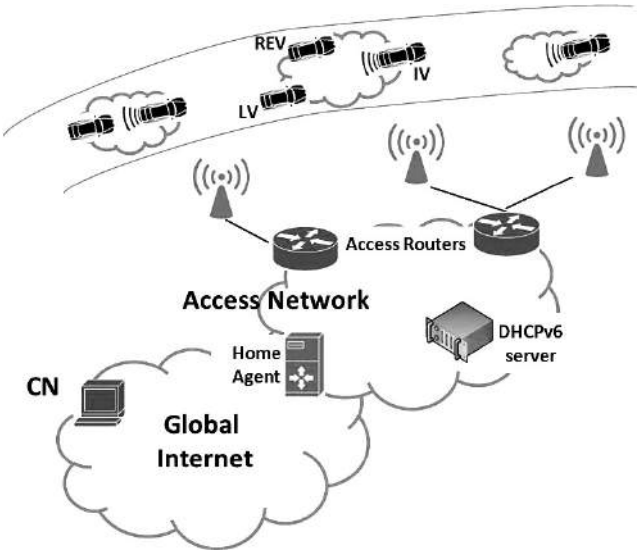


Figure 6.1: IP-based Group Vehicular Communications on a V2V2I setting

Beyond usual V2I and V2V architectures, recent proposals argue for an extended IP-based group (cluster) vehicle to infrastructure communications paradigm. Figure 6.1 illustrates an

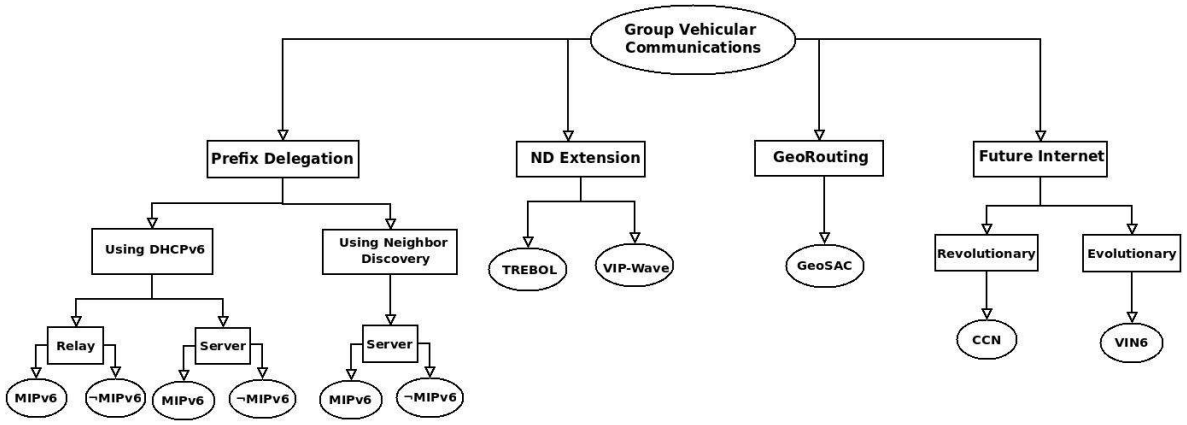


Figure 6.2: Taxonomy of IPv6 configuration techniques for vehicular group communications

example of such settings. In [174], authors discriminate functional roles of vehicles based on their ability to connect directly to the infrastructure through a long or short range egress interface. Thus, Internet Vehicles (IV) are directly connected to the infrastructure/Internet through an LTE/802.11p on one egress interface while it shares this access on another egress interface. Range Extending Vehicles (REV) play the role of relays towards the infrastructure or IVs; eventually, a Leaf Vehicle (LV) at the end of the chain would have access to the infrastructure. This is a generalization of the pattern proposed in the VANET literature through different terms, *relaying* being more frequent [31] [127] [136] [91].

Using the lexical field of VANET, Figure 6.1 presents a topology either called a *cluster* or *V2V2I*, depending on the context. In the IP terminology (NEMO in particular) these structures can be referred to as *nested* networks. While both terminologies are correct in our study, we prefer the terms *group* or *V2V2I* communications, which can also be found in the literature of this topic. In practice, V2V2I may be enabled by the recent evolution of 802.11p related standards, field deployments and experiments. While 802.11p Road Side Units (RSUs) continue their deployment, the support of 802.11p interface may become mandatory in vehicles (cf. eCall [116]), introducing LVs and REVs to the road. Recently car manufacturers proposed V2I communications through LTE due to higher market penetration and large coverage, making IVs a reality.

The conservation of an IPv6 end-to-end communication model among heterogeneous nodes and the support of multi-hop vehicular architecture are the core topics of this chapter. Figure 6.2 summarizes the main IPv6 configuration techniques for vehicular group communications. We distinguish 4 main trends: Prefix delegation (PD), Neighbor discovery (ND) extension, Geographical routing, and Future Internet initiatives.

6.1.1 Prefix delegation

Group IP-based communications may involve in-vehicle embedded networks. To that end, each vehicle needs to have a proper *unique* a *globally-scoped* IPv6 prefix for its internal network composed from fixed machines and IP-capable devices, and mobile temporary devices (HUDs, tablets, phones and more). This section presents state-of-the-art for prefix delegation through DHCPv6 with its PD extension. After reviewing this technique, we propose our own alternative prefix delegation mechanism through ND.

6.1.1.1 Limits of DHCPv6-PD

Two cases can be considered with DHCPv6: the IV is either DHCPv6 server or DHCPv6 relay. The REV is relay and the LV is client in both cases.

DHCPv6 solution depends on a 4-way handshake. The LV sends a *Solicit* message to discover the DHCPv6 servers on the link (IVs); the IV responds with an *Advertise* message. The LV sends a *Request* message including a PD option, to which the IV replies by a *Confirm* message with the delegated prefix. The LV can now advertise the delegated prefix inside the vehicle.

If the IV implements a DHCPv6 *relay*, additional messages will be triggered along the chain of relays until a server is reached in the infrastructure through the Access Router. Figure 6.3 depicts the messages exchange corresponding to this case.

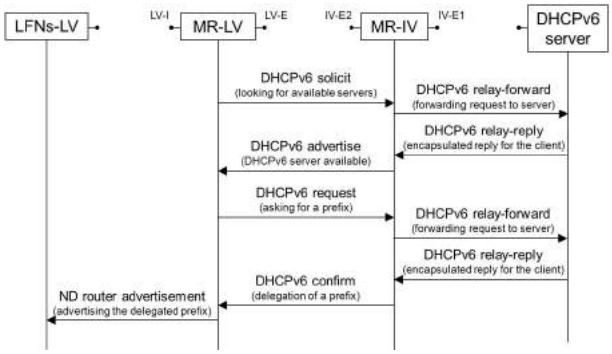


Figure 6.3: Auto-configuration using DHCPv6 with IV as DHCPv6 relay

Figure 6.4 illustrates the Handover procedure, the involved network entities and timing diagram for Prefix Delegation through DHCPv6 protocol combined to Mobile IPv6 for mobility management. After the IV obtains a Care-of-Address in the new subnet, it tries to register the new CoA-to-HoA binding at its HA. The IV then solicits a pool of IPv6 addresses that are anchored at the HA (Home Network Prefixes, HNPs). The IV can now maintain this addressing pool and acts as a DHCPv6 server for the potential LV clients. Note that the use of DHCPv6 prefix delegation with rapid commit (2 messages) can be an optimization.

The DHCPv6-PD cannot be included in the V2V2I solution space. Moreover, the suitability of the DHCPv6 protocol in any vehicular context is very questionable, especially on the following points.

The number of messages exchanged. The highly-mobile context supposes short communication opportunities for LVs, which requires short messages exchanges for auto-configuration techniques. This requirement makes DHCPv6 *unsuitable* for V2V2I, due to a high number of messages exchanged (Figure 6.3). Moreover, the ETSI recommends *not* using a stateful address configuration mechanism (namely, DHCPv6) in a vehicular environment [68].

Deployment complexity. The server delegating the prefix needs to update every hop (router) towards the requesting LV. DHCPv6-PD standard mentions it as an additional out-of-band control plane, performed using routing protocols (e.g.; OSPF) or such. Our Figure 6.2 taxonomy illustrates this with two possibilities for the IV: running MIPv6-NEMO or not. With MIPv6-NEMO, the PD technique does not require routing update from the Home Agent (HA) to the IV. Only the HA needs to bind the delegated prefixes to IV's Care of Address (CoA). Not running MIPv6-NEMO, requires the update of the Access Router (AR) and relays with the delegated prefixes, which needs to be uninstalled after a handover. This solution is not addressed in this paper due to the complexity of the control plane.

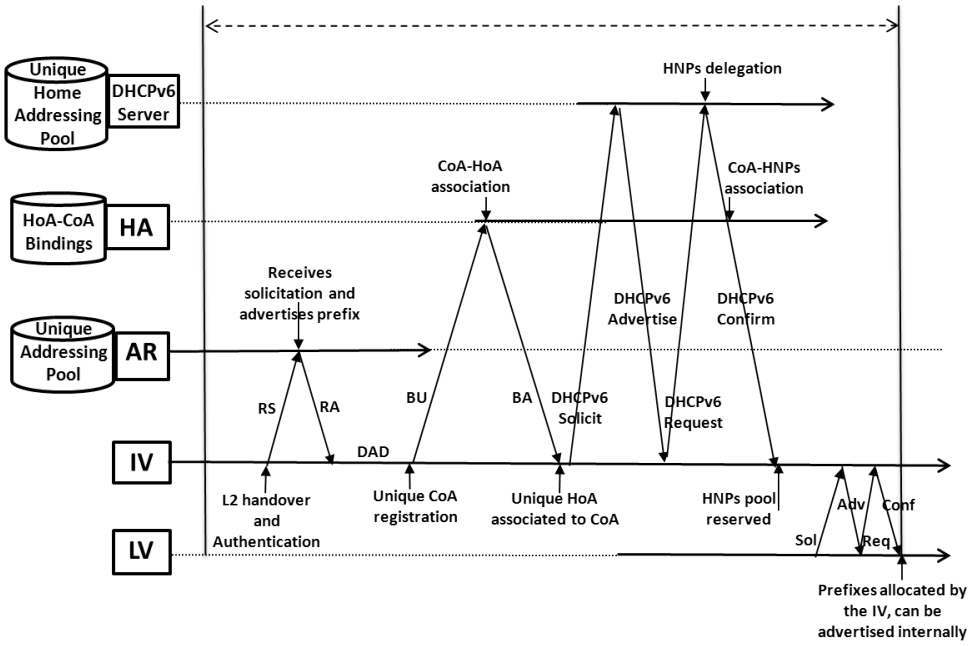


Figure 6.4: Handover procedure and timing diagram for Prefix Delegation through DHCPv6 protocol.

Additionnal software required. Using DHCPv6 to auto-configure the devices inside the LV requires that both the LV and the IV implement the DHCPv6 protocol on their MR (depending on the roles). The problem is that vehicular embedded devices are most of the time hardware and resource constrained (processor power, available memory) and implementing an additional software such as DHCPv6 may not always be possible.

6.1.1.2 Neighbor Discovery alternative

As a default IPv6 stack protocol, each IPv6-enabled device implements ND. Using ND with our PD option reduces the number of messages that are exchanged between the LV and the IV, and reduces the auto-configuration latency.

Message exchange diagram is illustrated in Figure6.5. The LV uses PD option in the *Router Solicitation (RS)* message to asks for prefixes, while the IV delegates prefixes using this option in the *Router Advertisement (RA)* message. Routers that provide the ND-PD service may be discovered via periodic *RA* messages or immediate *RS* messages. The LV when receiving an *RA* message including the PD flag, knows that the ND-PD service is provided through the announcing router (the IV in our context). This feature reduces auto-configuration through PD to only two necessary messages in comparison to DHCPv6.

Figure 6.6 illustrates the Handover procedure, the involved network entities and timing diagram for Prefix Delegation through ND protocol combined to Mobile IPv6 for mobility management. As the ND protocol runs on one hop neighbors only, we still rely on the DHCPv6 protocol to request an HNP pool for the IV after it completes its registration. The IV can now maintain this addressing pool and acts as a delegating router for the potential LV clients in its cluster.

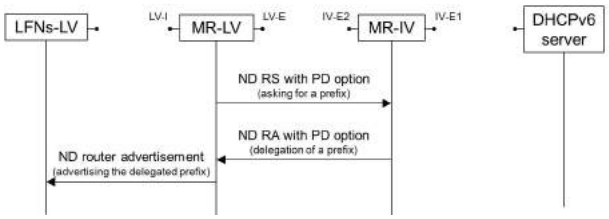


Figure 6.5: Locally Fixed Nodes (LFNs) auto-configuration using ND-PD

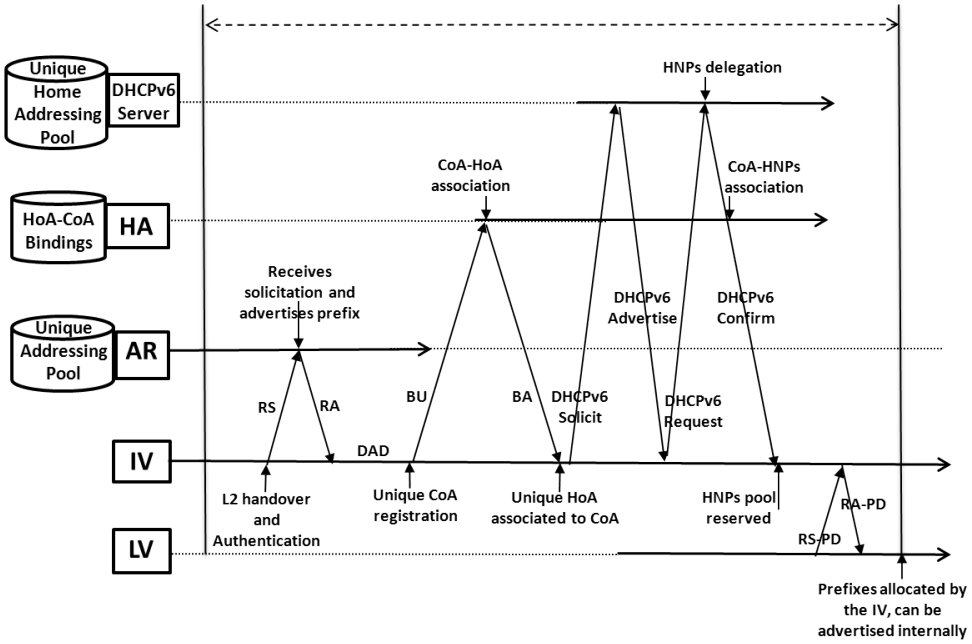


Figure 6.6: Handover procedure and timing diagram for Prefix Delegation through Neighbor Discovery protocol.

6.1.2 Neighbor Discovery extensions

Apart from prefix delegation, the second category of our taxonomy explores the proposals that extend standard Neighbor Discovery protocol. The objective is to tailor ND for IP vehicular communications and supporting high-mobility scenarios. In this area of work, we mention: TREBOL [91] and VIP-Wave [31].

TREBOL is a tree-based and configurable protocol which benefits from the inherent tree-shaped nature of vehicle to Internet traffic to reduce the signaling overhead. Based on an augmented version of Router advertisement messages (Configuration Messages, CM), TREBOL enhances standard ND to extend the RSU announcements on the roadside to reach nearby vehicles. This allows the neighboring vehicles to reach the infrastructure even beyond RSU radio coverage area. TREBOL defines a backoff timer that the IV has to wait before forwarding the CM. This timer is a function of current speed and position to create optimal sized clusters

$$T_{backoff} = \frac{\|((\|pos - sendPos\|) - prefR)\|}{R} \times D_{pos} + \frac{\|speed - prefS\|}{maxSpeedDiff} \times D_{speed}$$

While the main contribution of the TREBOL approach is efficient routing through tree-shaped topologies, the addressing aspect is less present. Indeed, this proposal assumes the responsibility of prefix uniqueness to the RSU's (no infrastructure-less communications), and the Duplicate Address Detection (DAD) operations to be unnecessary since MAC addresses are used in auto-configuration (MAC can be spoofed). In addition, the in-vehicle embedded network configuration is not treated.

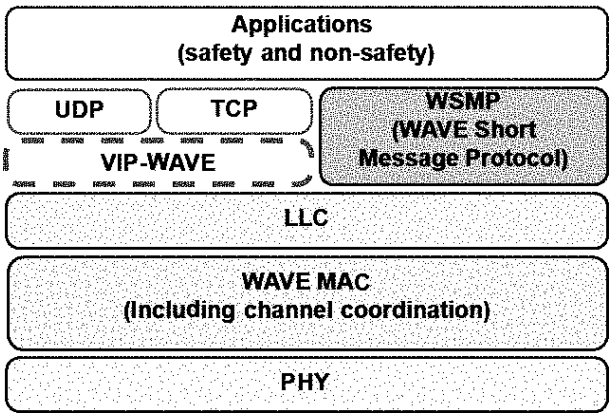


Figure 6.7: VIP-WAVE reference protocol stack

Figure 6.8 illustrates the Handover procedure, the involved network entities and timing diagram for address configuration through ND protocol. Note that the authors do not claim the use of any mobility management protocol and rely on Configuration Messages to relay the prefix announcement from the Infrastructure. The obtained prefix can only serve for one configured address in the LVs and IVs.

Conceptually similar to this approach, VIP-WAVE [31] defines lightweight vehicular-specific Neighbor Discovery protocol for IEEE 802.11p/WAVE. In particular, this approach tackles the DAD problem and supports multi-hop communications between vehicles. For DAD, VIP-WAVE distinguishes non-extended services (not mobile) and extended services (mobile through PMIPv6) and relies on MAC addresses. In-vehicle embedded network configuration is not treated.

Figure 6.9 illustrates the Handover procedure, the involved network entities and timing diagram for address configuration through VIP-WAVE approach. This solution assumes mobility management support for the IV and LV through PMIPv6 protocol. In the absence of a direct connection to the RSUs, the LV searches for a nearby IV to relay its packets to the infrastructure. After sending a WAVE Service Announcement relay request message (WSA) to a nearby IV, this IV relays the request to the connected RSU in order to update the mapping of this LV as topologically connected to the IV. The IV can then confirm the relay request to the LV through WSA relay confirm message.

6.1.3 GeoNetworking

IPv6 in Geographic networking (GeoNet) [127] can be described as a two-level addressing approach. In an IP session, the vehicles use the geographic coordinates to reach a neighboring vehicle or the infrastructure; the IPv6 destination address is not used. When the packet reaches the RSU, the GeoNet header is ripped and the packet routed based on the IPv6 destination. The vehicle behind the RSU is reachable globally thanks to a globally-scoped prefix advertised by the

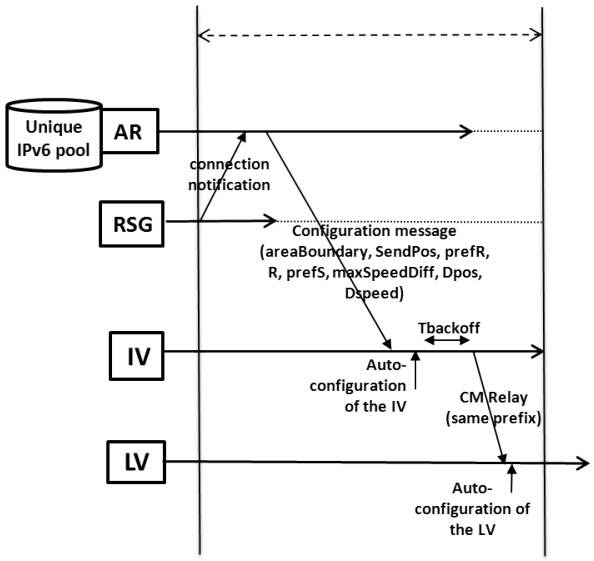


Figure 6.8: Handover procedure and timing diagram for TREBOL protocol.

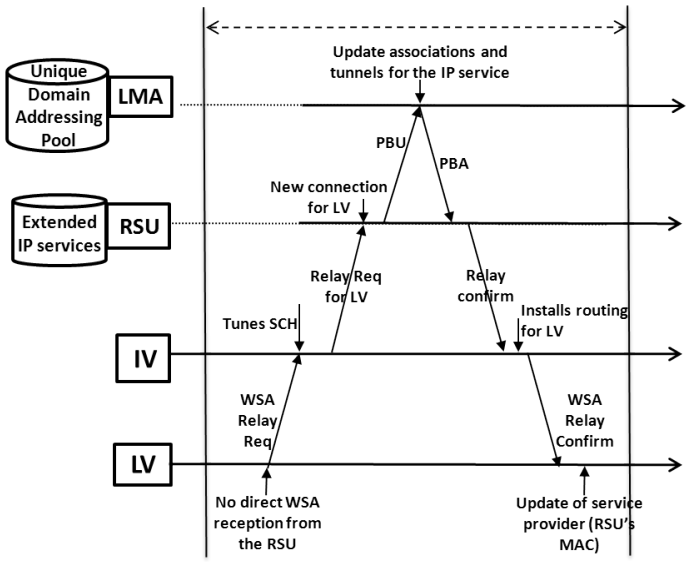


Figure 6.9: Handover procedure and timing diagram for VIP-WAVE protocol.

RSU. GeoNet may be coupled to MIPv6-NEMO for in-vehicle network reachability regardless of the advertised prefix [18].

While IP-based vehicle-to-infrastructure communications are made possible with MIPv6-NEMO, V2V IP-based communications are highly sub-optimal. If Mobile Network Prefixes (MNPs) are used, a packet sent from an in-vehicle network to another has to reach respective HAs in what is usually referred to as Pinball Routing problem [136]. Relevant to our study, we mention the GeoSAC proposal which is similar to TREBOL for its addressing configuration procedure [17].

6.1.4 Motivating novel approaches

The Internet Architecture Board considers IP semantics overload as the problem to be solved today in order to narrow the explosion of inter-routing tables in the core network [154]. The growing community of mobile and multi-homed Internet users is a worsening factor. To address the issue, recent proposals explore the naming and addressing problem [85]. In particular, evolutionary and revolutionary approaches advocate for the split of locator and identification functions of the IP namespace [183].

IP-based communications are key to leverage market penetration and deployment costs of the 802.11p architecture. With respect to this objective, the protocol stacks proposed by standardization bodies (IEEE, ETSI, ISO) include IPv6 support. In this context, correct addressing architecture is required to guarantee *uniqueness* of the destination and routablity of the address.

Figure *taxonomy* through its Future Internet branch illustrates recent efforts to combine FI initiatives and Vehicular networking. For instance, very recently authors of [214] and [6] proposed to extend Content-Centric Networking (FI revolutionary approach, [117]) for vehicular networks to address content dissemination related use cases. These approaches are out of scope for our *IP-based evolutionary* approaches study.

6.2 Future Vehicular Internet

In this chapter we discuss the other leaf of the taxonomy, evolutionary-based approaches for FVI through Vehicle Identification Numbers and try to pose the problem statement that drives our research.

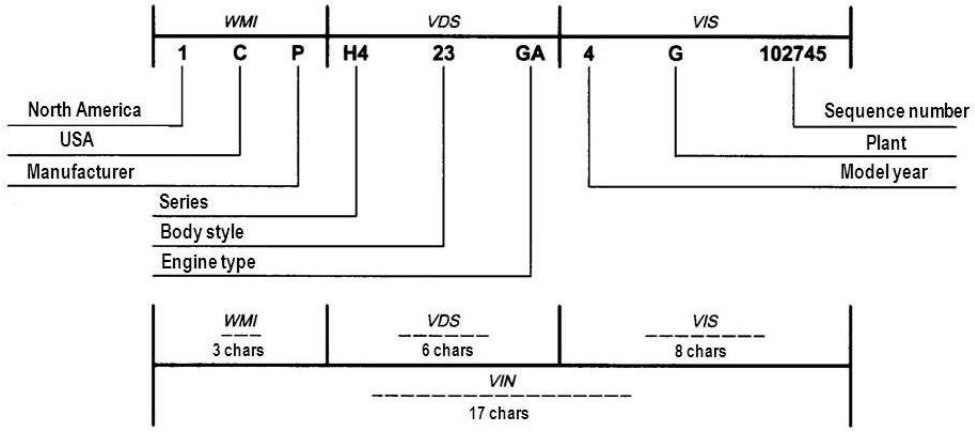


Figure 6.10: Vehicle Identification Number: structure and content

Figure 6.10 illustrates the Vehicle Identification Number. In Chapter 5, we presented the VIN namespace and focused on its use as is a vehicular-specific ID space for the following reasons:

- ISO-3779 and ISO-3780 standard
- Mandatory, unique, and present in every vehicle
- Hierarchical vehicular-specific endpoint identifier

Solving the vehicular networking challenges by simply adapting the usual indirection approaches may not be sustainable [127]. Indeed, some VIN databases for developers [213] claim including up to 2^{31} *distinct VIN codes of vehicles* in North America only since 1996 (regularly

updated). VIN is provisioned to uniquely identify up to 2^{78} vehicles worldwide *every 30 years* which is already several orders of magnitude bigger than IPv4's 2^{32} numbering space. Futuristic scenarios forecasting vehicles integration to the Internet may *not be scalable* without serious changes and adaptation.

VIN-based networking proposals are rare but do exist [131] [130]. We proposed to further the use of VIN and derive an addressing architecture compatible with a FI architecture that handles vehicular-Internet interactions in a sustainable manner.

6.2.1 Problem statement

Figures 6.11, 6.12, and 6.13 are the result of the previous analytical model (Chapters 4 and 5 for the signaling overload, the address configuration delay, and the e2e delay metrics for the protocols LISP-MN and centralized mobility management architectures (MIPv6-NEMO and PMIPv6-NEMO). The main observation is that LISP-MN based solution for handling Vehicle-to-Internet communications cost more in terms of signaling overhead when compared to centralized mobility schemes and induces more delay for configuration and control plane packet forwarding. Introducing group communications for these approaches as an accumulation of control messages will increase the signaling overhead and worsen the overall performance of the solutions, shortening the effective data plane communications opportunities, adding complexity to group managements and threatening the overall scalability of the system.

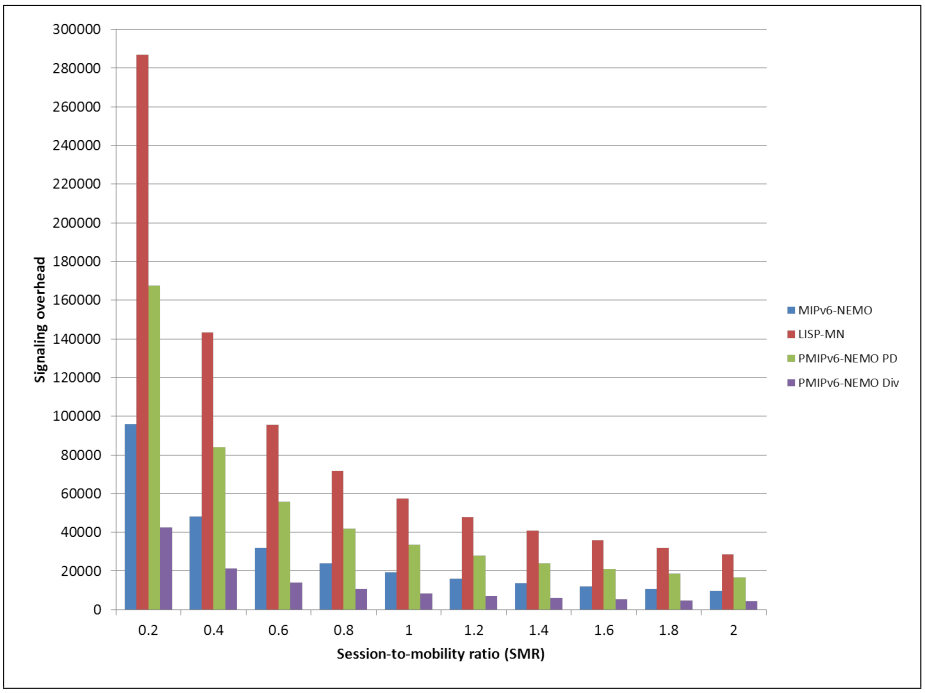


Figure 6.11: Comparing LISP-MN cost vs. Centralized mobility approaches (MIPv6 and PMIPv6) NEMO extensions as function of the SMR.

In order to tackle this issue, one could make the observation in the previous message exchange diagrams of our taxonomy, that the best signaling optimization possible is to relocate network components closer to the edge network, in order to limit the interactions with central architectural elements. Remains the problem of *topological addressing correctness*, that requires *anchoring* in the core network.

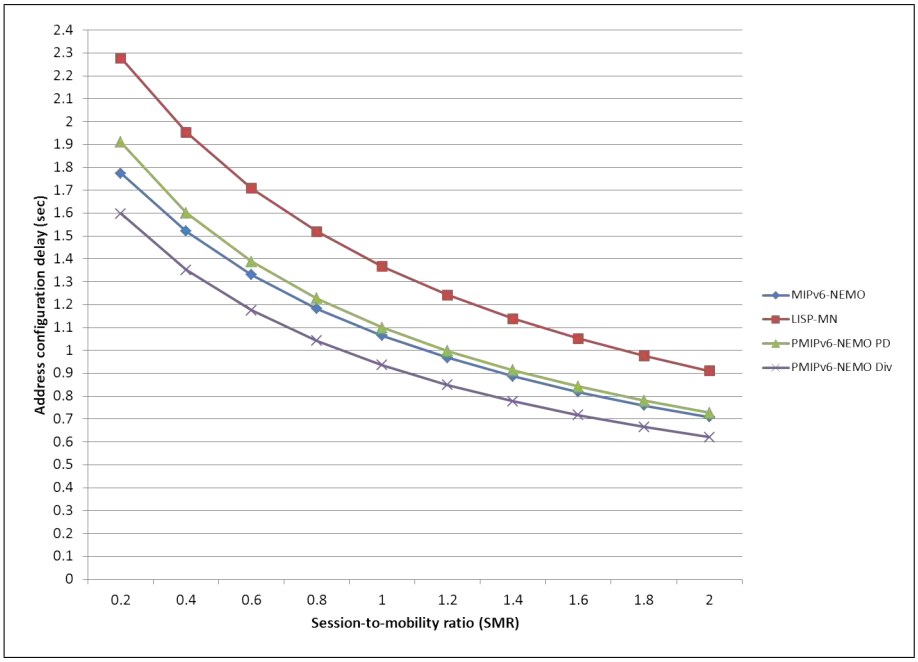


Figure 6.12: Comparing LISP-MN address configuration delay vs. Centralized mobility approaches (MIPv6 and PMIPv6) NEMO extensions as function of the SMR.

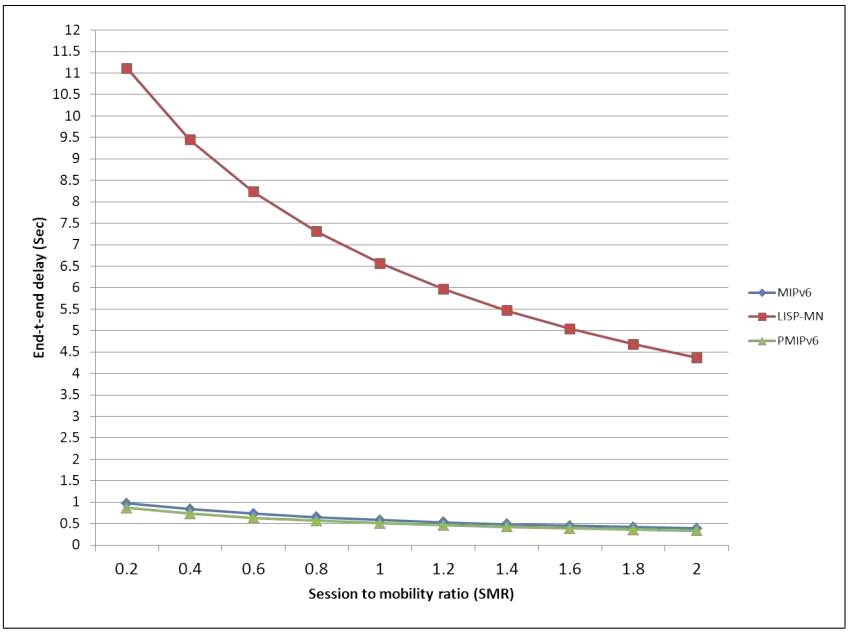


Figure 6.13: Comparing LISP-MN end-to-end delay vs. Centralized mobility approaches (MIPv6 and PMIPv6) as function of the SMR.

6.3 VIN6: VIN-based IPv6 Internet of Vehicles

This section introduces VIN-based Unique Local IPv6 Addressing (VULA) and VIN-based Network Address Translation (VNT). In our approach, we define VULA as a globally-scoped addressing anchored at the IV and limited for V2V group communications only. We then defined

the VNT as a solution to the RLOC auto-configuration problem: the vehicles inside the group (LVs) are only configured with VULA addressing, and only the IV is subject to handover procedure signaling. As for the LISP Mapping System update messages we also propose that the IV groups all the active LVs in one update message towards the mapping server.

6.3.1 VULA: VIN-based Unique Local IPv6 Addressing

The IPv6 addresses are valid in a certain scope: local, site or global. RFC 4193 "Unique Local IPv6 Unicast Addresses (ULA)" [103] defines the site-scoped IPv6 addresses (previous site-local format deprecated in RFC 3879). These prefixes must be generated with a pseudo-random algorithm, and result is considered as global and used accordingly (multi-hop) inside the same site (limited by a border router). Algorithm 3 illustrates one possible instance of ULA generation algorithm.

ULA prefixes generation method is infrastructure-less: local to the vehicle. While the pseudo-random algorithm may assure privacy, the main drawback is the possible collision at a large scale [103].

Algorithm 3 IPv6 Unique Local Addresses generation

1) Get the current NTP format time on 64bits.
2) Get the EUI-64 of the system. If not available, convert the MAC (48bits) into EUI-64 using RFC 4291. If not available, use a unique system identifier (e.g. VIN).
3) Concatenate values 1 and 2 into a 128bits key.
4) Compute the SHA-1 of this key into a 160bits result.
5) Use the least significant 40bits as a Global ID.
6) Concatenate: FC00::/7, L, and the 40bits Global ID to create a /48 ULA prefix.

Algorithm 4 VIN to IPv6 conversion algorithm

A, B, E, and F are extracted from the VIN code
X is a Binary vector, Y is the bitmap to fill
$X_1 \leftarrow f$(A,VIN), $X_2 \leftarrow f$(D,VIN), $X_3 \leftarrow f$(E,VIN), $X_4 \leftarrow f$(F,10). {f arguments are the selected fields and the numeral base to use (radix) when reading}
for $i = 1$ to 4 **do**
  $Y_i \leftarrow g(X_i, type)$ {g arguments are the binary value to map and the bitmap type. The bitmap type defines the bits placement (prefix, endpoint ID).}
end for

VIN semantics and algorithm 4 allows us to create scalable and hierarchical Future Internet IPv6 Provider Independent addressing space that identifies up to 2^{51} distinct vehicles [110]. Figure 6.14 illustrates VULA addressing architecture for globally and locally scoped IPv6 addresses.

In the context of Group IP-based vehicular communications, each vehicle (uniquely defined by its VIN) has to generate a unique and collision-free addressing pool for its internal network. The IV and REV have also to create an addressing pool to distribute to neighboring vehicles upon request. VIN numbers' *uniqueness property* needs to be *conserved* when Algorithm 4 is applied. We presented in Chapter 5 the formal uniqueness proof and highlighted the reversibility of used functions (bijectiveness).

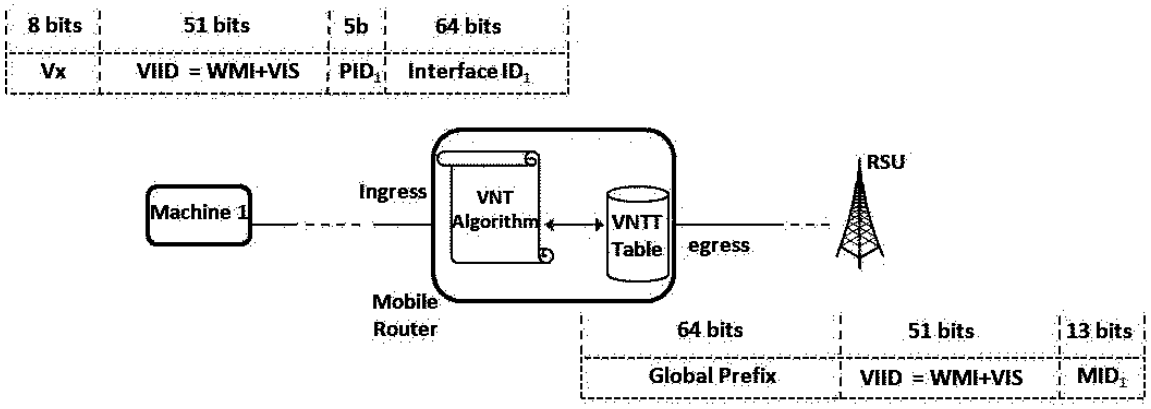


Figure 6.14: VIN-based IPv6 addressing architecture. The compression gain achieved with our algorithm helps defining additional parts that enables more end-to-end services. Top bitmap illustrates VULA address. Bottom bitmap represents topologically correct address format. In the center, Mobile Router generates VULA prefix using VIN and applies VNT algorithm for translation.

Table 6.1: Parameters of VIN-based addressing architecture

Parameter	Definition	Values
Vx	Addressing scope	V_1 for global and V_2 for VULA
PID	Prefix ID used for internal devices (fixed or mobile) and neighboring vehicles	P_k^f for internal fixed devices, P_k^m for internal mobile devices, and P_k^e P e for external prefixes
MID	Machine ID assigned sequentially, randomly, or permanently	M_k^f for internal fixed devices, M_k^t for temporary connections

6.3.2 VNT: VIN-based Network Address Translation

VULA uses VIN namespace to create a collision-free addressing architecture. In Figure 6.14, the MR uses the (WMI, VIS, MID) tuple to achieve stateless address auto-configuration (SLAAC) using the prefix announced by the RSU. For group communications, the VULA prefix using the (V_x, WMI, VIS, PID) tuple allows the IV to announce it internally for embedded devices and to neighboring vehicles *with no collision conflict thanks to the uniqueness property.* Embedded devices and neighboring vehicles' MRs are able to perform (SLAAC) using IV's VIN (group leader).

Table 6.1 summarizes the parameters included in Figure 6.14. VULA prefix for group communications assumes that the scope is set to V_2 (e.g.; 0xFD for ULA). Since PID is 5 bits, we set $P_k^f \in [0, 7]$, Pk $P_k^m \in [8, 15]$, and $P_k^e \in [16, 31]$. MID parameter is assigned in a reactive fashion, as explained below.

VIN-based addressing assures the uniqueness of the VULA prefix and the routability in a limited domain, which is the group composed of the IV, REVs (optional) and the LVs. When

a device from the group, embedded in the IV or a neighboring LV, attempts to communicate globally with a CN in the Internet the scope of VULA is not sufficient as it is local to the group. A transition mechanism is thus needed.

Figure 6.14 illustrates such a mechanism. VIN-based Network Address Translation is a transition mechanism that converts VULA addresses to global unique addresses (GUA) using a correspondence table (VNTT). The GUA is based on the RLOC prefix that the IV receives from Router Advertisements performed by the RSUs/Access routers. VNTT maintains tuples of the form (PID, Interface ID, MID) for each communication as illustrated in the algorithms of Figure 6.15 for outgoing packets and 6.16 for incoming packets.

The IV as the cluster head announces to the group a VULA IPv6 prefix based on its VIN. The LVs in the group receives this announcement and determine that it is coming from an IV (IV flag set in the message). The LV decides if it wants to join the group or not based on an internal leader selection algorithm[1].

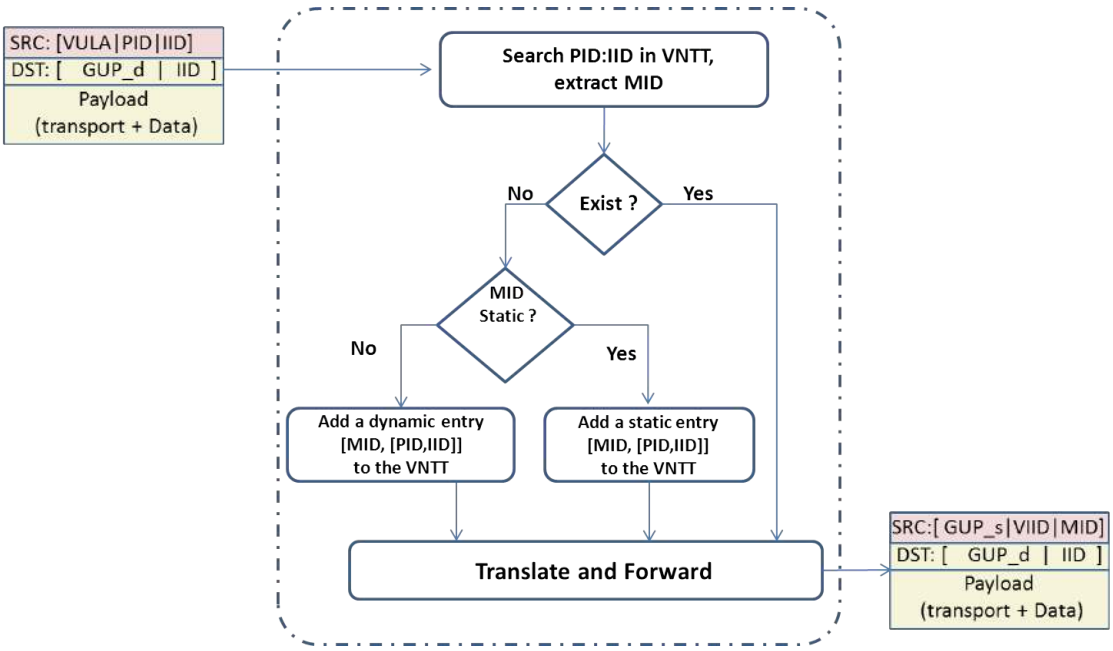


Figure 6.15: VULA to GUA translation algorithm. A packet with VULA source address is translated to GUA before forwarding. MID is assigned to the tuple (P, IID) and the correspondence stored. The selected MID is either static or dynamic.

If yes, the LV will auto-configure a VULA scoped address using the IV's VIN for the prefix and its VIN for lowest part (IID+MID). If the LV is not actively sending packets and just configures the address and default route, the IV is not aware of it. If the LV sends packets inside the group (to the IV for example), the IV creates an entry for this LV in its VNTT by extracting the IID+MID of the source address in the message. All packets travel through the IV as the gateway of the cluster, because the VULA addressing is topologically derived from its VIN and anchored at the IV. This forms a tree-shaped network with the IV at the root, LV at the leaves, and optionally REVs in the middle. It the packet has global destination, the VNT algorithm is used. The IV translates this VULA address (with PID from the *external* category)

[1]Several algorithms may be applied at this level: selecting the IV with highest/lowest VIN number, the VIN that belongs to the same manufacturer, first received announcement and maybe more. The description of such algorithm or how the cluster is formed at layer-2 is not in the scope our proposal.

to a global address by affecting one of its *temporary* MIDs. The translation algorithm is the same, if the packet comes from an *internal* PID (fixed or mobile) with permanent static MID. After the conversion, the IV's VNTT stores the correspondence between those identifiers before forwarding the packet to the destination. On the other hand, in case of an incoming packet, the IV analyzes the MID part to determine the destination VULA address. If the MID does not exist in its VNTT, the packet is dropped. If the correspondence exist, the (PID, IID) tuple are retrieved from the VNTT, the destination address translated to the corresponding VULA address and the packet forwarded on the proper interface.

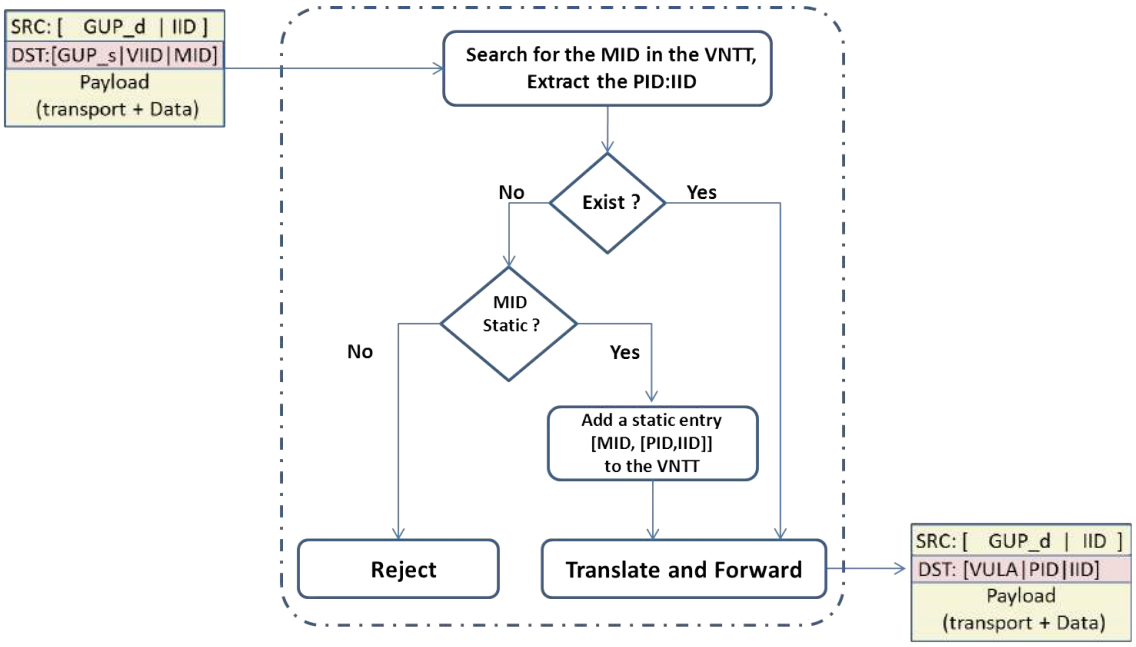


Figure 6.16: GUA to VULA translation algorithm. A packet with GUA destination address is translated to VULA before forwarding based on its MID section. The corresponding tuple (P, IID) are retrieved from the translation table. If MID does not exist in the table, the packet is dropped.

6.3.3 Extending LISP-MN to support group communications

The last part of our LISP-MN based proposal is to handle the mapping update operations. As stated earlier, an up-to-date accurate EID-to-RLOC binding is of utmost importance in LISP and determines whether a packet is correctly delivered to the destination or not. We also showed by comparing LISP-MN to other mobility architectures and protocols that this operation is expensive in terms of signaling load. In our LISP-MN based group communications, we propose to group the VIN6 EIDs used by the active LVs along with IV's VIN6 EID6 in one grouped Mapping Update message to the Mapping Server in the federated Mapping System. Figure 6.17 illustrates our proposal.

The IV and LVs encounter can happen at any time of the IV's journey, and not necessarily when connected to an RSU. After the IV configures an RLOC, it has to refresh its EID-to-RLOC binding at the Mapping System to allow corresponding nodes to reach it. The IV also keeps a list of active LVs' VIN6 EIDs at the VNTT after the LVs sends packets inside the group or globally. The IV groups those VIN6 EIDs in its Mapping Update message along with the corresponding RLOC using the appropriate MID it allocated for the LVs. These mappings are

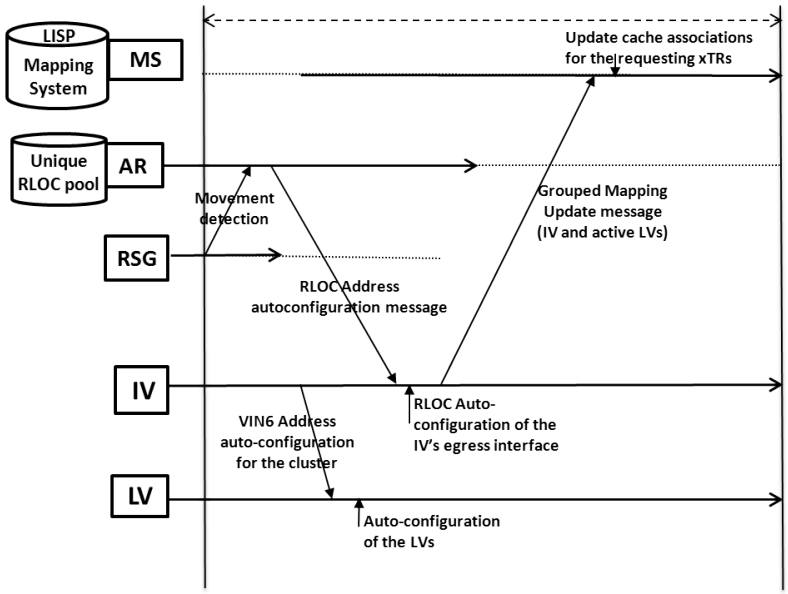


Figure 6.17: Handover procedure and timing diagram for LISP-MN based group communications protocol.

then processed by the Mapping Server and each binding updated separately. The LVs related entries are marked as nested behind IV's VIN6 EID to keep track of the global location of each vehicle separately. When an xTR needs to retrieve a mapping for an IV's VIN6 EID, no changes happen when compared to regular LISP-MN nodes. When an LV's mapping is retrieved, the Mapping System returns the IV's RLOC with an MID code in the lowest part of the address that only the IV can know about which LV it belongs to. The algorithm in Figure 6.16 is then applied when the related packet is processed.

6.4 Features summary and discussion

This section gives a detailed qualitative and analytic overview of our taxonomy.

6.4.1 Involved entities

In addition to the Road Side Units that connect the vehicles to the Infrastructure, depending on the technique, additional functional entities may be involved. For instance, Prefix Delegation techniques both involve DHCPv6 servers and MIPv6 Home Agents. VIP-WAVE involves the Local Mobility Anchor (LMA) and Mobile Access Gateways (MAGs) of the PMIPv6 protocol [31], in particular for extended services (LMA and MAGs in PMIPv6 replace the HA in MIPv6). While GeoSAC does not involve supplementary network entities, other GeoNetworking approaches might do. TREBOL and VIN6 do not involve more entities than RSUs group communications. If the communications are global, VIN6 needs to update the Mapping System. The comparison is summarized in Table 6.2.

Table 6.2: Involved entities comparison

Feature	DHCPv6-PD	ND-PD	TREBOL	VIP-WAVE	GeoSAC	VIN6
Additional Entities	DHCPv6 Server, Relay(s) and MIPv6 HA	DHCPv6 Server and MIPv6 Home Agent	No	PMIPv6's LMA and MAG	Not in GeoSAC but MIPv6 HA in other works [18]	Not for cluster, Mapping System for global

6.4.2 Messages overhead

Quick configuration techniques require short messages exchange. In Prefix Delegation approaches, control plane contain MIPv6 and DHCPv6-PD messages. The IV has to register its CoA at its HA before requesting an addressing pool from its home DHCPv6 server. Same procedure occurs in ND-PD. Other protocols do not need this prior IV configuration, as the IV mainly acts as a relay and not a server, so less messages. To configure an LV, the IV needs to be prepared. That means that the total number of messages is cumulated.

To generalize the principle, let's assume the group of vehicles is organized in a balanced binary tree having L depth (nesting level). Then, the total number of LVs (leaf nodes) is 2^L, the number of REVs (intermediate nodes) is $\sum_{k=1}^{L-1} 2^k$, and there is 1 IV (root). The table summarizes the number of overhead messages that we obtain in each protocol. Note that, compared to the size of the group, Prefix Delegation approaches cost the most in terms of messages, while other approaches grow linearly (1 additional message for 1 additional vehicle). Results illustrated in Table 6.3.

6.4.3 Address configuration delay

Address configuration delay for the IV depends on the initial initialization phase. This step is important for Prefix Delegation approaches while it is shorter for other approaches. We define T_{RA} [17] as the duration between the moment the IV enters in the RSU coverage and the moment the RSU sends an unsolicited RA randomly chosen between $T_{RA_{min}}$ and $T_{RA_{max}}$.

We suppose that the delay for a MIPv6 BU message is $T_{BU} = T_{BA}$, and the delay for PMIPv6 PBU message is $T_{PBU} = T_{PBA}$. We also suppose that all the DHCPv6 messages induce a delay of T_{DHCPv6}, and all ND-PD messages induce a delay of T_{ND-PD}. We do not count the Mapping Updates messages in VIN6 approach as they are not mandatory for the termination of the address configuration phase. Results are shown in Table 6.4.

6.4.4 Additional mobility extensions

In our taxonomy we showed that certain configuration techniques call for MIPv6-NEMO usage. In particular, Prefix Delegation makes use of MIPv6 to avoid routes update overhead at each delegation. VIP-WAVE uses PMIPv6 for extended services and some GeoNetworking approaches [18] make use of MIPv6-NEMO to configure in-vehicle network. TREBOL and VIN6 might be combined with MIPv6, PMIPv6 or LISP-MN (as we proposed for VIN6). However, TREBOL and VIN6 do not require it for group auto-configuration and communication (Table 6.5).

Table 6.3: Messages overhead comparison

Feature	DHCPv6-PD	ND-PD	TREBOL	VIP-WAVE	GeoSAC	VIN6
Messages to configure IV	2 BU/BA + 4 DHCPv6	2 BU/BA + 4 DHCPv6	1 CM	1 WSA + 2 PBU/PBA	1 RA	1 RA
Messages to configure LV	4 DHCPv6 if IV is Server, 8 DHCPv6 if IV is Relay	2 ND-PD messages (IV always Server)	1 CM from the IV or the RSU	1 WSA from relay (IV) if non-extended service, 1 WSA + 2 PBU/PBA if extended	1 RA from the IV or RSU	1 RA from IV
Messages to configure L nested vehicles	$4 \times \sum_{k=1}^{L} 2^k$ if IV is Server, $4 \times \sum_{k=0}^{L} 2^k$ if IV is Relay	2×2^L, no relay is possible	$\sum_{k=1}^{L} 2^k$	$\sum_{k=1}^{L} 2^k$	$\sum_{k=1}^{L} 2^k$	$\sum_{k=1}^{L} 2^k$

Table 6.4: Address configuration delay comparison

Feature	DHCPv6-PD	ND-PD	TREBOL	VIP-WAVE	GeoSAC	VIN6
Address conf. Delay for IV	$T_{RA} + 2 \times T_{BU} + 4 \times T_{DHCPv6}$	$T_{RA} + 2 \times T_{BU} + 2 \times T_{DHCPv6}$	T_{RA}	$T_{WSA} + 2 \times T_{PBU}$	T_{RA}	T_{RA}
Address conf. Delay for LV	$4 \times T_{DHCPv6}$ if IV is Server, $8 \times T_{DHCPv6}$ if IV is Relay	$2 \times T_{ND-PD}$	$T_{backoff} + T_{CM}$	$T_{WSA} + 2 \times T_{PBU}$	T_{relay}	T_{RA}

6.4.5 Addressing scope

The prefixes configured in each technique are globally- scoped as the infrastructure is delivering them. VIN6 has the advantage to define both global and local scopes (VULA) as illustrated in Table 6.6.

Table 6.5: Additional mobility extensions comparison

Feature	DHCPv6-PD	ND-PD	TREBOL	VIP-WAVE	GeoSAC	VIN6
Need for Mobility Extension	YES	YES	NO	YES (PMIPv6 for extended services)	Not for GeoSAC but other GeoNet approaches do [18]	Not for group, Yes for global reachability

Table 6.6: Addressing Scope comparison

Feature	DHCPv6-PD	ND-PD	TREBOL	VIP-WAVE	GeoSAC	VIN6
Addressing scope	Global	Global	Global	Global	Global	Global and Local

6.4.6 Addressing topology

Addressing topology depends on the auto-configuration method and the prefix delivered. In TREBOL, VIP-WAVE, and GeoSAC the addressing is flat as the same prefix is relayed to the neighbors. In Prefix Delegation techniques, the addressing is hierarchical as the addressing pool depends on an Authoritative Server. VIN6 has a hierarchical 2-level addressing: VULA for the group and Global for the IV to RSU link. Noteworthy, GeoSAC may route upon geographical coordinates making it a 2-level routing approach. GeoSAC and VIN6 mix two namespaces: Geographic coordinates and IPv6 for GeoSAC; VIN and IPv6 for VIN6. Comparison summarized in Table 6.7.

Table 6.7: Addressing topologies comparison

Feature	DHCPv6-PD	ND-PD	TREBOL	VIP-WAVE	GeoSAC	VIN6
Address topology	Hierarchical	Hierarchical	Flat	Flat	Flat but routing on 2-levels	Hierarchical (2-level)

6.4.7 Infrastructure dependency

TREBOL, VIP-WAVE, and GeoSAC do not function in the absence of supporting fixed infrastructure. On the other hand, Prefix Delegation approaches continue to work independently after initialization and configuration, but with no global reachability. VIN6 is designed to enable group communication in the presence or the absence of infrastructure alike. Indeed, the group initialization and configuration is based on the VIN namespace which is topologically correct independently of the infrastructure. Moreover, the group configuration remains stable and is not impacted by the successive IV handovers (Table 6.8).

Table 6.8: Infrastructure dependency comparison

Feature	DHCPv6-PD	ND-PD	TREBOL	VIP-WAVE	GeoSAC	VIN6
Infra. dependency	Initialization	Initialization	YES	YES	YES	NO

6.5 Conclusion and future work

Dynamic IPv6 addressing and routing configuration in vehicular networks is an important challenge that has attracted a fair amount of attention recently. The main enabler is the advent of several heterogeneous wireless transmission technologies for vehicular networks.

In order to analyze the proposals in this discipline, we first classified the main trends into a comprehensive taxonomy. We distinguished the Prefix delegation, ND extensions, GeoRouting and Future Internet approaches and detailed several examples of each branch. The evaluation summarized the features of each approach and characterized analytically the control overhead and the configuration delay. In particular, this chapter showed the inefficiency of legacy prefix delegation approaches in dynamic scenarios due to its control overhead and induced delay. This chapter also emphasizes some use cases where mobility extensions are more of a burden than an enabler.

Solving the vehicular networking challenges by simply adapting the usual indirection approaches may not be sustainable. In this chapter we showed that the configuration delay and signaling overhead may be expensive if we apply approaches intended to single MRs to group of vehicles. We then proposed to consider the use of Future Internet paradigm. Using VIN namespace, we presented a set of conversion and translation algorithms that create autonomous groups of vehicles with no required infrastructure interactions. We are then able to create with no further information but the IV's VIN, a domain that is guaranteed uniquely addressed. The evaluation showed interesting features of VIN6 that are worthy of attention when compared to other approaches. For instance, VIN6 uses limited control overhead thanks to its 2-level addressing approach anchored at the IV.

We intend to pursue this proposal by further thorough analytical study and simulation, to prove that the use of VIN6 in a cluster of vehicles can significantly lower the signaling overhead and shorten the configuration delay when compared to other approaches. Further, we can imagine implementing the VNT extension into the LISPMob software, an open source implementation of LISP-MN protocol.

Chapter 7

Conclusions and Future work

7.1 The road so far

The Internet experienced massive growth since its inception, especially by interconnecting research networks (ARPANET) to commercial network owners (ISPs) in 1988 by the NSFNET project. One of the keys to its success is the simplicity of its network architecture, often referred to as "dumb network, smart ends": complex functionalities resides on the computers connecting to the network; the latter focuses on routing data between those computers. This principle allowed the development of complex applications with no modification to the underlying network. Other technical and non-technical principles have driven the current Internet architecture expansion.

However, as stated by the Internet Architecture Board (IAB), there is a particular concern about the impacts of scalability on Internet routing. Indeed, the use of more specific IP routing-prefixes (usually, Provider Independent addressing) to support multihoming, Mobility, Traffic Engineering and other unforeseen applications at the early Internet stages, increases significantly both entropy and sizes of BGP inter-routing tables. These scalability concerns are worsen by the introduction of novel use cases including Machine-to-Machine communications, Internet of things, Vehicle-to-Internet communications and an ever growing number of mobile users.

To solve this issue, proposals are based on a common concept: the separation of locator and identifier in the numbering of Internet devices, often referred to as the "Loc/ID split". Basically, Loc/ID split about solving the current Internet routing and addressing architecture problem of IP semantics overload. A single numbering space, the IP address is used to define both roles of locating and identifying the hosts. Splitting these functions apart by using different numbering spaces for EIDs and RLOCs yields several advantages, including improved scalability of the routing system through greater aggregation of RLOCs. Our detailed review of the main Future Internet trends and proposals showed that:

- From the host perspective, the proposals tend to upgrade the protocol stack by including an additional identity layer. We seen how HIP and Shim6 considered that this layer should be secured, while LIN6 and others considered this sublayer as a mean to achieve stability at the TCP layer.
- Network-based approaches focus on the design of efficient addressing architectures from which the derived routing architecture would be scalable. LISP achieves this through an additional RLOc-to-EID translation-level, and GSE through the hierarchical addressing which reflects a path from the root (tier-1 providers) to the final domain.

- Revolutionary approaches are diverse in the approach and the desired objective. While CCN redefines the moto of the Internet from "where" to "what", ROFL tackles the hierarchical addressing namespaces to prove that scalability and isolation property can be achieved through more than just addressing architecture.

Vehicular networking serves as one of the most important enabling technologies to support a large set of applications related to vehicles, vehicle traffic, drivers, passengers and pedestrians. Intelligent Transportation Systems (ITS) that aim to manage vehicle traffic, assist drivers with safety and provide entertainment for passengers, are no longer limited to trials and experiments. Thanks to the active investments of car manufacturers and Public Transport Authorities, the essential enabling technologies components (radios, Access Points, spectrum, standards) are coming into place to finalize the deployment of VANETs (Vehicular Adhoc Network) and pave the way to unlimited market opportunities for vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-Internet applications.

Vehicle-to-Internet communications with regards to standardization run on an IPv6 end-to-end model. Recent efforts within IETF pushed the IP version upgrade from IPv4 (depleted addressing pools) to version 6, that is provisioned to uniquely address all mobile consumer electronics devices and all vehicles. With the native support of mobility, privacy, security and optimized auto-configuration techniques, IPv6 brings some upgrades when compared to IPv4. In the Future Internet context, the evolutions that IPv6 need to undergo for a better vehicular IP-based services support must follow the current Future Internet approaches: Identifier/Locator split must be included in Future Vehicular Internet architecture design.

The first contribution of this work was the study of IP-based services for Vehicle-to-Internet communications. In this context we were interested in eHealth and FEV services. We described the technical challenges of these two applications and presented our integrated eHealth platform and described the involved protocols. We also presented our mobility-supporting architecture in the context of FEV-related service. We reviewed the characteristics of both use cases and determined their common technical requirements for in-vehicle IP-based services. We also determined the importance of mobility-supporting IP-based protocols and mobility management architectures.

The next contribution was indeed the study of the mobility architectures. Mobility management has always been a key issue for network operators and of great value for users and application developers. We first proposed to study the addressing architectures in order to understand the importance of topology correctness. We explained the difference between infrastructure-based and infrastructure-less addressing architectures and their possible uses in vehicle-to-Internet communications. We then proposed to classify these mobility architectures into centralized and distributed approaches. Initially, the Mobile IP centralized architecture was the de facto solution for IP-based mobility. We explained how the accurate binding ID and Location determines the network functionalities and their deployment in a mobility architecture. The recent DMM paradigm pushed by network operators, aims at flattening those centralized mobility architectures and to relocate the anchors closer to the user and the edge network to avoid traversing and overloading the core. We also reviewed the solutions proposed in the field of network mobility and proposed two possible extensions to existing DMM paradigm, through HNP prefix division and DHCPv6 prefix delegation. In order to understand the performance of these proposals, we conducted an analytical evaluation using a parameterized analytical model. Obtained results showed that our proposed partially distributed mobility approaches can lower the signaling load and the address configuration delay for the users. In terms of data plane, the end-to-end delay can also be decreased in DMM. Finally, we also showed that the DMM scheme through its dynamic anchoring feature can save resources in the network by using tunnels and

re-routing only if required, for example, if the LFNs in the vehicle are running long lasting applications.

The next contribution is our first attempt at defining the Future Vehicular Internet through evolutionary network-based approaches. While vehicular networking has been studied through the CCN paradigm, at the best of our knowledge, we are the first to formulate the issue in these terms. Solving the vehicular networking challenges by simply adapting the legacy indirection infrastructure may not be sustainable. Indeed, some VIN databases for developers [213] claim including up to 2^{31} *distinct VIN codes of vehicles* in North America *only* since 1996 (regularly updated). VIN is provisioned to uniquely identify up to 2^{78} vehicles worldwide *every 30 years* which is already several orders of magnitude bigger than IPv4's 2^{32} numbering space. Futuristic scenarios forecasting vehicles integration to the Internet may *not be scalable* with this networking model.

We then proposed to dig further in the VIN semantics and introduced it as an alternative namespace to design Provider Independent addressing. We proposed then to build a scalable and hierarchical Future Internet (FI) IPv6 PI addressing space that identifies up to 2^{51} distinct vehicles. We also presented an original approach to create vehicular-specific endpoint identifiers and integrate vehicular communications in an evolutionary and sustainable manner in FI. Our addressing architecture is compatible with a subset of evolutionary network-based approaches (such as LISP and GSE). Our large vehicle identification space (2^{35}) per manufacturer allows using pseudonyms in local and global communications.

From an addressing/naming perspective, one major difference in using VIN6 with MIPv6-NEMO is that the VIN6 addressing was also used to route the packets and reach the destination. Indeed, by advertising the VIN6 PIA in a BGP message into the global routing system, correspondent nodes' packets routing is based upon the presence of such routes in the DFZ. The benefit of using VIN6 here is that the addressing can be aggressively aggregated. When used with the LISP architecture, VIN6 can only be used as Endpoint Identifiers and not Routing Locators. The VIN6 addressing only serves the purpose of identifying the vehicle and its inside network.

From a routing perspective, in the LISP based solution that we propose, the CN's packets can avoid the manufacturer domain and be routed optimally through shortest RLOC-based path, unless the vehicle is topologically present inside the manufacturer's domain. The manufacturer domain through its hosted Mapping Server follows the locations of the vehicle but not the content of the packets sent from the vehicle. This is different in MIPv6 based solution where the data path and the control path are the same and traverse the Home Agent hosted in the manufacturer domain.

Our last contribution pushed further the use of VIN namespace and introduced group IP-based communications. Dynamic IPv6 addressing and routing configuration in vehicular networks is an important challenge that has attracted a fair amount of attention recently. The main enabler is the advent of several heterogeneous wireless transmission technologies for vehicular networks.

In order to analyze the proposals in this discipline, we first classified the main trends into a comprehensive taxonomy. We distinguished the Prefix delegation, ND extensions, GeoRouting and Future Internet approaches and detailed several examples of each branch. The evaluation summarized the features of each approach and characterized analytically the control overhead and the configuration delay. In particular, we showed the inefficiency of legacy prefix delegation approaches in dynamic scenarios due to its control overhead and induced delay. We also pointed out that in some cases mobility is more of a burden than an enabler. We then quantified this burden in our problem statement by comparing the actual overhead suffered from the use of LISP-MN as an alternative to MIPv6 and PMIPv6.

Solving the vehicular networking challenges by simply adapting the usual indirection approaches may not be sustainable. We then proposed to consider to apply some of the principles of Future Internet paradigm in our model. Using VIN namespace, we presented a set of conversion and translation algorithms that create autonomous groups of vehicles with no required infrastructure interactions. We are then able to create with no further information but the IV's VIN, a domain that is guaranteed uniquely addressed. The evaluation showed interesting features of VIN6 that are worthy of attention when compared to other approaches. For instance, VIN6 uses limited control overhead thanks to its 2-level addressing approach anchored at the IV.

7.2 What remains ahead

The findings in this thesis report have shown that applying Future Internet paradigm to vehicle-to-Internet communications is a promising field and a necessity to preserve the scalability of the Internet architecture. However, several open issues need to be addressed before actual deployment.

- As for the mobility management protocols, one possible perspective can be the use of simulation to approach real-life network conditions with higher load. This is to challenge the limits of those architectures and demonstrate the value of possible Routing Optimizations. In particular, is it possible to install intermediate anchors that dynamically support some of the IP flows of mobile nodes ? also, what could be a proper analytical model for the prefix lifetime in order to optimize the use of these dynamic anchors ?
- As for our VIN6-EID LISP-MN proposal, we observed the high overhead when compared to other centralized mobility approaches. We intend to pursue this proposal and improve it through extensive simulation study to lower the signaling overhead and shorten the configuration delay when compared to other approaches. We can also implement the VNT extension into the LISPMob software, an open source implementation of LISP-MN protocol.
- Apply more Future Internet approaches, evolutionary or revolutionary to determine which induces less control overhead in vehicular scenarios. The comparison to LISP may trigger some observation that can further change some parts of the protocol.

Bibliography

[1] *3GPP Long Term Evolution*. Online on 15 Mai 2012 at: http://ipv6.com/articles/wireless/3GPP-Long-Term-Evolution.htm.

[2] *4WARD, The FP7 4WARD project*. Online on 20/03/2012 at: http://www.4ward-project.eu/index.php?s=overview.

[3] B. Aboba et al. "RFC 4282 - The Network Access Identifier". In: *IETF* (2005).

[4] *AKARI, Architecture Design Project for New Generation Network*. Online on 20/03/2012 at: http://akari-project.nict.go.jp/eng/index2.htm.

[5] S. Akhshabi and C. Dovrolis. "The Evolution of Layered Protocol Stacks Leads to an Hourglass-Shaped Architecture". In: *SIGCOMM'11* (2011).

[6] Marica Amadeo, Claudia Campolo, and Antonella Molinaro. "Enhancing content-centric networking for vehicular environments". In: *Computer Networks* 57.16 (2013). Information Centric Networking, pp. 3222 –3234. ISSN: 1389-1286. DOI: http://dx.doi.org/10.1016/j.comnet.2013.07.005. URL: http://www.sciencedirect.com/science/article/pii/S1389128613002211.

[7] *AmbuCom, "Ambulance Communicante", FUI14 project*. Online on 19/10/2014 at: www.ambucom.fr.

[8] American Registry for Internet Numbers (ARIN). *The IANA IPv4 Address Free Pool is Now Depleted*. Online on 07/05/2012 at: https://www.arin.net/announcements/2011/20110203.html.

[9] J. Arkko and I. van Beijnum. "RFC5534 - Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming". In: *IETF* (2009).

[10] R. Atkinson, S. Bhatti, and S. Hailes. "Evolving the Internet Architecture Through Naming". In: *IEEE Journal on Selected Areas in Communications* 28.8 (2010), pp. 1319–1325. ISSN: 0733-8716. DOI: 10.1109/JSAC.2010.101009.

[11] RJ. Atkinson and SN. Bhatti. "RFC 6740 - Identifier-Locator Network Protocol (ILNP) Architectural Description". In: *IETF* (2012).

[12] T. Aura. "RFC3972 - Cryptographically Generated Addresses (CGA)". In: *IETF* (2005).

[13] E. Baccelli, T. Clausen, and R. Wakikawa. "IPv6 operation for WAVE; Wireless Access in Vehicular Environments". In: *IEEE Vehicular Networking Conference (VNC)*. 2010, pp. 160–165. DOI: 10.1109/VNC.2010.5698260.

[14] M. Bagnulo. "RFC5535 - Hash-Based Addresses (HBA)". In: *IETF* (2009).

[15] Baid, A. and Mukherjee, S. and Tam Vu and Mudigonda, S. and Nagaraja, K. and Fukuyama, J. and Raychaudhuri, D. "Enabling vehicular networking in the MobilityFirst future internet architecture". In: *IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. 2013, pp. 1–3. DOI: 10.1109/WoWMoM.2013.6583417.

[16] Baid, A. and Tam Vu and Raychaudhuri, D. "Comparing alternative approaches for networking of named objects in the future Internet". In: *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2012, pp. 298–303. DOI: 10.1109/INFCOMW.2012.6193509.

[17] Baldessari, R. and Bernardos, C.J. and Calderon, M. "GeoSAC - Scalable address autoconfiguration for VANET using geographic networking concepts". In: *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008.* 2008, pp. 1–7. DOI: 10.1109/PIMRC.2008.4699949.

[18] Ines Ben Jemaa et al. "Validation and evaluation of NEMO in VANET using geographic routing". English. In: *10th International Conference on Intelligent Transport System Telecommunications - ITST 2010*. Kyoto, Japan, Nov. 2010, 6 p. URL: http://hal.inria.fr/inria-00567786.

[19] Bernardos, CJ. and de la Oliva, A. and Giust, F. "An IPv6 Distributed Client Mobility Management approach using existing mechanisms (Internet Draft)". In: *IETF* (2014).

[20] Bernardos, CJ. and Zuniga, JC. "PMIPv6-based distributed anchoring (Internet Draft)". In: *IETF* (2014).

[21] Bertin, P. and Bonjour, S. and Bonnin, J. "Distributed or Centralized Mobility?" In: *IEEE Global Telecommunications Conference*. 2009, pp. 1–6. DOI: 10.1109/GLOCOM.2009.5426302.

[22] Pravin Bhagwat, Satish Tripathi, and Charles Perkins. "Network layer mobility: an architecture and survey". In: *IEEE Personal Communications* 3.3 (1996), pp. 54 –64. ISSN: 1070-9916. DOI: 10.1109/98.511765.

[23] M.S. Blumental and D.D. Clark. "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World". In: *ACM Transactions on Internet Technology*. ACM, 2001.

[24] Bolla, R. and Repetto, M. "A Comprehensive Tutorial for Mobility Management in Data Networks". In: *IEEE Communications Surveys Tutorials* 16.2 (2014), pp. 812–833. ISSN: 1553-877X. DOI: 10.1109/SURV.2013.071913.00140.

[25] D. Boswarthick, O. Elloumi, and O. Hersent. "M2M communications, a systems approach". In: ed. by D. Boswarthick, O. Elloumi, and O. Hersent. Wiley, 2012. Chap. 7, "IPv6 for M2M", pp. 448–450.

[26] S. Brim et al. "Mobility and Privacy (Internet Draft)". In: *IETF* (2011).

[27] M. Caesar et al. "ROFL: Routing On Flat Labels". In: *SIGCOMM'06*. ACM, 2006.

[28] Maria Calderon et al. "Vehicular Networks: Techniques, Standards and Applications". In: ed. by Hassnaa Moustafa and Yan Zhang. CRC, 2009. Chap. 9, "IP Address Autoconfiguration in Vehicular Networks", pp. 249–274.

[29] *Card Guard Products & Technologies*. Online on 15/05/2012 at: http://www.cardguard.com/cardguard.

[30] B. Carpenter. "RFC1958 - Architectural Principles of the Internet". In: *IETF* (1996).

[31] S. Cespedes, N. Lu, and X. Shen. "VIP-WAVE: On the Feasibility of IP Communications in 802.11p Vehicular Networks". In: *IEEE Transactions on Intelligent Transportation Systems* PP.99 (2012), pp. 1 –16. ISSN: 1524-9050. DOI: 10.1109/TITS.2012.2206387.

[32] Cespedes, S. and Xuemin Shen and Lazo, C. "IP mobility management for vehicular communication networks: challenges and solutions". In: *IEEE Communications Magazine* 49.5 (2011), pp. 187 –194. ISSN: 0163-6804. DOI: 10.1109/MCOM.2011.5762817.

[33] H. Chan. "Problem statement for distributed and dynamic mobility management (Internet draft)". In: *IETF* (2011).

[34] H. Chan et al. "RFC7333 - Requirement for Distributed Mobility Management". In: *IETF* (2014).

[35] D. R. Cheriton and M. Gritter. "TRIAD: A Scalable Deployable NAT-based Internet Architecture". In: *Stanford Computer Science Technical Report* (2000).

[36] Cisco. "IPv6 addressing white paper". In: *White paper* (2008).

[37] D.D. Clark. "RFC814 - Name, Addresses, Ports, and Routes". In: *IETF* (1982).

[38] D.D. Clark. "The Design Philosophy of the DARPA Internet Protocols". In: *ACM SIGCOMM*. ACM, 1988.

[39] D.D. Clark et al. "Addressing Reality: An Architectural Response to Real-World Demands on the Evolving Internet". In: *ACM SIGCOMM'03*. ACM, 2003.

[40] D.D. Clark et al. "Tussle in Cyberspace: defining Tomorrow's Internet". In: *ACM SIGCOMM'02*. ACM, 2002.

[41] D. Cocker. "Multiple Address Service for Transport (MAST)". In: *Applications and the Internet, IEEE/IPSJ International Symposium on* (2004).

[42] D. Cocker. "Multiple Address Service For Transport (MAST): An Extended Proposal (Internet Draft)". In: *IETF* (2003).

[43] Andrea Conti et al. "Vehicular Networks: Techniques, Standards and Applications". In: ed. by Hassnaa Moustafa and Yan Zhang. CRC, 2009. Chap. 4, "Heterogeneous Wireless Communications for Vehicular Networks", pp. 63–106.

[44] Coras, F. and Saucez, D. and Iannone, L. and Donnet, B. "On the performance of the LISP beta network". In: *Networking Conference, 2014 IFIP*. 2014, pp. 1–9. DOI: 10.1109/IFIPNetworking.2014.6857102.

[45] C. Cox. "An introduction to LTE, LTE, LTE-Advanced, SAE and 4G Mobile Communications". In: Wiley, 2011. Chap. 2, "System architecture evolution", pp. 21–46.

[46] M. Crawford et al. "Separating Identifiers and Locators in Addresses: An Analysis of the GSE Proposal for IPv6 (Internet Draft)". In: *IETF* (1999).

[47] *CVIS, Cooperative Vehicle Infrastructure Systems*. Online on 15/11/2014 at: http://www.cvisproject.org/.

[48] J. Day. "Patterns in Network Architecture, a return to fundamentals". In: ed. by Prentice Hall. Prentice Hall, 2008. Chap. 5, "Background on Naming and Addressing", pp. 141–183.

[49] J. Day. "Patterns in Network Architecture, a return to fundamentals". In: ed. by Prentice Hall. Prentice Hall, 2008. Chap. 8, "Making Addresses Topological", pp. 283–315.

[50] J. Day. "Patterns in Network Architecture, a return to fundamentals". In: ed. by Prentice Hall. Prentice Hall, 2008. Chap. 9, "Multihoming, Multicast, and Mobility", pp. 317–349.

[51] S. Deering. "Watching the Waist of the Protocol Hourglass". In: *IETF 51 plenary, London* (2001).

[52] Deguang Le and Xiaoming Fu and Dieter Hogrefe. "A review of mobility support paradigms for the internet". In: *IEEE Communications Surveys Tutorials* 8.1 (2006), pp. 38 –51. ISSN: 1553-877X. DOI: 10.1109/COMST.2006.323441.

[53] Do, T-X. and Kim, Y. "Network Mobility Support in the Distributed Mobility Management (Internet draft)". In: *IETF* (2014).

[54] Dominik Klein and Michael Höfling and Matthias Hartmann and Michael Menth. "Integration of LISP and LISP-MN into INET". In: *5th International Workshop on OMNeT++*. Desenzano, Italy, Mar. 2012, pp. 299–306.

[55] R. Droms et al. "RFC3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". In: *IETF* (2003).

[56] R. Droms et al. "RFC6276 - DHCPv6 Prefix Delegation for Network Mobility (NEMO)". In: *IETF* (2011).

[57] R. Droms et al. "RFC6276 - DHCPv6 Prefix Delegation for Network Mobility (NEMO)". In: *IETF* (2011).

[58] T. Duchrow et al. "Towards electric mobility data mining". In: *Electric Vehicle Conference (IEVC), 2012 IEEE International*. 2012, pp. 1–6. DOI: 10.1109/IEVC.2012.6183199.

[59] *e-DASH*. Online on 15/11/2014 at: http://edash.eu.

[60] Dr Ulrich Eberle and Dr Rittmar von Helmolt. "Sustainable transportation based on electric vehicle concepts: a brief overview". In: *Energy Environ. Sci.* 3 (6 2010), pp. 689–699. DOI: 10.1039/C001674H. URL: http://dx.doi.org/10.1039/C001674H.

[61] *eCo-FEV, Combining infrastructures fro efficient electric mobility*. Online on 15/11/2014 at: http://www.eco-fev.eu.

[62] *eCoMove, Cooperative Mobility Systems and Services for Energy Efficiency*. Online on 15/11/2014 at: http://www.ecomove-project.eu.

[63] W.M. Eddy. "At what layer does mobility belong?" In: *IEEE Communications Magazine* 42.10 (2004), pp. 155 –159. ISSN: 0163-6804. DOI: 10.1109/MCOM.2004.1341274.

[64] Elmokashfi, Ahmed and Dhamdhere, Amogh. "Revisiting BGP Churn Growth". In: *SIGCOMM Comput. Commun. Rev.* 44.1 (Dec. 2013), pp. 5–12. ISSN: 0146-4833. DOI: 10.1145/2567561.2567563. URL: http://doi.acm.org/10.1145/2567561.2567563.

[65] Jakob Eriksson, Hari Balakrishnan, and Samuel Madden. "Cabernet: vehicular content delivery using WiFi". In: *Proceedings of the 14th ACM international conference on Mobile computing and networking*. MobiCom '08. San Francisco, California, USA: ACM, 2008, pp. 199–210. ISBN: 978-1-60558-096-8. DOI: 10.1145/1409944.1409968. URL: http://doi.acm.org/10.1145/1409944.1409968.

[66] Ernest, P.P. and Chan, H.A. and Falowo, O.E. and Magagula, L.A. and Cespedes, S. "Network-based distributed mobility management for network mobility". In: *IEEE 11th Consumer Communications and Networking Conference (CCNC)*. 2014, pp. 417–425. DOI: 10.1109/CCNC.2014.6866604.

[67] *ETSI Intelligent Transport Systems (ITS)*. Online on 07/05/2012 at: http://etsi.org/WebSite/Technologies/IntelligentTransportSystems.aspx.

[68] ETSI Standard. *TS 102 636-6-1 - Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols*. Tech. rep. 2011.

[69] D. Evans. *The Internet of Things, The Next Evolution Of The Internet*. Online on 07/05/2012 at: http://www.slideshare.net/CiscoIBSG/internet-of-things-8470978.

[70] EXALTED consortium. *IP Networking System for M2M communications for EXALTED use cases*. Tech. rep. FP7 EXALTED (EXpAnding LTE for Devices), June 2012.

[71] D. Farinacci et al. "Locator/ID Separation Protocol (LISP) (Internet Draft)". In: *IETF* (2009).

[72] D. Farinacci et al. "RFC 6830 - Locator/ID Separation Protocol (LISP) (Internet Draft)". In: *IETF* (2013).

[73] Farinacci, D. and Lewis, D. and Meyer, D. and White, C. "LISP Mobile Node (Internet draft)". In: *IETF* (2015).

[74] Feixiong Zhang and Nagaraja, K. and Zhang, Y. and Raychaudhuri, D. "Content delivery in the MobilityFirst future Internet architecture". In: *Sarnoff Symposium (SARNOFF), 2012 35th IEEE*. 2012, pp. 1–5. DOI: 10.1109/SARNOF.2012.6222763.

[75] A. Feldmann. "Internet Clean-Slate Design: What and Why?" In: *ACM SIGCOMM Computer Communication Review* 37.3 (2007).

[76] A. Ford et al. "RFC6824 - TCP Extensions for Multipath Operation with Multiple Addresses". In: *IETF* (2013).

[77] Paul Francis and Ramakrishna Gummadi. "IPNL: A NAT-extended internet architecture". In: SIGCOMM '01. ACM, 2001, pp. 69–80.

[78] Fuller, V. and Farinacci, D. "RFC 6833 - Locator/ID Separation Protocol (LISP) Map-Server Interface". In: *IETF* (2013).

[79] *Future Internet Engineering, European Regional Development Funding Project*. Online on 30/05/2012 at: https://www.iip.net.pl/en/project.

[80] Matthias D. Galus et al. "Integrating Power Systems, Transport Systems and Vehicle Technology for Electric Mobility Impact Assessment and Efficient Control". In: *Smart Grid, IEEE Transactions on* 3.2 (2012), pp. 934–949. ISSN: 1949-3053. DOI: 10.1109/TSG.2012.2190628.

[81] A. Garcia-Martinez, M. Bagnulo, and I. Van Beijnum. "The Shim6 architecture for IPv6 multihoming". In: *IEEE Communications Magazine* 48.9 (2010), pp. 152–157. ISSN: 0163-6804. DOI: 10.1109/MCOM.2010.5560599.

[82] *GENI, exploring networks of the future*. Online on 19/03/2012 at: http://www.geni.net/.

[83] *Geographic addressing and routing for vehicular communications (GeoNet), FP7 ICT*. Online on 08/05/2012 at: http://www.geonet-project.eu/?page_id=9.

[84] Mario Gerla and Leonard Kleinrock. "Vehicular networks and the future of the mobile Internet". In: *Computer Networks* 55.2 (2011). <ce:title>Wireless for the Future Internet</ce:title>, pp. 457 –469. ISSN: 1389-1286. DOI: http://dx.doi.org/10.1016/j.comnet.2010.10.015. URL: http://www.sciencedirect.com/science/article/pii/S1389128610003324.

[85] Gerla, Mario and Kleinrock, Leonard. "Vehicular Networks and the Future of the Mobile Internet". In: *Comput. Netw.* 55.2 (Feb. 2011), pp. 457–469. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2010.10.015. URL: http://dx.doi.org/10.1016/j.comnet.2010.10.015.

[86] Giust, F. and Bernardos, C.J. and De La Oliva, A. "Analytic Evaluation and Experimental Validation of a Network-Based IPv6 Distributed Mobility Management Solution". In: *IEEE Transactions on Mobile Computing* 13.11 (2014), pp. 2484–2497. ISSN: 1536-1233. DOI: 10.1109/TMC.2014.2307304.

[87] Giust, F. and de la Oliva, A. and Bernardos, Carlos J. and Da Costa, R.P.F. "A network-based localized mobility solution for Distributed Mobility Management". In: *14th International Symposium on Wireless Personal Multimedia Communications (WPMC)*. 2011, pp. 1–5.

[88] Giust, F. and de la Oliva, A. and Bernardos, C.J. "Flat access and mobility architecture: An IPv6 distributed client mobility management solution". In: *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2011, pp. 361–366. DOI: 10.1109/INFCOMW.2011.5928839.

[89] Gohar, M. and Seok Joo Koh. "Network-Based Distributed Mobility Control in Localized Mobile LISP Networks". In: *IEEE Communications Letters* 16.1 (2012), pp. 104–107. ISSN: 1089-7798. DOI: 10.1109/LCOMM.2011.111011.111898.

[90] K. et al. Gosse. "Vehicular Networking, Automotive applications and beyond". In: ed. by Wiley. Wiley, 2009. Chap. 8, "Standardization of vehicle-to-Infrastructure Communication", pp. 171–201.

[91] Gramaglia, M. and Calderon, M. and Bernardos, Carlos J. "TREBOL: Tree-Based Routing and Address Autoconfiguration for Vehicle-to-Internet Communications". In: *IEEE 73rd Vehicular Technology Conference (VTC Spring)*. 2011, pp. 1–5. DOI: 10.1109/VETECS.2011.5956233.

[92] S. Gundavelli et al. "RFC 5213 - Proxy Mobile IPv6". In: *IETF* (2008).

[93] A. Gurtov, M. Komu, and R. Moskowitz. "Host Identity Protocol: Identifier/Locator Split for Host Mobility and Multihoming". In: *The Internet Protocol Journal* (March 2009).

[94] D. H. Gustafson and J. C. Wyatt. "Evaluation of ehealth systems and services". In: *British Medical Journal* 328 (7449 2004), pp. 1150–1150. DOI: 10.1136/bmj.328.7449.1150.

[95] Youn-Hee Han, JinHyeock Choi, and Seung-Hee Hwang. "Reactive Handover Optimization in IPv6-Based Mobile Networks". In: *IEEE Journal on Selected Areas in Communications* 24.9 (2006), pp. 1758–1772. ISSN: 0733-8716. DOI: 10.1109/JSAC.2006.875112.

[96] Hanka, O. "How to prevent identity fraud in locator/identifier-Split architectures". In: *International Conference on Computing, Networking and Communications (ICNC)*. 2012, pp. 683–689. DOI: 10.1109/ICCNC.2012.6167510.

[97] Hanka, O. "The cost of location privacy in locator/identifier-split architectures". In: *IEEE International Performance Computing and Communications Conference (IPCCC)*. 2011, pp. 1–6. DOI: 10.1109/PCCC.2011.6108112.

[98] Hartenstein, H. and Laberteaux, K.P. "A tutorial survey on vehicular ad hoc networks". In: *IEEE Communications Magazine* 46.6 (2008), pp. 164–171. ISSN: 0163-6804. DOI: 10.1109/MCOM.2008.4539481.

[99] Helmbrecht, M. and Olaverri-Monreal, C. and Bengler, K. and Vilimek, R. and Keinath, A. "How Electric Vehicles Affect Driving Behavioral Patterns". In: *IEEE Intelligent Transportation Systems Magazine* 6.3 (2014), pp. 22–32. ISSN: 1939-1390. DOI: 10.1109/MITS.2014.2315758.

[100] T. Henderson, P. Nikander, and M. Komu. "RFC 5338 - Using the Host Identity Protocol with Legacy Applications". In: *IETF* (2008).

[101] L. Heuser, Z. Nochta, and N-C. Trunk. "ICT Shaping The World: A Scientific View ". In: John Wiley & sons, 2008. Chap. 5, "Towards The Internet of Things".

[102] R. Hinden. "RFC1955 - New Scheme for Internet Routing and Addressing (ENCAPS) for IPNG". In: *IETF* (1996).

[103] R. Hinden and B. Haberman. "RFC4193 - Unique Local IPv6 Unicast Addresses". In: *IETF* (2005).

[104] Höfer, Christina and Petit, Jonathan and Schmidt, Robert and Kargl, Frank. "POPCORN: Privacy-preserving Charging for Emobility". In: *Proceedings of the 2013 ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*. CyCAR '13. Berlin, Germany: ACM, 2013, pp. 37–48. ISBN: 978-1-4503-2487-8. DOI: 10.1145/2517968.2517971. URL: http://doi.acm.org/10.1145/2517968.2517971.

[105] C. Huitema and B. Carpenter. "RFC3879 - Deprecating Site Local Addresses". In: *IETF* (2004).

[106] G. Huston. *Growth of the BGP Table - 1994 to Present (http://bgp.potaroo.net/)*. 2012.

[107] *IANA IPv4 Special-Purpose Address Registry*. Online on 15/05/2014 at: http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml..

[108] Iannone, L. and Saucez, D. and Bonaventure, O. "RFC 6834 - Locator/ID Separation Protocol (LISP) Map-Versioning". In: *IETF* (2013).

[109] "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services". In: *IEEE Std 1609.3-2010 (Revision of IEEE Std 1609.3-2007)* (2010), pp. 1–144. DOI: 10.1109/IEEESTD.2010.5680697.

[110] Imadali, S. and Petrescu, A. and Boc, M. and Veque, V. "VIN6: VIN-based IPv6 provider independent addressing for future vehicular internet communications". In: *IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC)*. 2013, pp. 2940–2945. DOI: 10.1109/PIMRC.2013.6666650.

[111] "Intelligent transport systems – Communications access for land mobiles (CALM) – IPv6 Networking". In: *ISO/TC 204 Intelligent transport systems* (2012).

[112] Internet Society. *World IPv6 Launch*. Online on 05/12/2012 at: http://www.worldipv6launch.org/.

[113] D.S. Isenberg. "The Rise of the Stupid Network: Why the Intelligent Network Was a Good Idea Once But Isn't Anymore". In: *Essay* (1997).

[114] *ISO/IEC 3779:2009 Road vehicles - Vehicle identification number (VIN) - Content and structure*. Tech. rep. International Organization for Standardization, 2009.

[115] *iTETRIS, An Integrated Wireless and Traffic Platform for Real-Time Road Traffic Management Solutions*. Online on 15/11/2014 at: http://www.ict-itetris.eu/.

[116] ITS. *eSafety : eCall | emergency call for car accident | Europa-Information Society*. Online on 15 February 2013 at: http://ec.europa.eu/information _society/activities/esafety/ecall/index_en.htm.

[117] V. Jacobson et al. "Networking Named Content". In: *CoNEXT'09* (2009).

[118] Van Jacobson et al. "Networking Named Content". In: *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies*. CoNEXT '09. Rome, Italy: ACM, 2009, pp. 1–12. ISBN: 978-1-60558-636-6. DOI: 10.1145/1658939.1658941. URL: http://doi.acm.org/10.1145/1658939.1658941.

[119] Jakab, L. and Cabellos-Aparicio, A. and Coras, F. and Saucez, D. and Bonaventure, O. "LISP-TREE: A DNS Hierarchy to Support the LISP Mapping System". In: *IEEE Journal on Selected Areas in Communications* 28.8 (2010), pp. 1332–1343. ISSN: 0733-8716. DOI: 10.1109/JSAC.2010.101011.

[120] Jianli Pan and Jain, R. and Paul, S. and Chakchai So-in. "MILSA: A New Evolutionary Architecture for Scalability, Mobility, and Multihoming in the Future Internet". In: *IEEE Journal on Selected Areas in Communications* 28.8 (2010), pp. 1344–1362. ISSN: 0733-8716. DOI: 10.1109/JSAC.2010.101012.

[121] Jianli Pan and Paul, S. and Jain, R. and Bowman, M. "MILSA: A Mobility and Multihoming Supporting Identifier Locator Split Architecture for Naming in the Next Generation Internet". In: *IEEE Global Telecommunications Conference, 2008*. 2008, pp. 1 –6. DOI: 10.1109/GLOCOM.2008.ECP.436.

[122] Jong-Hyouk Lee and Bonnin, J. and Lagrange, X. "Host-based distributed mobility management support protocol for IPv6 mobile networks". In: *IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2012, pp. 61–68. DOI: 10.1109/WiMOB.2012.6379140.

[123] Jong-Hyouk Lee and Bonnin, J.-M. and Seite, P. and Chan, H.A. "Distributed IP mobility management from the perspective of the IETF: motivations, requirements, approaches, comparison, and challenges". In: *IEEE Wireless Communications* 20.5 (2013), pp. 159–168. ISSN: 1536-1284. DOI: 10.1109/MWC.2013.6664487.

[124] Jun Li and Shvartzshnaider, Y. and Francisco, J. and Martin, R.P. and Nagaraja, K. and Raychaudhuri, D. "Delivering Internet-of-Things services in MobilityFirst Future Internet Architecture". In: *3rd International Conference on the Internet of Things (IOT)*. 2012, pp. 31–38. DOI: 10.1109/IOT.2012.6402301.

[125] V.P. Kafle, H. Otsuki, and M. Inoue. "An ID/locator split architecture for future networks". In: *Communications Magazine, IEEE* 48.2 (2010), pp. 138 –144.

[126] R.E. Kahn, S.A. Gronemeyer, and R.C. Burchfiel J.and Kunzelman. "Advances in Packet Radio Technology". In: *Proceedings of the IEEE, vol. 66, no. 11*. IEEE, 1978.

[127] Karagiannis, G. and Altintas, O. and Ekici, E. and Heijenk, G. and Jarupan, B. and Lin, K. and Weil, T. "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards and Solutions". In: *IEEE Communications Surveys Tutorials* 13.4 (2011), pp. 584 –616. ISSN: 1553-877X. DOI: 10.1109/SURV.2011.061411.00019.

[128] J. Kempf. "RFC4831 - Goals for Network-Based Localized Mobility Management (NETLMM)". In: *IETF* (2007).

[129] Ki-Sik Kong and Wonjun Lee and Youn-Hee Han and Myung-Ki Shin and HeungRyeol You. "Mobility management for all-IP mobile networks: MOBILE IPV6 VS. PROXY MOBILE IPV6". In: *IEEE Wireless Communications* 15.2 (2008), pp. 36–45. ISSN: 1536-1284. DOI: 10.1109/MWC.2008.4492976.

[130] M. Kicherer, T. Schlichter, and L. Voelker. "Method for determining an address of a component of a vehicle". Patent US 2012/0054340 A1 (US). 2012.

[131] B-W. Kim and Suwon-si. "Method for setting an Internet Protocol Address using a Vehicle Identification Number". Patent US 7917603 (US). 2011.

[132] Timo Kosch et al. "Automotive Inter-networking". In: Wiley, 2012. Chap. 3, "System Architecture", pp. 37–65.

[133] J. Laganier, T. Koponen, and L. Eggert. "RFC5203 - Host Identity Protocol (HIP) Registration Extension". In: *IETF* (2008).

[134] Lara, Adrian and Ramamurthy, Byrav and Nagaraja, Kiran and Krishnamoorthy, Aravind and Raychaudhuri, Dipankar. "Using OpenFlow to Provide Cut-through Switching in MobilityFirst". In: *Photonic Netw. Commun.* 28.2 (Oct. 2014), pp. 165–177. ISSN: 1387-974X. DOI: 10.1007/s11107-014-0461-3. URL: http://dx.doi.org/10.1007/s11107-014-0461-3.

[135] Leroy, Damien and Bonaventure, Olivier. "Preparing Network Configurations for IPv6 Renumbering". In: *Int. J. Netw. Manag.* 19.5 (Sept. 2009), pp. 415–426. ISSN: 1099-1190. DOI: 10.1002/nem.717. URL: http://dx.doi.org/10.1002/nem.717.

[136] Hyung-Jin Lim et al. "Route Optimization in Nested NEMO: Classification, Evaluation, and Analysis from NEMO Fringe Stub Perspective". In: *IEEE Transactions on Mobile Computing* 8.11 (2009), pp. 1554–1572. ISSN: 1536-1233. DOI: 10.1109/TMC.2009.76.

[137] A. Lindem and J. Arkko. "OSPFv3 Auto-Configuration (work in progress)". In: *IETF* (2014).

[138] B. Liu, S. Jiang, and C. Byrne. "Guidance of Using Unique Local Addresses (Internet Draft)". In: *IETF* (2013).

[139] D. Liu et al. "Distributed Mobility Management: Current practices and gap analysis (Internet draft)". In: *IETF* (2014).

[140] Lorincz, Konrad and Malan, David J. and Fulford-Jones, Thaddeus R. F. and Nawoj, Alan and Clavel, Antony and Shnayder, Victor and Mainland, Geoffrey and Welsh, Matt and Moulton, Steve. "Sensor Networks for Emergency Response: Challenges and Opportunities". In: *IEEE Pervasive Computing* 3.4 (Oct. 2004), pp. 16–23. ISSN: 1536-1268. DOI: 10.1109/MPRV.2004.18. URL: http://dx.doi.org/10.1109/MPRV.2004.18.

[141] R. Maia et al. "Electric vehicle simulator for energy consumption studies in electric mobility systems". In: *Integrated and Sustainable Transportation System (FISTS), 2011 IEEE Forum on*. 2011, pp. 227–232. DOI: 10.1109/FISTS.2011.5973655.

[142] Makaya, C. and Pierre, Samuel. "An Analytical Framework for Performance Evaluation of IPv6-Based mobility Management Protocols". In: *IEEE Transactions on Wireless Communications* 7.3 (2008), pp. 972–983. ISSN: 1536-1276. DOI: 10.1109/TWC.2008.060725.

[143] D. Massey et al. "A Scalable Routing System Design for Future Internet". In: *IPv6'07*. ACM, 2007.

[144] L. Mathy and L. Iannone. "LISP-DHT: Towards a DHT to map identifiers onto locators". In: *ReArch'08*. ACM, 2008.

[145] D. Meyer. "The Locator Identifier Separation Protocol (LISP)". In: *The Internet Protocol Journal* 11.1 (2008), pp. 23–35. ISSN: 1944-1134.

[146] D. Meyer, L. Zhang, and K. Fall. "RFC4984 - Report from the IAB Workshop on Routing and Addressing". In: *IETF* (2007).

[147] MIC. *Ordinance Regulating Radio Equipment*. Tech. rep. Japan's Ministry of Internal Affairs and Communication, 2004. URL: Online19/11/2013at:$http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Resources/Legislation/MRA/040527\_1.pdf$.

[148] R. Moskowitz and P. Nikander. "RFC4423 - Host Identity Protocol (HIP) Architecture". In: *IETF* (2006).

[149] R. Moskowitz et al. "RFC5201 - Host Identity Protocol". In: *IETF* (2008).

[150] Hassnaa Moustafa, Sidi-Mohammed Senouci, and Moez Jerbi. "Vehicular Networks: Techniques, Standards and Applications". In: ed. by Hassnaa Moustafa and Yan Zhang. CRC, 2009. Chap. 1, "Introduction to Vehicular Networks", pp. 1–20.

[151] *MPTCP, MultiPath TCP - Linux Kernel implementation*. Online on 20/03/2012 at: http://mptcp.info.ucl.ac.be/.

[152] Geoff Mulligan. "The 6LoWPAN architecture". In: *Proceeding of EmNets '07*. Cork, Ireland, 2007.

[153] Naderi, Habib and Carpenter, Brian E. "A Review of IPv6 Multihoming Solutions". In: *IARA ICN 2011 : The Tenth International Conference on Networks*. 2011.

[154] T. Narten, R. Draves, and S. Krishnan. "RFC4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6". In: *IETF* (2007).

[155] T. Narten, W. Nordmark E.and Simpson, and H. Soliman. "RFC4861 - Neighbor Discovery for IP version 6 (IPv6)". In: *IETF* (2007).

[156] C. Ng et al. "RFC4889 - Network Mobility Route Optimization Solution Space Analysis". In: *IETF* (2007).

[157] Tien-Thinh Nguyen, Christian Bonnet, and Jerome Harri. "Proxy mobile IPv6 for electric vehicle charging service: Use cases and analysis". In: *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*. 2013, pp. 127–131. DOI: 10.1109/PIMRC.2013.6666117.

[158] P. Nikander, A. Gurtov, and T.R. Henderson. "Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks". In: *IEEE Communications Surveys Tutorials* 12.2 (2010), pp. 186–204. ISSN: 1553-877X. DOI: 10.1109/SURV.2010.021110.00070.

[159] P. Nikander et al. "RFC5202 - End-Host Mobility and Multihoming with the Host Identity Protocol". In: *IETF* (2008).

[160] J. Noel Chiappa. "Endpoints and Endpoint Names: A Proposed Enhancement to the Internet Architecture (Internet Draft)". In: *IETF* (2000).

[161] E. Nordmark and M. Bagnulo. "RFC5533 - Shim6: Level 3 Multihoming Shim Protocol for IPv6". In: *IETF* (2009).

[162] M. O'Dell. "8+8 - An Alternate Addressing Architecture for IPv6 (Inetrnet Draft)". In: *Online on 19/03/2012 at: http://www.potaroo.net/ietf/all-ids/draft-odell-8+8-00.txt* (1996).

[163] M. O'Dell. "GSE - An Alternate Addressing Architecture for IPv6 (Internet Draft)". In: *IETF* (1997).

[164] A. Odlyzko. "'Smart' and 'Stupid' Networks: why the Internet is like Microsoft". In: *Mixed Media* (1997).

[165] T. Oiwa et al. "A network mobility protocol based on LIN6". In: *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th.* Vol. 3. 2003, 1984 –1988 Vol.3. DOI: 10.1109/VETECF.2003.1285372.

[166] C. Pagliari et al. "What is eHealth (4): a scoping exercise to map the field." In: *J Med Internet Res* 7.1 (2005), e9.

[167] J. Pan et al. "Enhanced MILSA Architecture for Naming, Addressing, Routing and Security Issues in the Next Generation Internet". In: *IEEE International Conference on Communications, 2009. ICC '09.* 2009, pp. 1–6. DOI: 10.1109/ICC.2009.5198998.

[168] Jianli Pan, S. Paul, and R. Jain. "A survey of the research on future internet architectures". In: *IEEE Communications Magazine* 49.7 (2011), pp. 26–36. ISSN: 0163-6804. DOI: 10.1109/MCOM.2011.5936152.

[169] Craig Partridge. "A conversation with van jacobson, ACM". Making the case for content-centric networking.

[170] A. Patel et al. "RFC 4283 - Mobile Node Identifier Option for Mobile IPv6 (MIPv6)". In: *IETF* (2005).

[171] Pekka Savola. *Linux IPv6 Router Advertisement Daemon (radvd).* Latest stable version: 1.9.1, June 2012. Online on 18/11/2012 at: http://www.litech.org/radvd/.

[172] C. Perkins, D. Johnson, and J. Arkko. "RFC6275 - Mobility Support in IPv6". In: *IETF* (2011).

[173] A. Petrescu et al. "Default Router List Option for DHCPv6 (DRLO) (work in progress)". In: *IETF* (2013).

[174] Petrescu, A. and Boc, M. and Ibars, C. "Joint IP networking and radio architecture for vehicular networks". In: *11th International Conference on ITS Telecommunications (ITST).* 2011, pp. 230–236. DOI: 10.1109/ITST.2011.6060059.

[175] Petrescu, A. and Boc, M. and Janneteau, C. "Network Mobility with Proxy Mobile IPv6 (Internet draft)". In: *IETF* (2012).

[176] Chairman Powell and Commissioner Adelstein. *Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band).* Tech. rep. Federal Communication Commission (FCC), 10 February 2004. URL: Online19/11/2013at:$http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-03-324A1.pdf$.

[177] Pratt, R. and Tuffner, F. and Gowri, K. *Electric Vehicle Communication Standards Testing and Validation - Phase I: SAE J2847/1.* Tech. rep. Pacific Northwest National Laboratory report for the U. S. Department of Energy, Sept. 2011. URL: Online03/01/2015at:http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20913.pdf.

[178] *PRECIOSA, Privacy Enabled Capability in Co-operative Systems and Safety Applications.* Online on 15/11/2014 at: http://www.preciosa-project.org/.

[179] Bruno Quoitin et al. "Evaluating the benefits of the locator/identifier separation". In: *Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture.* MobiArch '07. Kyoto, Japan: ACM, 2007, 5:1–5:6. ISBN: 978-1-59593-784-1. DOI: 10.1145/1366919.1366926. URL: http://doi.acm.org/10.1145/1366919.1366926.

[180] B. Raunio. "The Internet of things". In: *A report from the November 5, 2009 seminar.* .SE:s Internet guide, Sweden nr. 16, English edition (2010).

[181] Y. Rekhter et al. "RFC1918 - Address Allocation for Private Internets". In: *IETF* (1996).

[182] P. Resnick. "RFC7282 - On Consensus and Humming in the IETF". In: *IETF* (2014).

[183] James Roberts. "The clean-slate approach to future Internet design: a survey of research initiatives". In: *Annals of Telecommunications (Annales Des Télécommunications)* 64.5-6 (2009), pp. 271–276. URL: http://www.springerlink.com/index/10.1007/s12243-009-0109-y.

[184] Rodríguez Natal, Alberto and Jakab, Loránd and Portolés, Marc and Ermagan, Vina and Natarajan, Preethi and Maino, Fabio and Meyer, David and Cabellos Aparicio, Albert. "LISP-MN: Mobile Networking Through LISP". English. In: *Wireless Personal Communications* 70.1 (2013), pp. 253–266. ISSN: 0929-6212. DOI: 10.1007/s11277-012-0692-5. URL: http://dx.doi.org/10.1007/s11277-012-0692-5.

[185] Rottondi, Cristina and Fontana, Simone and Verticale, Giacomo. "Enabling Privacy in Vehicle-to-Grid Interactions for Battery Recharging". In: *MDPI Energies* 7.5 (2014), pp. 2780–2798. ISSN: 1996-1073. DOI: 10.3390/en7052780. URL: http://www.mdpi.com/1996-1073/7/5/2780.

[186] P. Saint-Andre. "RFC6120 - Extensible Messaging and Presence Protocol (XMPP): Core". In: *IETF* (2011).

[187] J. Saltzer. "RFC1498 - On the Naming and Binding of Network Destinations". In: *IETF* (1993).

[188] J.H. Saltzer, D.P. Reed, and D.D. Clark. "End-to-End Arguments in System Design". In: *MIT Lab for computer science*. ACM, 1984.

[189] D. Saucez et al. "Designing a Deployable Internet: The Locator/Identifier Separation Protocol". In: *IEEE Internet Computing* 16.6 (2012), pp. 14–21. ISSN: 1089-7801. DOI: 10.1109/MIC.2012.98.

[190] Damien Saucez, Luigi Iannone, and Benoit Donnet. "A First Measurement Look at the Deployment and Evolution of The locator/Id Separation Protocol". In: *SIGCOMM Comput. Commun. Rev.* 43.2 (Apr. 2013), pp. 37–43. ISSN: 0146-4833. DOI: 10.1145/2479957.2479963. URL: http://doi.acm.org/10.1145/2479957.2479963.

[191] F. Schaub, Zhendong Ma, and F. Kargl. "Privacy Requirements in Vehicular Communication Systems". In: *International Conference on Computational Science and Engineering (CSE '09)*. Vol. 3. 2009, pp. 139–145. DOI: 10.1109/CSE.2009.135.

[192] Rajiv C. Shah and Jay P. Kesan. "The Privatization of the Internet's Backbone Network". In: *Journal of Broadcasting and Electronic Media* 51.1 (2007), pp. 93–109. DOI: 10.1080/08838150701308077. eprint: http://dx.doi.org/10.1080/08838150701308077. URL: http://dx.doi.org/10.1080/08838150701308077.

[193] J.F. Shoch. "A note on Inter-Network Naming, Addressing, and Routing". In: *Internet Experiment Note* (1978).

[194] D. Slamanig and C. Stingl. "Privacy aspects of ehealth". In: *ares* 0 (2008), pp. 1226–1233.

[195] D. Smetters and V. Jacobson. "Securing Network Content". In: *Parc technical report* (2009).

[196] I. Soto et al. "Nemo-enabled localized mobility support for internet access in automotive scenarios". In: *Communications Magazine, IEEE* 47.5 (2009), pp. 152–159. ISSN: 0163-6804. DOI: 10.1109/MCOM.2009.4939291.

[197] D.D. Stancil, F. Bai, and L. Cheng. "Vehicular Networking, Automotive applications and beyond". In: ed. by Wiley. Wiley, 2009. Chap. 3, "Communication systems for Car-2-X Networks", pp. 45–81.

[198] ETSI Standard. *European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band*. Tech. rep. European Telecommunications Standards Institute, 2009. URL: Online19/11/2013at:$http://www.etsi.org/deliver/etsi_es/202600_202699/202663/01.01.00_50/es_202663v010100m.pdf$.

[199] International standard. *ISO 15118-1:2013, "Road vehicles - Vehicle to grid communication interface - Part 1: General information and use-case definition"*. Tech. rep. International Organization for Standardization, 2013.

[200] International standard. *ISO/IEC 7498-1:1994 Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*. Tech. rep. International Organization for Standardization, Second Edition, 1994.

[201] Ion Stoica et al. "Chord: A scalable peer-to-peer lookup service for internet applications". In: SIGCOMM '01. ACM, 2001, pp. 149–160.

[202] S.D. Strowes. "Compact routing for the future internet". PhD thesis. University of Glasgow, 2012.

[203] Lakshminarayanan Subramanian et al. "HLP: a next generation inter-domain routing protocol". In: *Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*. SIGCOMM '05. Philadelphia, Pennsylvania, USA: ACM, 2005, pp. 13–24. ISBN: 1-59593-009-4. DOI: 10.1145/1080091.1080095. URL: http://doi.acm.org/10.1145/1080091.1080095.

[204] Department of Information Teraoka-lab, Faculty of Science Computer Science, and KEIO Univ. Technology. "LIN6". In: *Online on 15/03/2012 at: $http://www.tera.ics.keio.ac.jp/?page_id=653$* (2010).

[205] Y. Toor, P. Muhlethaler, and A. Laouiti. "Vehicle Ad Hoc networks: applications and related technical issues". In: *Communications Surveys & Tutorials, IEEE* 10.3 (2008), pp. 74–88. DOI: 10.1109/COMST.2008.4625806. URL: http://dx.doi.org/10.1109/COMST.2008.4625806.

[206] *TRIAD, Translating Relaying Internet Architecture integrating Active Directories*. Online on 20/03/2012 at: http://www-dsg.stanford.edu/triad/.

[207] *Trilogy, Architecting the future Internet*. Online on 20/03/2012 at: http://http://trilogy-project.org/.

[208] O. Troan and R. Droms. "RFC3633 - IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6". In: *IETF* (2003).

[209] Turner, J.S. and Taylor, D.E. "Diversifying the Internet". In: *IEEE Global Telecommunications Conference*. Vol. 2. 2005, 6 pp.–760. DOI: 10.1109/GLOCOM.2005.1577741.

[210] G. Van de Velde et al. "IPv6 Network Architecture Protection". In: *IETF* (2005).

[211] Venkataramani, Arun and Kurose, James F. and Raychaudhuri, Dipankar and Nagaraja, Kiran and Mao, Morley and Banerjee, Suman. "MobilityFirst: A Mobility-centric and Trustworthy Internet Architecture". In: *SIGCOMM Comput. Commun. Rev.* 44.3 (July 2014), pp. 74–80. ISSN: 0146-4833. DOI: 10.1145/2656877.2656888. URL: http://doi.acm.org/10.1145/2656877.2656888.

[212] Ovidiu Vermesan et al. "Smart, connected and mobile: Architecting future electric mobility ecosystems". In: *Design, Automation Test in Europe Conference Exhibition (DATE), 2013*. 2013, pp. 1740–1744. DOI: 10.7873/DATE.2013.350.

[213] VinPower. *VinPower: VIN Solutions for The Automotive Industry*. Online on 09/04/2013 at: http://www.vinpower.com/.

[214] L. Wang et al. "Data naming in Vehicle-to-Vehicle communications". In: *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2012, pp. 328 –333. DOI: 10.1109/INFCOMW.2012.6193515.

[215] Ward, J. and Worrall, S. and Agamennoni, G. and Nebot, E. "The Warrigal Dataset: Multi-Vehicle Trajectories and V2V Communications". In: *IEEE Intelligent Transportation Systems Magazine* 6.3 (2014), pp. 109–117. ISSN: 1939-1390. DOI: 10.1109/MITS.2014.2315660.

[216] M. Wasserman and F. Baker. "RFC6296 - IPv6-to-IPv6 Network Prefix Translation". In: *IETF* (2011).

[217] B. Wiedersheim et al. "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough". In: *Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*. 2010, pp. 176–183. DOI: 10.1109/WONS.2010.5437115.

[218] Gongjun Yan et al. "WEHealth: A Secure and Privacy Preserving eHealth Using NOTICE". In: *Proceedings of the International Conference on Wireless Access in Vehicular Environments (WAVE)*. Dearborn, MI, 2008.

[219] X. Yang, D. Clark, and A.W. Berger. "NIRA: A New Inter-Domain Routing Architecture". In: IEEE/ACM Transactions on Networking '07. IEEE/ACM, 2005.

[220] L. Yeh, T. Lemon, and M. Boucadair. "Prefix Pool Option for DHCPv6 Relay Agent on the Provider Edge Routers (work in prgress)". In: *IETF* (2013).

[221] Yizhen Wu and Ke Chen and Kaiping Xue and Dan Ni. "NEMO-based mobility management in LISP network". In: *Sixth International Conference on Wireless Communications and Signal Processing (WCSP)*. 2014, pp. 1–6. DOI: 10.1109/WCSP.2014.6992174.

[222] X. Zhou et al. "RFC7148 - Prefix Delegation Support for Proxy Mobile IPv6". In: *IETF* (2014).

[223] Z. Zhu, R. Wakikawa, and L. Zhang. "RFC6301 - A Survey of Mobility Support in the Internet". In: *IETF* (2011).

[224] Zuniga, J.C. and Bernardos, C.J. and de la Oliva, A. and Melia, T. and Costa, R. and Reznik, A. "Distributed mobility management: A standards landscape". In: *IEEE Communications Magazine* 51.3 (2013), pp. 80–87. ISSN: 0163-6804. DOI: 10.1109/MCOM.2013.6476870.

Glossary

Notation	Description	Pages
B		
BGP	Border Gateway Protocol	7
D		
DFZ	Default Free Zone	I, 1, 16
DMM	Distributed Mobility Management	76
DSRC	Dedicated Short-Range Communication	47
E		
E2E	end-to-end	2, 8, 9, 42
EHR	Electronic Health Record	60
F		
FEV	Fully Electric Vehicle	51, 52, 70
I		
ITS	Intelligent Transportation Systems	I, 1, 42, 45, 47
IVC	Inter-Vehicle Communication	I, 1, 2, 39, 42

Notation	Description	Pages
L		
LFN	Locally Fixed Node	82
LMS	LISP Mapping System	116
M		
MR	Mobile Router	56
N		
NAT	Network Address Translation	8, 11
NEMO	Network Mobility	70
P		
PAA	Provider Allocated Addressing	71
PHR	Personal Health Record	55
PIA	Provider Independent Addressing	71
S		
SDO	Standard Development Bodies	48
T		
TE	Traffic Engineering	14
U		
ULA	Unique IPv6 Local Addresses	72

Notation	Description	Pages
V		
V2I	Vehicle-to-Infrastructure	45, 50
V2V	Vehicle-to-Vehicle	45, 50
VANET	Vehicular Ad-Hoc Network	I, 1, 2, 39, 42
VNT	VIN-based Network Address Translation	140
VULA	VIN-based Unique Local IPv6 Addressing	140
W		
WAVE	Wireless Access in Vehicular Environments	47