Geographic addressing and routing
for vehicular communications
http://www.geonet-project.eu/

ICT-2007.6.1: ICT for intelligent
vehicles and mobility services

GeoNet STREP N°216269

D1.2 Final GeoNet Architecture Design

DATE	January 20th, 2010
CONTRACTUAL DATE OF DELIVERY TO THE EC	M22 – December 2009
ACTUAL DATE OF DELIVERY TO THE EC	M23 – December 2009
EDITOR, COMPANY	Thierry Ernst, INRIA
WORKPACKAGE	WP1 Architecture
DOCUMENT CODE	GeoNet-D.1.2-v1.2
SECURITY	Public

DOCUMENT HISTORY

Release	Date	Reason of change	Status	Distribution
0.0	23/11/09	First internal draft	Draft	Internal
0,1	08/12/09	First version circulated internally	Draft	Internal
0.5	17/12/09	Version for review	Pre final	Internal
0,6	29/12/09	Reviewed version	Pre final	EC
0,7	04/01/10	Adjustment with D2.2	Pre final	Internal
0,8	05/01/10	Input from GeoNet partners	Pre final	Internal
1.0	12/01/10	Final version submitted to EC	Final	EC
1.1	20/01/10	Few typos were fixed	FInal	ETSI
1.2	17/06/10	Revised final version submitted to EC	Final	EC

Name of the coordinating person: Arnaud de La Fortelle, INRIA
E-mail: Arnaud.de_La_Fortelle@inria.fr

Contents

1. Executive Summary

1.1 Introduction

This document, as its title "Final GeoNet Architecture Design" stands for, describes the final version of the communication architecture as it is implemented under the framework of the GeoNet project. The architecture presented in this deliverable corresponds to the most up-to-date version of the IPv6 GeoNetworking architecture designed by the GeoNet project. The GeoNet project being completed in February 2010, there will not be any further update of this architecture in the framework of the GeoNet project and this architecture is thus the final one. It is hoped that the output of GeoNet will either be integrated or will influence the design of ETSI TS ITS [ETSI-TS-106-665] and ISO TC204 WG16 [ISO-21217] standardised ITS communication architectures where GeoNetworking capabilities are currently being integrated [ETSI-TS-102-636-6-1].

The architecture presented in this document is a revision of the “Preliminary Architecture Design” as found in [GeoNetD1.1]. New modules have been included, most noticeably a vertical management layer. The final design has largely inherited from feedback received internally in the course of the GeoNet project based on the specification [GeoNetD2.2], implementation [GeoNetD3.1] and conformance tests [GeoNetD4.1] phases. For details, the interested readers can access to the other deliverables available from the GeoNet web page.

Though it is a public document available to a large audience, the reader should be reminded that as a deliverable (D1.2) of the GeoNet project the first purpose of this document is to report to the European Commission the output of the Work Package 1 “Architecture”.

1.2 Objectives

The GeoNet project aims at combining IPv6 networking and Car-to-Car Communication Consortium's (C2C-CC) GeoNetworking capabilities into a single protocol stack for Intelligent Transportation Systems (ITS). We refer to *IPv6 GeoNetworking* as the combination of these two capabilities. The work currently undergoing within the C2C-CC was assumed as the starting point. Scenarios not involving IPv6 or communications in IPv6 not involving C2C-CC's GeoNetworking are out of scope of the GeoNet project. In addition, the GeoNet project is tasked to work only on the network layer. This is reflected by the red box in Figure 1 which shows the part of the C2C-CC protocol stack affected by GeoNet's work.

The purpose of this architecture document is to describe what is IPv6 GeoNetworking: what functions are to be provided, under which conditions it shall operate (e.g. communication scenarios, communication environment with or without infrastructure support) and how it shall perform (e.g. scale to a large number of vehicles).

Prior to the definition of the GeoNet architecture as described in the following sections, earlier work on the topics related to GeoNet was analysed, including past IETF work on GeoNetworking. An analysis of IETF IPv6 mobility standards (turning around NEMO and the CALM Communication Architecture work as implemented in the CVIS project) was conducted in order to identify the necessary protocol extensions to be brought to IPv6 so that C2C-CC's GeoNetworking features fits together with an IPv6 protocol stack. Then, partners agreed on the terminology (see in Annex D for the complete definitions), design goals (Section 3) and GeoNetworking scenarios (Section 4). The discussions led to the design of the GeoNet architecture (Section 5) combining IPv6 networking with mobility support together with C2C-CC's GeoNetworking capabilities. The architecture is divided into modules and Service Access Points (SAPs) between layers. The modules and SAPs are outlined in Section 6 and specified in the GeoNet deliverable [GeoNetD2.2].

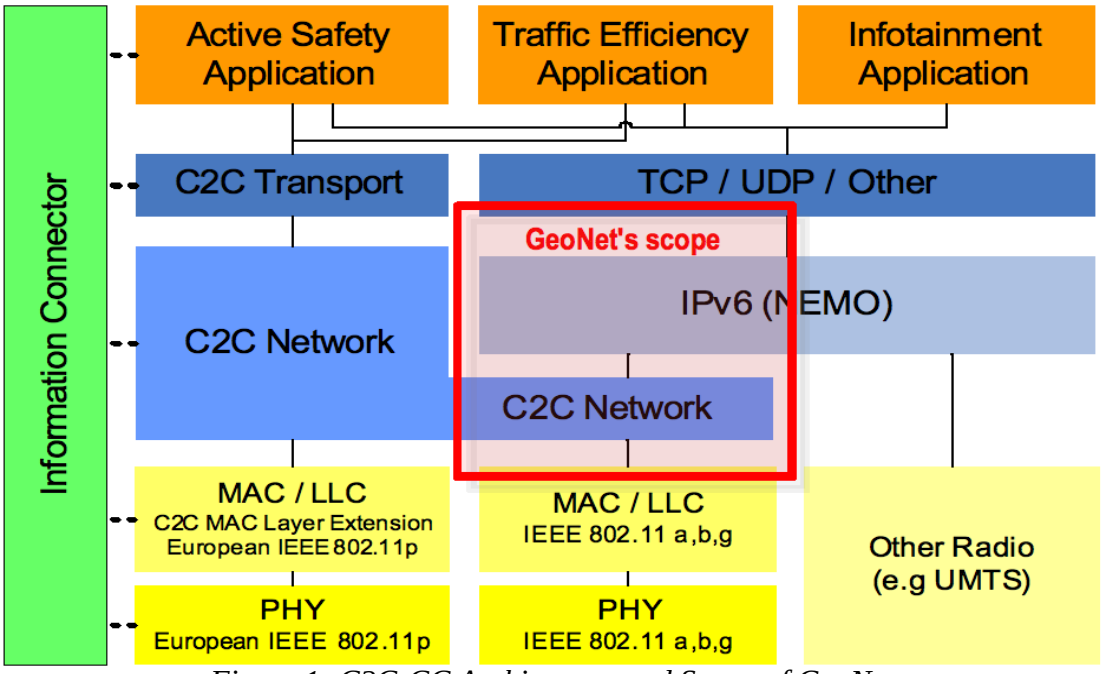

Figure 1: C2C-CC Architecture and Scope of GeoNet

1.3 Relation with Standardisation Activities

In an effort towards harmonisation, the European Commission's COMeSafety Specific Support Action has issued an European ITS Communication Architecture [COMeSafety2008] (see Figure 2). The GeoNet architecture complies with this architecture by relying on the IPv6 suite of protocols for communications taking place over the Internet or between vehicles using IP-based applications while acting as communication endpoints. By continuously contributing to ETSI ITS activities, GeoNet aims at influencing the standardisation of ITS communications in Europe, particularly the work performed on IPv6 GeoNetworking by ETSI TC ITS [ETSI-TS-102-636-6-1]. GeoNet know-how on the design of IPv6 GeoNetworking shall also help enhancing ITS communication architectures defined by ETSI TC ITS [ETSI-TS-102-665] and ISO TC 204 [ISO-21217].

Though no specific emphasis is put on the ISO TC 204 WG16's CALM communication architecture, the GeoNet architecture also complies with ISO's CALM IPv6 Networking specification [ISO-21210] as implemented within the CVIS European project: the same approach is used for maintaining Internet connectivity and session continuity (NEMO [RFC3963] and MCoA [RFC5648] protocols are parts of the GeoNet architecture as in ISO's CALM). This will ensure an easier integration of GeoNet's output within CALM's standardisation effort.

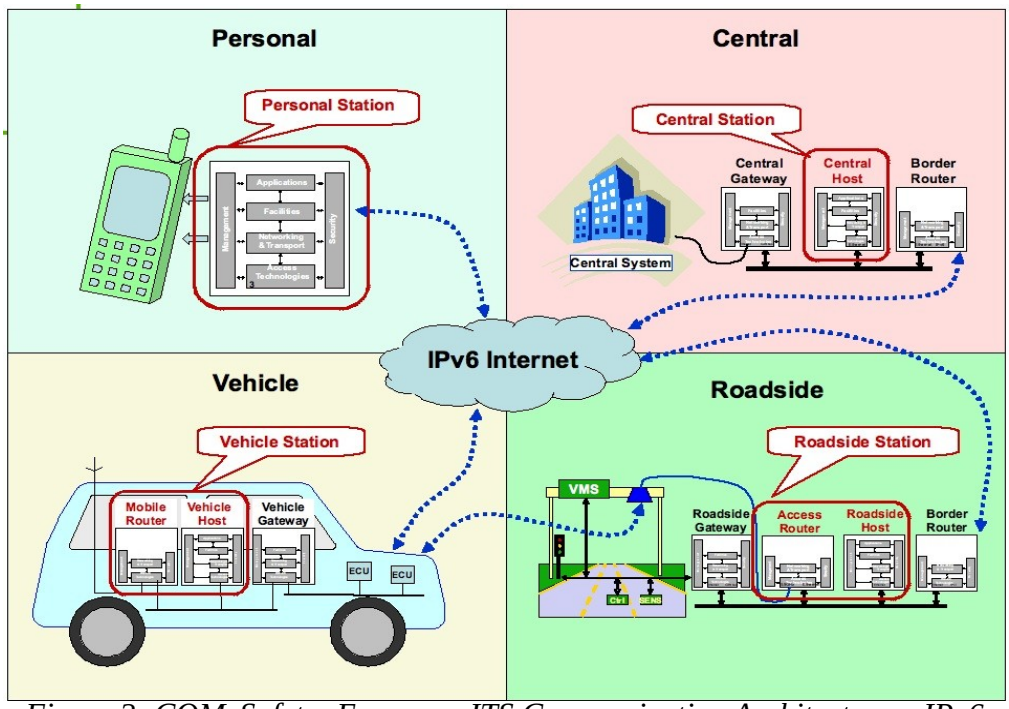

Figure 2: COMeSafety: European ITS Communication Architecture – IPv6

In the COMeSafety, ETSI and ISO ITS communication architectures as illustrated on Figure 2, involved communication system components include the vehicle sub-system, the roadside sub-system, the central sub-system (in charge of providing application and network services and other functions to vehicles and the roadside) and the personal sub-system (third parties located in the Internet communicating with ITS-dedicated components and typically belonging to the users, possibly portable and themselves brought into vehicles).

In GeoNet, this model is simplified as the entities involved are IPv6 nodes located in any of these sub-systems or anywhere in the Internet and communicating end-to-end using on one hand IPv6 and on the other hand GeoNetworking (C2CNet over the GeoNet domain) capabilities. The IPv6 entities involved in GeoNet communications are thus as follows:

- **IPv6 nodes located in the vehicle sub-system**: the IPv6 Mobile Router (MR) and its attached IPv6 nodes (respectively, the On-Board Unit (OBU) and Application Units (AUs));

- **IPv6 nodes located in the roadside sub-system**: the IPv6 Access Router (AR) and its attached IPv6 nodes (respectively the Roadside Unit (RSU) and AUs);

- **IPv6 nodes located in the Internet**: IPv6 nodes located in the central or personal sub-systems or anywhere in the Internet and corresponding with vehicles and the roadside. These typically include ITS-dedicated servers, the Home Agent, nodes hosting other networking functions (e.g. DNS) and other third parties.

1.4 Architecture Design Overview

The GeoNet architecture includes a cross-management layer as introduced in the ITS station architecture specified by ETSI [ETSI-TS-102-665] and ISO [ISO-21217]. The architecture considers three types of nodes that implement a subset of these modules: GeoNet OBUs in the vehicle, GeoNet RSUs on the roadside and nodes running GeoAware applications.

The GeoNet architecture supports safety, non safety and infotainment types of applications and considers communications involving nodes located in the vehicle sub-system (see Section 4):

- **Infrastructure-less communications**: between vehicles alone without infrastructure support;

- **Infrastructure-based communications**: between vehicles and roadside peers or Internet peers.

The mode of communication could be either point-to-point (unicast or anycast), or point-to-multipoint (multicast). For both modes, GeoNet introduces a geographic range of communication (respectively GeoUnicast, GeoAnycast and GeoBroadcast).

The GeoNetworking features are only implemented into the mobile routers and access routers which are respectively referred to as GeoNet OBUs and GeoNet RSUs. From an IP point of view all of these system components are independent IPv6 networks linked over the Internet. GeoNet OBUs and GeoNet RSUs form a vehicular ad-hoc network (VANET) cloud which we refer to as the GeoNet domain where routing is performed using GeoNetworking addressing and routing. As a result from this, all functional modules and Service Access Points (SAPs) are presented in an abstract form (see Section 6). Modules are detailed for each IPv6 entity involved, i.e. the mobile router, the access router and other IPv6 nodes.

Among several options, it was concluded that IPv6's multicast capabilities would best fit the objective of combining IPv6 and GeoNetworking into a single communication architecture. IP multicast is used to efficiently propagate data packets to a set of recipients. The principle of IP multicast is that only one copy of a given packet is transmitted on any given link, and only to the condition that there is are known destinations reachable through this link.

2. Structure of the Document

The present document is structured as follows:

- Section 3 lists the design goals of the GeoNet architecture;
- Section 4 discusses communication scenarios supported by the GeoNet architecture;
- Section 5 presents the design of the GeoNet architecture and discusses the role of the different layers, their interaction and the procedures for distributing IPv6 packet over the C2C-CC network layer;
- Section 6 describes the main functional modules and Service Access Points (SAPs) between layers;Davis
- Section 7 details how packets delivery is performed over the GeoNet domain made of nodes with GeoNetworking capabilities;
- Annex A lists all the persons who directly contributed to this document;
- Annex B presents a thorough security and privacy threat analysis conducted in parallel to ensure that the new architecture does not introduce new security and privacy concerns in addition to well-known ones;
- Annex C presents the State-of-the-Art analysis (earlier work performed on GeoNetworking (addressing and routing, with or without IPv6);
- Annex D lists the terms that are used to defined the GeoNet architecture. The terminology is divided into three main families: GeoNet newly defined terms, IPv6 terms and generic networking. The reader is advised to refer to this section whenever a new term appears or in case of doubt in the interpretation of some term;
- Annex E lists all references provided in this document.

3. Design Goals

This section presents the design goals which have led to the GeoNet architecture in its present form. They take into account the motivations behind IPv6 GeoNetworking (communication modes and scenarios, Internet connectivity, etc.), the type of applications to be supported (safety, traffic efficiency and infotainment), and deployment considerations (in-vehicle networks, backward compatibility, security, scalability, performance, etc.). They serve as guidelines and help understanding the technical choices made during the design of the architecture. The design goals are as follows:

1. **IPv6 support**: The GeoNet architecture shall combine C2C-CC's GeoNetworking with IPv6 networking. This combination is referred to as IPv6 GeoNetworking.

2. **Communication endpoints**: The GeoNet architecture shall support communications involving on one side a vehicle endpoint and on the other side i) other vehicle endpoints (V2V), ii) roadside endpoints (V2I & I2V) or iii) Internet endpoints.

3. **Geographic data transmission**: The GeoNet architecture shall support data transmission from a vehicle node or an infrastructure node to i) another vehicle or infrastructure node in a certain geographic position, ii) a set of vehicles or infrastructure nodes in a certain geographic zone or iii) an arbitrary vehicle or infrastructure node in a certain geographic zone.

4. **Communication modes:** Vehicles shall be able to form a self-organised ad-hoc communication network without infrastructure coordination and the network may or may not be connected to the infrastructure. The GeoNet architecture shall thus provide for i) direct communication between endpoints without involving the infrastructure ii) communications between endpoints via the infrastructure and iii) communications between endpoints via the Internet.

5. **Destination set**: Routing functions must efficiently support point-to-point, and point-to-multipoint communication

6. **Internet connectivity**: in-vehicle embedded IP nodes shall be accessible from the Internet and be able to communicate with any peer node attached to the Internet. The Internet connectivity shall be provided through any communication media (either sequentially or simultaneously).

7. **Compatibility and interoperability**: The GeoNet architecture ensure backward compatibility with legacy systems, features and protocols and interoperability with architectures designed by ETSI TC ITS and ISO TC204 WG16.

8. **Reusability:** Existing mechanisms able to cope with particular system requirements shall be reused whenever possible instead of designing new ones.

9. **Migration Transparency and Seamless Mobility:**

   - **Ubiquitous connectivity** to the Internet has to be provided to all devices in a vehicle, since continuous sessions are expected to be maintained as the vehicle changes its point of attachment.

   - **Media diversity**: IPv6 GeoNetworking shall allow the use of multiple communication media while using GeoNetworking capabilities on one specific media.

   - **Disconnected access**: IPv6 GeoNetworking shall continue to work even in the face of lack of Internet access or intermittent access to the Internet.

10. **Local and global mobility:**

    - **Global mobility support:** a vehicle can change its point of attachment from an access network to another access network under a different administrative authority and using different access media.

    - **Local mobility support:** a vehicle can change its point of attachment to an access network while using the same access media.

11. **Separability:** policies can be dynamically changed according to the applications and environment.

12. **Scalability:**

    - The solution shall not impact the Internet routing structure, especially its routing table.

    - The solution should work with an unlimited number of vehicles worldwide.

    - The solution should work under sparse and dense population of nodes.

13. **Security and location privacy:**

    - **Location Privacy:** The GeoNet architecture shall ensure that current position of the vehicles can not be determined by non-authorised third parties. top

    - **Protection:** The GeoNet architecture should provide a level of security equivalent or higher than legacy IPv6 standards (i.e. the solution shall not create new threats). It shall ensure protection of IPv6 control messages (the level of protection depends on the use case) and allow the protection of payload messages when needed by the application. Protection includes authentication of the sender, authorisation to perform the action, confidentiality of the data contained in the messages, anti-replay of messages, etc."

14. **Performance:** IPv6 GeoNetworking capabilities shall be provided in such a way that efficient IPv6 communications are realised therefore minimising latency, processing overhead, packet overhead, routing inefficiencies. Performance requirements are set by application type: end-to-end latency, priority, transmission rate, etc. It is particularly relevant within the context of security, due to the high processing requirements and packet overhead usually required by security operations (e.g., cryptography).

    - **Prioritisation:** the GeoNet architecture shall provide a mechanism to process packets with different priorities, highest priority for safety packets.

    - **Reliability:** The GeoNet architecture should provide reliable network layer communications, with highest reliability for safety messages. The GeoNet architecture shall allow extensions by mechanisms for guaranteeing reliable link layer communications.

    - **Latency:** Low-latency network layer implementation of the GeoNet architecture should be possible. The GeoNet architecture shall allow extensions by mechanisms for guaranteeing low-latency link layer communications.

    - **Efficiency:** The GeoNet architecture overhead should be kept low. This concerns both implicit and explicit signalling, routing and packet forwarding and the number of re-transmissions. Take notice that trade-offs between efficiency and reliability should be studied (for better Overhead Ratio).

    - **Fairness:** The GeoNet architecture should be fair among different nodes with respect to bandwidth usage and fairness applies for the same type of messages.

    - **Robustness:** The GeoNet architecture should be robust again security attack and malfunction in communication nodes.

15. **Protocol layering**: The GeoNet architecture follows the classical Internet protocol layered approach, in a transparent and end-to-end manner, without involving middle-boxes that perform any transformation/translation to protocol headers, others than the source node and end node themselves.

4. Communication Scenarios

The purpose of this section is to define the communication scenarios supported by the GeoNet architecture. Only scenarios involving both IPv6 and GeoNetworking are considered by the GeoNet project although non-IP communications could typically be supported too. At the beginning of the project, GeoNet defined communication scenarios for GeoNetworking, and made major contributions to the technical specification in ETSI TC ITS [ETSI-TS-102-636-2]. Based on these scenarios, GeoNet further draws communications scenarios requiring IPv6 support.

From an IPv6 GeoNetworking perspective, communication scenarios are first classified according to the sender and the receiver **communication endpoints** (vehicle, roadside, Internet)**.** These are further distinguished according to their **communication mode**, i.e. whether only the vehicles (infrastructure-less), the vehicles and the roadside, or the vehicles and the Internet are involved. Then, another distinction is the **destination range**: is the destination a single communication endpoint or multiple communication endpoints? A quality discrimination factor is the type of flow: road safety, traffic efficiency, infotainment or signalling.

The number of hops (e.g. Single hop or Multi-hop) is not a discrimination factor since single-hop may be considered as a special case of multi-hop. Performance requirements (e.g. latency and reliability) are not considered in the classification. However, it has to be noted that different communication flows under the same communication mode may have totally different requirements on performance, which may have an important influence on the protocol design. This is why we introduce **flow type** as a quality discrimination factor.

Some typical scenarios are presented at the end of this section after a brief description of each of the IPv6 flow types, communication endpoints, communication modes and destination ranges. Only scenarios that must be supported by the IPv6 GeoNetworking architecture are described. This is why these scenarios differ quite substantially from scenarios discussed in ETSI TC ITS documents. The list is not exhaustive.

4.1 IPv6 Flow Type

There are basically four types of IPv6 communication flows to be considered in scenarios belonging to IPv6 GeoNetworking:

- IPv6 application-bound safety communication flows.
- IPv6 application-bound traffic efficiency communication flows.
- IPv6 application-bound infotainment communication flows.
- IPv6 network-bound signalling communication flows.

Note that safety and traffic efficiency communication flows not based on IP could also be supported by the GeoNet architecture but are not in the scope of GeoNet as a project and thus are not dealt with in GeoNet deliverables.

4.2 IPv6 Communication Endpoints

Without detailing which nodes are effectively involved, what matters the most for discriminating between the scenarios is whether the communication endpoints are located in the **vehicle**, the **roadside** or anywhere else in the **Internet**. As a result, the following communication modes hold in the context of IPv6 GeoNetworking:

- **Vehicle-Vehicle**: Communication occurs between a vehicle and another vehicle.
- **Vehicle-Roadside**: Communication occurs between a vehicle and the roadside.
- **Vehicle-Internet**: Communication occurs between a vehicle and a node located in the Internet.

Communication between endpoints not involving a vehicle (e.g. Roadside-Internet) is out of scope of IPv6 GeoNetworking.

Also, a roadside endpoint may sometimes functions similarly to as a vehicle endpoint. In such cases, it will be considered a vehicle endpoint.

4.3 IPv6 Communication Modes

Looking from another angle, what also matters to define the scenarios is whether:

- no infrastructure is traversed: Vehicle-Vehicle;
- the roadside is involved: Vehicle-Roadside; or
- the Internet is involved: Vehicle-Internet.

4.3.1 Vehicle-based Communication Modes

This mode covers Vehicle-to-Vehicle communications **without infrastructure support**. Communication occurs between a vehicle and another or several vehicles. Applications based on IPv6 as well as other applications not based on IP can be supported, but only IPv6-based communications are in the scope of GeoNet**.** This mostly concerns safety and traffic efficiency applications.

4.3.2 Roadside-based Communication Modes

This mode covers Vehicle-to-Roadside, Roadside-to-Vehicle and Vehicle-to-Vehicle communications **with infrastructure support**. Applications based on IPv6 as well as other applications not based on IP can be supported, but only IPv6-based communications are in the scope of GeoNet. This mostly concerns safety and traffic efficiency applications.

4.3.3 Internet-based Communication Modes

This mode covers Vehicle-Internet communications with infrastructure support. Note that any destination reachable through the Internet - including a destination vehicle - is considered as an Internet communication endpoint from the viewpoint of the source. Only applications based on IPv6 are supported. This mostly concerns infotainment, but numerous safety and traffic efficiency applications could benefit from this communication mode.

4.4 Destination Range

The destination range to consider from an IPv6 communication flow viewpoint are the following:

- **IPv6 unicast**: Communication between a single communication endpoint and at another single communication endpoint.
- **IPv6 multicast**: Communication between a single communication endpoint and multiple communication endpoints
- **IPv6 anycast**: Communication between a single communication endpoint and a single arbitrary communication endpoint from a set of predefined devices.

The destination range to consider from a GeoNetworking communication flow viewpoint are the following:

- **GeoUnicast**: Communication between a single communication endpoint and its identified counterparty located at a given geographical position.
- **GeoAnycast**: Communication between a single communication endpoint and a single arbitrary communication endpoint from a set of predefined devices within a given geographical area.
- **GeoBroadcast**: Communication between a single communication endpoint and all communication endpoints within a given geographical area.

Unicast, multicast and anycast are legacy communication means in IPv6. Geocast (i.e. GeoUnicast, GeoAnycast and GeoBroadcast) does not currently exist in IPv6 though the description of scenarios in the following sub-sections demonstrates the needs to explicitly send information to a destination or set of destinations in a specific geographic position or area. We will see in forthcoming sections of this document how the proposed IPv6 GeoNetworking architecture will accommodate such scenarios and needs.

Take notice that in a situation where there are multiple destinations (typically GeoBroadcast or IP multicast), the distinct destinations may be ranged simultaneously into several of the communication endpoints and communication modes (e.g. Vehicle-Vehicle and Vehicle-Roadside).

4.5 Description of Scenarios

The scenarios below are listed according to the communication mode and the destination range. The other distinctive parameters of the classification (endpoints, destination range, flow type and number of hops) are given in the description of each scenario.

The scenarios are numbered according to two letters and one order number (XYi):

- 1st letter is either Vehicle-based (V), Roadside-based (R) or Internet-based (I);
- 2nd letter is either Unicast (U), Multicast (M) or Anycast (A).

Figure 3 below shows a combination of three scenarios:

1. Vehicle A detect black ice on the road. As an immediate action, the traffic hazard application running on Vehicle A informs all the cars driving on the same road behind it about this traffic hazard and the information is forwarded (GeoBroadcast) as long as there are vehicle forwarders within a limited geographical area. As a result the GeoBroadcast message reaches Vehicle B which further GeoBroadcast the same message to other vehicles and the message reaches vehicle C). This corresponds to scenario VM1 in the forthcoming sub-sections.

2. In addition, this road hazard information is going to be valid for some time and vehicles not immediately following but heading to the same spot could benefit from this information too. Vehicle A would thus send this information to a traffic road center server located in the Internet, through the Internet access provided by RSU1 (Vehicle B could also transmit this information through e.g. a 3G media, but this is out of scope of the scenarios investigated by the GeoNet project). IP – thus IPv6 – must be used in such a case, and Vehicle A transmits this information using IPv6 unicast, but through the RSU, either directly as shown on the figure, or through intermediate vehicles when there is no RSU in the radio range. GeoUnicast is thus used to reach the RSU. This corresponds to scenario IU1 in the forthcoming sub-sections.

3. The road traffic center server periodically transmits road hazard information to all vehicles in some specific geographic area. The black ice report only concern vehicles heading to a specific point on a specific road. The server would thus send an IP packet using IPv6 multicast to RSU2 which would in turn GeoBroadcast it to all vehicles in the specific geographic area. Vehicle E would get the packet first and would retransmit it to other vehicles (i.e. Vehicles D and F). This corresponds to scenario IM1 in the forthcoming sub-sections.

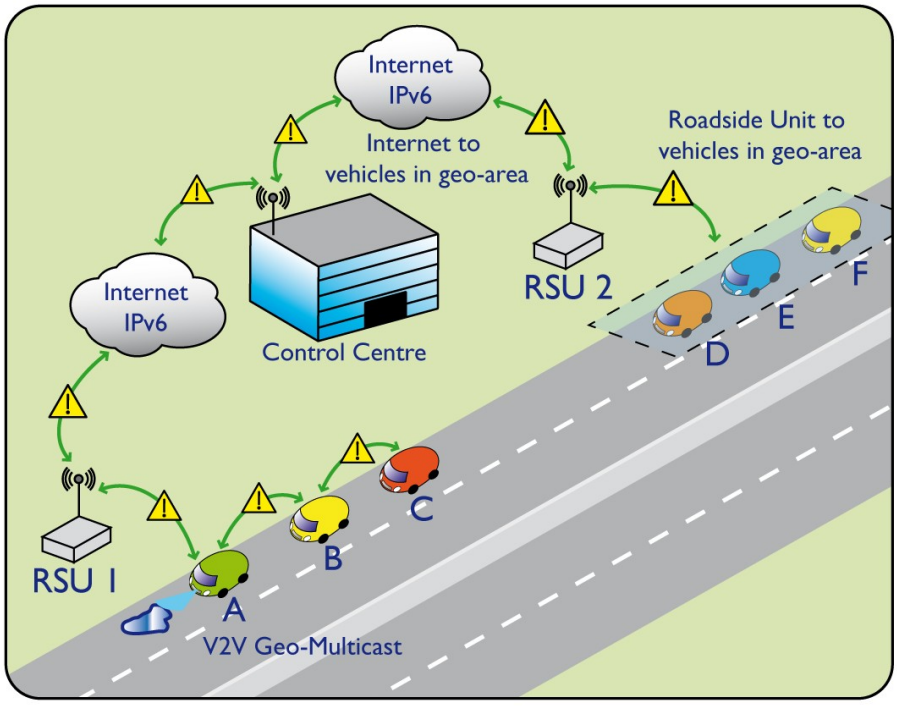

Figure 3: Example Use Case: Road Traffic Hazard Alert

4.5.1 IPv6 Vehicle-based Unicast Scenarios (VU)

Scenario VU1: Packets exchanged between two vehicles without infrastructure support:

- Endpoints: vehicles.
- Destination range: single vehicle endpoint of known identity whose position and identity are known through received beacons and/or a location service (GeoUnicast).
- Example use cases:
  - Road safety: Event-driven low-latency transmission from a vehicle announcing to a peer vehicle behind that it is decreasing speed.
  - Infotainment: Delay-tolerant gaming between two vehicles with known identities.

4.5.2 IPv6 Vehicle-based Anycast Scenarios (VA)

Scenario VA1: Packets exchanged between two vehicles without infrastructure support:

- Endpoints: vehicles.
- Destination range: single vehicle endpoint identified by location (GeoAnycast).
- Example use cases:
  - Traffic efficiency: Event-driven low-latency query from a vehicle to an unknown neighbour vehicle heading in the opposite direction to report about traffic congestion.

4.5.3 IPv6 Vehicle-based Multicast Scenarios (VM)

Scenario VM1: Packets transmitted from a vehicle to multiple vehicles without infrastructure support:

- Endpoints: vehicles.
- Destination range: multiple vehicle endpoints within a circle of specified radius around originator (GeoBroadcast).
- Example use cases:
  - Road safety: Event-driven low-latency broadcast to multiple vehicles located within a geographical area in order to reliably and quickly disseminate safety information such as reporting about black ice.
  - Road safety: Event-driven delay-tolerant IPv6 application-bound broadcast to multiple vehicles located within a geographical area piggy-backed over a sequence of beacons in order to reliably disseminate safety information by attaching it to scheduled network signalling.
  - IPv6 signalling: Periodic broadcast from a vehicle announcing the IP address range it can be reached at.

4.5.4 IPv6 Roadside-based Unicast Scenarios (RU)

Scenario RU1: Packets sent between the roadside and a vehicle at a specific location:

- Endpoints: roadside originator and vehicle destination or vice-versa.

- Destination range: single endpoint at specified geographic area or direction (GeoUnicast).
- Example use cases:
  - Road safety: event-driven low-latency packets sent from the roadside to a vehicle at a specific location and lane.
  - Traffic efficiency: vehicle requesting to the roadside an empty space in parking lot.

4.5.5 IPv6 Roadside-based Anycast Scenarios (RA)

Scenario RA1: Packet sent from a roadside to a vehicle within the roadside's service area:

- Endpoints: roadside originator and vehicle destination.
- Destination range: single endpoint (GeoAnycast).
- Example use cases:
  - A RSU wants to get road traffic status information about a designated area (icy road, traffic jam). This RSU sends out a INFO_Request in Anycast mode to reach any vehicle able to report road conditions within the designated area. Only one vehicle replies back to the RSU with some information.

4.5.6 IPv6 Roadside-based Multicast Scenarios (RM)

Scenario RM1: Delivery from the roadside to the vehicles within the roadside's service area:

- Endpoints: roadside originator and vehicle destinations.
- Destination range: specified geographic area (GeoBroadcast).
- Example use cases:
  - IPv6 signalling: IPv6 router advertisement and router solicitation sent between the vehicles and the roadside.
  - Road safety: Dynamic speed limit notification from the roadside to all vehicles.

- Delivery of information to a vehicle at an unknown position (position request query flooding when the IPv6 access router has a message to deliver to a vehicle in its service area, but the vehicle's position is not known or delivery acknowledgement has timed out, a position request query may be flooded within its service area. The target vehicle responds with its current position. This procedure may be restricted to messages above a certain priority class).

4.5.7 IPv6 Internet-based Unicast Scenarios (IU)

Scenario IU1: Bidirectional exchange between the vehicle and the Internet. Packets are first transmitted from the vehicle to the roadside and then from the roadside to the Internet, or vice versa:

- Endpoints: vehicle originator and Internet destination or vice versa.
- Destination range: single endpoints of known identity.
- Example use cases:
  - IPv6 signalling: IPv6 mobility management between vehicle and home agent.
  - IPv6 application: traffic hazard (black ice, ghost driver) reported from the vehicle to some well-known server in the Internet.

4.5.8 IPv6 Internet-based Multicast Scenarios (IM)

Scenario IM1: Periodic delivery from the Internet to multiple vehicles within a designated area, transmitted from an Internet source to the roadside and then GeoBroadcast to the service area of the roadside. Packets may be multi-hopped between the roadside and the vehicle:

- Endpoints: Internet originator and vehicle destinations.
- Destination range: multiple vehicle endpoints at specified geographic area (GeoBroadcast).
- Example use cases:
  - Road safety: Central server reporting about black ice to all vehicles in a geographic area.

5. GeoNet Architecture Design

In this section we present the design of the GeoNet architecture. It follows the design goals and scenarios needs as described in previous sections. We first explain the protocol layering inherited by the GeoNet architecture and then we detail each layer composing the GeoNet architecture. One important detail is the introduction of a vertical management layer. Then, since the concept of GeoNet is the combination of IPv6 over GeoNetworking capabilities provided by a sub network layer, the concept of IPv6 link is explained.

The building protocol blocks that meet the design goals are provided by existing protocols (specified by C2C-CC or SDOs such as IETF or ETSI), extensions to these existing protocols or newly defined protocols. Existing protocols known to provide a function needed for IPv6 GeoNetworking are explicitly mentioned whereas functions for which there is no known or efficient protocol are simply described. All these requirements are reported in a classical IETF style. Details of the specification and operation of the known or newly defined features are reported in [GeoNetD2.2]. Qualitative and quantitative requirements necessary to assess the fulfilment of the GeoNet architecture with these requirements will be provided in GeoNet deliverables [GeoNetD4.1], [GeoNetD5.1] and [GeoNetD7.1].

5.1 Protocol Layering and Scope of Architecture

The concept behind GeoNet is to combine IPv6 with GeoNetworking capabilities defined by the Car-to-Car Communication Consortium (C2C-CC). Here the term C2CNet refers to the network layer that performs geographical addressing and routing functions, and C2CNet transport layer is the transport layer located between non-IP applications and C2CNet.

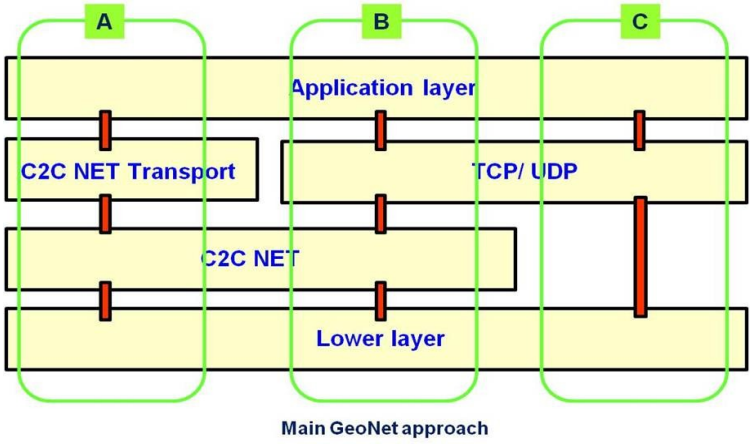

Figure 4: Protocol Layering and Approaches

Taking C2C-CC architecture design as in input to the GeoNet architecture, there can be three kinds of protocol layering as shown on Figure 4:

- In **approach A**, the application layer is over C2CNet transport, which is over C2CNet layer, which is over lower layers. There is no IP layer.

- In **approach B**, the application layer is over TCP/ IP, which is over C2CNet layer, which is over lower layers.

- In **approach C**, the application layer is over TCP/ IP, which is over lower layers. There is no C2CNet layer.

While all those approaches have their specific use cases, the GeoNet architecture focuses on approach B since the goal is to support communication scenarios requiring both IPv6 networking capabilities and GeoNetworking capabilities. So, the GeoNet architecture does not deal with any GeoNetworking function which is only required for non-IP applications (e.g. GeoNetworking transport).

As such, the GeoN**et architecture follow**s Approach B (IPv6 over C2CNet over ETSI ITS-G5/IEEE 802.11p [ETS-IES-202-663]) as illustrated on Figure 5, and more precisely:

- The application layer is over TCP/ IP and IPv6 is over the C2CNet layer.

- The C2CNet layer plays the role of the sub-IP layer for IPv6. From an IPv6 viewpoint, only the C2CNet layer is visible.

- The C2CNet identifier (C2CNet ID) plays the role of the sub-IP address defined in IPv6 (Neighbor Discovery) [RFC4861] for IPv6 address assignment.
  For the time bein**g, we assume C2CNet is** running over ETSI ITS-G5/IEEE 802.11p (including ITS-G5A and ITS-G5B)[1]. However this is for simplicity and in the future C2CNet can run over other wireless technologies. The GeoNet architecture design would not prevent the support of GeoNetworking capabilities over other media.

- The relationship between the C2CNet layer and ETSI ITS-G5/IEEE 802.11p is not under GeoNet's work scope. GeoNet adopts the specification developed by C2C-CC and/or ETSI.

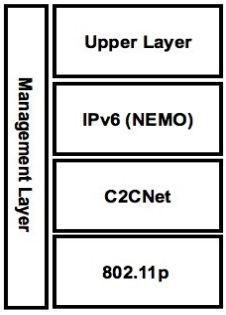

Figure 5: Protocol Stack for Approach B (on GeoNet OBU)

1 For the sake of simplicity in further text, when IEEE 11p is named, ETSI ITS-G5A / ITS-G5B as specified in [ETSI-ES-202-663] is always explicitly included in specification, since ETSI ITS-G5 is a profile of IEEE802.11.

5.2 IPv6 Architecture Components

The GeoNet architecture must take into consideration three subsystem components: the **vehicle**, the **roadside**, and the **Internet**.

It shall support **in-vehicle IP networks** (i.e. vehicles may embed a single or multiple IP subnets). As such, an architecture that would only support vehicles equipped with a single IP node is precluded. GeoNet is thus seeing vehicles as a network made of several communication nodes. A typical in-vehicle network comprises:

- An On-Board Unit (i.e. GeoNet OBU) functioning as an IPv6 mobile router (MR) in charge of communications with other vehicles, roadside units (GeoNet RSUs) and computers located in the Internet;
- A number of application units (AUs) such as a dedicated device for safety applications like hazard-warning, a navigation system with communication needs, a nomadic device such as a PDA that runs Internet applications, or infotainment devices. Such AUs are functioning as IPv6 nodes (MNNs).

Similarly, the roadside is a network made of several communication nodes. A typical roadside network comprises:

- A Road-Side Unit (i.e GeoNet RSU) functioning as an IPv6 access router (AR) in charge of forwarding data or providing access to GeoNet OBUs;
- A number of application units (AUs) such as a dedicated device for safety applications like hazard-warning, road signboards, etc. Such AUs are functioning as IPv6 nodes (CNs).

IPv6 nodes deployed in vehicle are referred to as **MNNs** (Mobile Network Nodes). From the point of view of MNNs, the nodes deployed in other vehicles, the infrastructure or the Internet and which MNNs are communicating with are referred to as **CNs** (Correspondent nodes). Within the scope of GeoNet, both are identical from a functionality viewpoint. Only differs the environment where they are located (mobile environment in the case of a vehicle subsystem, usually fixed environment in the case of the roadside or the central subsystem) and their role and the type of applications they are running.

In the context of IPv6 GeoNetworking where IPv6 and C2C-CC's GeoNetworking are combined into a single protocol stack, MR and AR with GeoNetworking capabilities are referred to as **GeoNet OBU** and **GeoNet RSU**, respectively. MNNs, CNs and other conventional IPv6 nodes acting as communication peers of IPv6 GeoNetworking flows must be able to process geocast packets and are referred to as **GeoNet-aware** nodes.

Both GeoNet OBU and RSU are functioning as IPv6 routers. As such they have an egress interface and an ingress interface, as illustrated on Figure 6. The egress interface is used

for communicating with other GeoNet OBUs and RSUs. The ingress interface is used to communicate with the attached IPv6 nodes (respectively MNNs and CNs), if any.

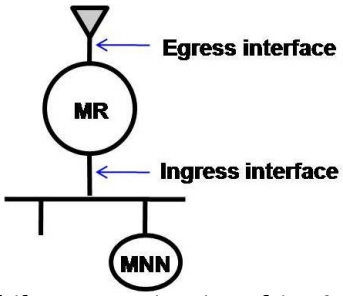

Figure 6: Mobile Router (MR) and its Attached MNNs

The GeoNet OBU / MR is in charge of ensuring that MNNs can communicate with CNs located in other vehicles, the roadside or the Internet. The GeoNet RSU / AR may provide Internet connectivity to GeoNet OBUs and their attached MNNs so that they could communicate with CN located in the Internet.

In conclusion, there are four types of IPv6 nodes acting as IPv6 GeoNetworking communication end-points, that is:

- **GeoNet OBU**: the IPv6 mobile router (MR);
- **GeoNet RSU**: the IPv6 access router (AR); and
- **GeoNet-aware nodes**: other IPv6 nodes enhanced with Pv6 GeoNetworking features and attached to either MR, AR or anywhere in the Internet.

Of course, the GeoNet architecture ensure backward compatibility and legacy IPv6 nodes not able to process IPv6 GeoNetworking flows can be located in the vehicle and the roadside. They may just not be able to process geocast-bound packets but can communicate with GeoNet OBUs, GeoNet RSUs and GeoNet-aware nodes by usual means.

5.3 Management Layer

Management-level functions are provided by a new layer, in a vertical plane. It contains all cross-layer functions, i.e. functions which role cannot be isolated from one layer to the other in situations where a decision has to be made at a particular layer based on parameters known by other layers.

Examples of such cross-layer functions include the ability for the application to take a decision based on the position (provided by the position sensor) or for the network layer to determine how to route or broadcast packets to vehicles in a target geographic area indicated by the application (in the current IPv6 design, there is no possibility to add

geographic information in the IPv6 header, so it has to be provided by other means, potentially involving multiple layers).

Such a vertical layer is not usual and differs from the well-known OSI layering design. However, similar vertical layer also appears in ITS communication architecture designed by COMeSafety [COMeSafety2008], ISO CALM [ISO-21217] and ETSI TC ITS [ETSI-TS-102-636-3]. It conforms to ITS needs, in of security management, interface management, and localisation management. Introducing such vertical management layer is thus in line with referenced standardisation effort. GeoNet views on the vertical place may differ from the design of standardised communication architectures. This is not an issue per se and will not disqualify the GeoNet architecture from interoperability with there architectures. The intend is to bring a new view from the perspective of the combination of IPv6 and GeoNetworking.

In particular, all cross-layer functions are contained in a single vertical management layer, contrary to the ETSI TC ITS [ETSI-TS-102-665] and ISO TC204 WG16 [ISO-21217] standardisation effort: we argue that there is no reasons to develop an independent vertical layer for each newly identified cross-layer function, as it is the case for any layer that provides various functions. We also argue that functions with different purposes are inter-related and need to exchange parameters with one another. Also; the definition of SAPs between different vertical layers would render the architecture design more complex.

Note that typical cross-layer functions such as matching outdoing interface to application preferences and user-specified policies are not considered in the GeoNet architecture: the reason is that it is not specific to GeoNet as the purpose of GeoNet is mostly to allow IPv6 over C2CNet and not to decide when this interface should be used. It will be the purpose of standardisation activities.

5.4 IP Layer

The GeoNet architecture must or may provide the following features at the IPv6 layer:

- **IPv6 basic networking** mechanims to acquire necessary IP parameters for communications such as IPv6 addressing, IPv6 forwarding and to enable IPv6 to run over different lower layer technologies, particularly C2CNet.

- **Internet access and mobility management**: In addition to be required for maintaining IPv6 global addressing and Internet connectivity for in-vehicle networks (the OBU and its attached nodes) as specified in standardised ITS architectures ISO CALM [ISO-21217] and ETSI TC ITS [ETSI-TS-102-665], Internet access is needed in all “Internet-based (IYi)” GeoNetworking scenarios indicated in Section 4. IPv6 global addressing, Internet reachability, session continuity and media-independent handovers (handover between different media) must be supported on the GeoNet OBU and must be compatible with IPv6 procedures defined in ETSI [ETSI- TS-102-636-3] and ISO CALM [ISO-21210] standardised ITS specifications.

- Both **IPv6 unicast** and **IPv6 multicast** communications are supported. In addition to the conventional use of multicast, IPv6 multicast is also needed in all “multicast range (XMi)” GeoNetworking scenarios indicated in Section 4. GeoNet extends the classical IP multicast scope to also consider a geographical area as an additional valid scope. By doing this, in addition to sending multicast packets aimed at being received by a set of receivers within the scopes defined in [RFC4291] (e.g., interface, link, site, global, etc.), IPv6 nodes can send multicast packets to a set of receivers within a well-defined geographical area. Note that this is very important, since vehicular applications do require the ability of addressing recipients on particular locations. The current IP addressing and routing architecture does not provide such a feature without any modification or extension. As for processing geocast packets, current multicast functions shall be used.

- **IPv6 security** is provided by legacy IPv6 security mechanisms such as IPsec [RFC2401], CGA [RFC4581] or SeND [RFC3971] and usually embedded within IPv6 networking protocols. Some of the issues specific to IPv6 GeoNetworking and requiring cooperation between layers are dealt within the Management Layer. Annex B of this present document provides a detailed security and privacy threat analysis.

- IPv6 nodes involved in IPv6 GeoNetworking may support other mechanisms to optimise the performance, for instance header compression at the IPv6 network layer (e.g. ROHC) [RFC3095]. However, this is out of scope of the GeoNet project.

- In order to ensure backward compatibility with legacy systems, features and protocols, the IPv6 layer shall allow transparent operation of legacy IPv6 applications running on top of IPv6 GeoNetworking, It should not break the proper operation of IPv6 network layer protocols, such as for instance security (e.g. IPsec), auto-configuration (e.g. stateless address configuration), multicast, or mobility management (e.g. nomadic devices attached to the vehicle and operating Mobile IPv6).

5.5 C2CNet Layer

C2CNet layer plays a crucial role in the GeoNet architecture as this is the layer in charge of the geographic addressing and forwarding functions, i.e. Forwarding an IPv6 packet from a source node to a destination node(s).

This layer supports addressing based on both individual node's identity and geographical position. It provides mechanisms for position-based forwarding.

The work performed within the C2C-CC [ETSI-TR-102-698] was considered as a starting point for the design of the C2CNet layer within GeoNet protocol stack. However, the common network header as specified by C2C-CC is defined for single-hop broadcast and

does not address multi-hop communications. The GeoNet project has thus extended the protocol stack designed by the C2C-CC to support multi-hop communications. As a result, the C2CNet layer as defined by the GeoNet project extends and complements its equivalent layer defined within the C2C-CC. At the time of writing of this document, ETSI TC ITS does not yet have a specification of the C2CNet layer.

The GeoNet architecture should provide the following functions at the C2CNet layer:

- **Status information exchange**: a mechanism to exchange status information (identity, position, speed, heading, time stamp and their accuracy).
- **Status information maintenance**: a database to maintain exchanged status information.
- **Signalling among communication nodes**: Two types of status signalling mechanisms are considered, explicit information exchange protocol (location service) and implicit one using periodical status packets (beaconing).
- Support of different **geographic areas**: Different shapes of areas and efficient coding are supported. The most comment shape is the circle.
- **Message buffering** used to buffer C2CNet packets when forwarding is not possible.
- **Congestion control:** should be used to optimise the C2CNet transmissions in order to minimise the network congestion.

5.5.1 C2CNet Layer Characteristics

The main characteristics of the C2CNet layer are the following:

- The C2CNet ID is an unique 64-bit identifier which identifies a vehicle. A vehicle may be provided with more than one C2CNet ID for privacy and security purposes.
- The C2CNet ID used in the C2CNet header belongs to the either i) a GeoNet OBU or GeoNet RSU in case the destination belongs to a vehicle or roadside and is thus directly reachable within the GeoNet domain or ii) a GeoNet RSU serving as an access router (AR) in case the destination is reachable in the Internet and thus not reachable within the GeoNet domain
- Depending on the georouting protocol used to forward data, the C2CNet packet's header includes in particular i) C2CNet ID of source and destination, ii) Geographic location of source and destination.
- C2CNet uses position-based forwarding mechanisms to deliver packets from a source to a destination.

5.5.2 C2CNet Forwarding Mechanism

Inside the C2CNet domain, a packet is forwarded with C2CNet specific forwarding mechanisms. With the information contained in the C2CNet header, a packet is forwarded with position based routing. The routing decision is based on geographic location of communication peers, source, destination & intermediary nodes.

The C2CNet forwarding mechanism does not rely on the information contained in the IPv6 header. Within the C2CNet domain, only the information contained in the C2CNet header is used (see Figure 7).

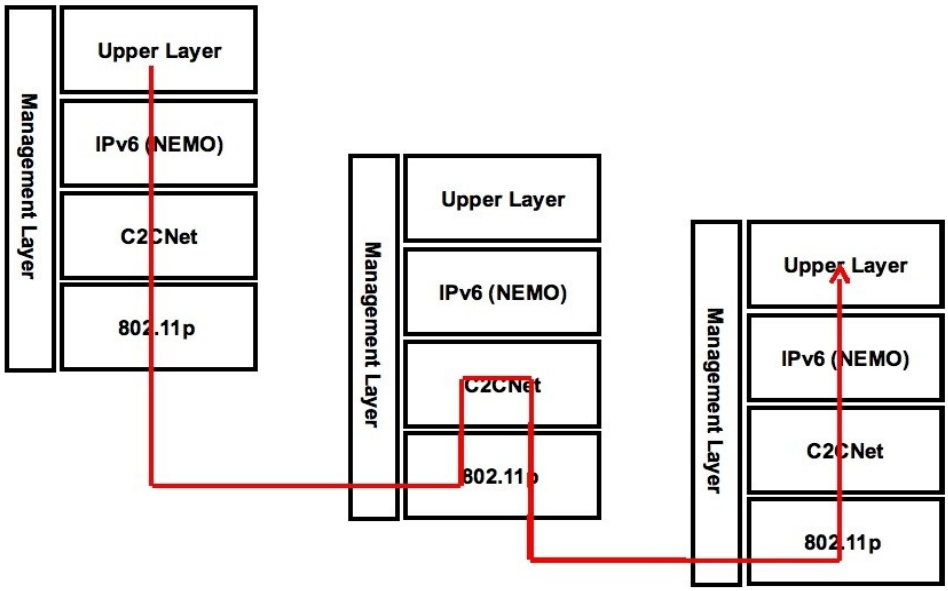

Figure 7: Packet Delivery Inside GeoNet Domain

5.5.3 Position-based Routing

Defining specific position-based routing mechanism is not in GeoNet's work scope. GeoNet is thus specifying very simple and basic forwarding algorithms, which are not necessary the most suitable for GeoNetworking. They are however sufficient to apply the integration of IPv6 and GeoNetworking. As such position-based routing as defined in GeoNet include the following:

- The C2CNet header contains i) C2CNet ID of source and maybe destination, ii) Geographic location of source and maybe destination.
- Each C2CNet node carries a location table which is updated by means of beaconing and location service.

- Each C2CNet node makes a forwarding decision based on the geographic location of its communication peers such as source, destination and (C2CNet) neighbours.

5.5.4 Relationship Between IPv6 and C2CNet Layers

In case of IPv6 unicast, the IPv6 layer must find out what is the IP next hop to which the packet shall be forwarded given an IPv6 destination address. The IPv6 layer must then sends down to the C2CNet layer i) the IPv6 packet itself, and ii) the C2CNet ID corresponding to the IP next hop or geographic area information in case of GeoBroadcast & GeoAnycast.

6. Functional Modules and SAPs

This section presents the functional modules and SAPs that must be considered in the GeoNet architecture by IPv6 nodes implementing GeoNet features. Functional modules are classified according to their layer position from an OSI-like viewpoint. Similar to architectures presented by COMeSafety [COMeSafety2008] and under standardisation at ETSI TC ITS [ETSI-TS-102-636-2] and ISO CALM [ISO-21217], we introduce management as a new layer, a vertical plane that includes all the cross-layer functions (typically, management of GeoDestination, position information and security and privacy that require cooperation between layers).

In the following subsections we first outline the functional architecture and we next detail modules and SAPs composing the GeoNet architecture. Then, we detail what functional modules shall be implemented for GeoNet OBUs, GeoNet RSUs and GeoNet-aware nodes. The detail specification of the functional modules is provided in [GeoNetD2.2].

6.1 Functional Modules Diagram

The functional GeoNet architecture is illustrated on Figure 8. Contrary to ISO, ETSI and COMeSafety, the GeoNet project focuses only on the networking capabilities and thus potentially needed functions at the transport layer and above (abbreviated as “UL” for “Upper Layers”) or at the data layer and below (abbreviated as “LL” for “Lower Layers”) are

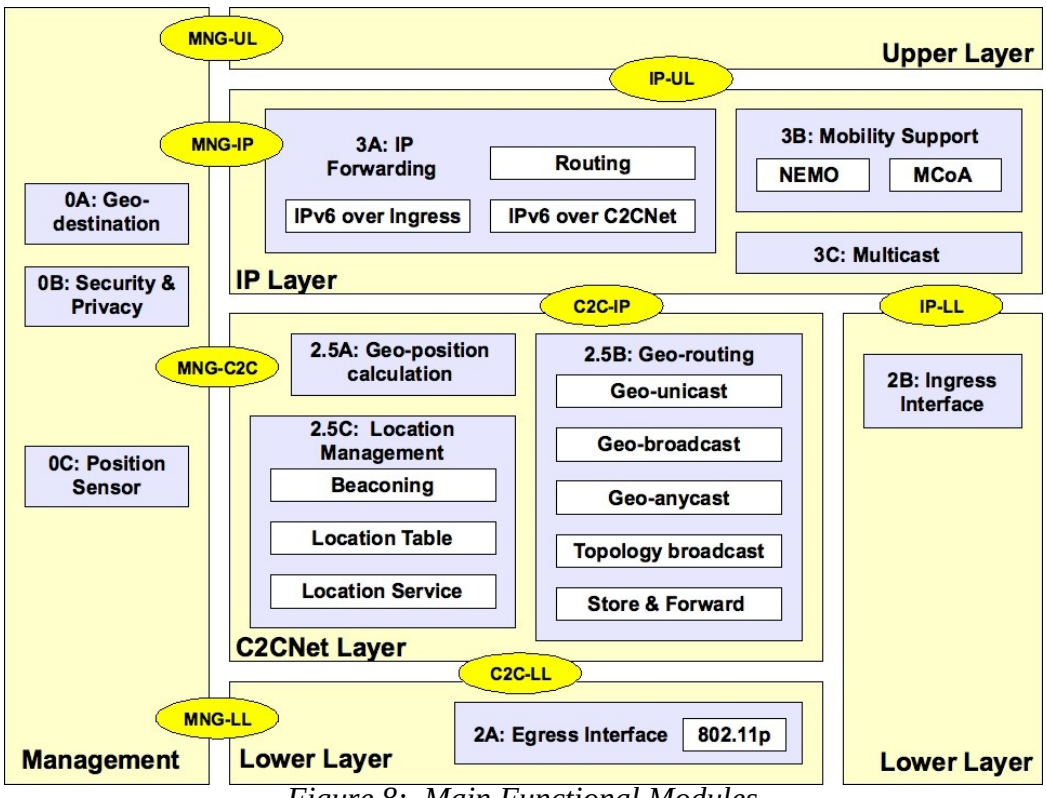

Figure 8: Main Functional Modules

not treated and thus not detailed in GeoNet deliverables. This is particularly the case for SAPs MNG-UL and IP-UL for which new functions or the adaptation of existing functions at other layers will be needed in order for applications to exploit new capabilities provided by IPv6 GeoNetworking.

The proposed functional architecture will further have to be extended in order to consider other functions not specifically related to IPv6 GeoNetworking but needed for operational deployment of IPv6 GeoNetworking, in particular Quality of Service (QoS) management (e.g. choice of the egress interface for outgoing packets at the GeoNet OBU) and security management (e.g. key exchange, access control, authorisation and accounting mechanisms). To build GeoNet OBU (MR), GeoNet RSU (AR) and GeoNet-aware (MNN & CN) IPv6 nodes, different functional modules must be implemented in combination with existing modules (such as IEEE 802.11p lower layer). For example, the NEMO module is implemented in MR but not in AR. Moreover the same module may behave differently in MR, AR or IPv6 nodes. For example, Module 3A “IP forwarding” performs router functions on MR but not on MNN.

6.2 Management Layer Modules

This layer is responsible for cross-layer management. Modules in this layer communicate with other layers through SAPs “MNG-C2C”, “MNG-IP”, “MNG-UL” and “MNG-LL”.

6.2.1 Module 0A: Geo-Destination

In order for IPv6 GeoNetworking to function, some information about the geographic area where the packets shall be transmitted to (GeoDestination) must be exchanged between the application layer and the C2CNet layer so that the application layer and the C2CNet layer share a common understanding.

One possible way is to encode the GeoDestination information directly in the packet. However it cannot be transmitted in the payload as it would violate the separation of layer principle, and currently there is no field in the IPv6 header nor optional header to carry this information besides using well-known multicast addressed mapped to dedicated areas. The mapping between a well-known multicast address and the target GeoDestination (in the form of latitude, longitude, radius, etc.) would thus be recorded in a table and accessed by both layers or encoded in the multicast address itself, but is still requiring a share of knowledge between layers.

From a conceptual viewpoint, this indicates a need for a cross-layer function and thus for a “Geo-Destination” module in the management layer. So, the mapping table would be implemented in this management layer and accessed by the application and the C2CNet layers through MNG-UL and MNG-C2C SAPs respectively. For some typically well-spread services, this information may be statistically configured, but for added value services, dynamic configuration will be needed. The means by which mapping between services

and GeoDestination would be advertised (service discovery, multicast group management fabric, etc.) mostly depends on the adopted solution for exchanging the GeoDestination information between the layers. The trade-off between the different solutions is discussed in [GeoNetD2.2] but at this stage it is too early to make a decision about the best solution. This will require further work.

6.2.2 Module 0B: Security & Privacy

Module “Security & Privacy” is in charge of tackling the security and privacy concerns that are specific to IPv6 GeoNetworking (see Annex B “Security & Privacy” of the present document for details). As such, this module is in charge of changing the C2CNet ID and the associated IPv6 address bound to this C2CNet ID so that the geographic location of the vehicle cannot be revealed from the IPv6 address carried in the IPv6 header.

The change of the C2CNet ID impacts both C2CNet and IP layers, so the decision algorithm in charge of changing the C2CNet ID is a cross-layer function and as such shall be implemented in the vertical management layer. The current C2CNet ID is accessed by the IP and the C2CNet layers through MNG-IP and MNG-C2C SAPs respectively.

Note that there are other security issues in GeoNet which are not managed by the cross-layer module: most security issues are indeed treated directly in independent modules. For example, security issues related to the global IPv6 address are addressed in Module 3A and security issues related to the NEMO tunnel in Module 3B.

6.2.3 Module 0C: Position Sensor

Module “Position Sensor” provides geographic information to GeoNet modules in the C2CNet Layer and Upper Layers through MNG-IP and MNG-UL SAPs respectively.

The routing mechanisms in GeoNet require information about the current geographical position. However the architecture avoids dependency from one of the well known positioning systems. There are several sources for position information. GPS may not be the best choice because of its limited grade of accuracy. The future Galileo system, odometer, gyrometer or accelerator sensors may add supplemental position information.

6.3 IP Layer Modules

This layer is responsible for IPv6 packet assembly and forwarding. Modules in this layer communicate with other layers through SAPs “C2C-IP”, “MNG-IP”, “IP-UL” and “IP-LL”.

6.3.1 Module 3A: IP Forwarding

Implemented in all IPv6 nodes, this module acquires necessary IP parameters for communications such as IPv6 addresses and prefix information. It performs common IPv6 functions such as IPv6 address configuration, IPv6 packet generation and packet forwarding and routing. It also enables IPv6 to run over different lower layer technologies, particularly C2CNet. Three sub-modules are defined:

1. **IPv6 over C2CNet:** Implemented in GeoNet nodes only, this sub-module enables IPv6 nodes to support GeoNetworking and is in charge of delivering efficiently a packet to its destination over the C2CNet link. It acquires necessary IP parameters such as IPv6 address and performs IP next hop determination and IP address resolution over the C2CNet link in order to communicate with nearby GeoNet OBUs and GeoNet RSUs. For privacy reasons, this sub-module also interact with module “0B: Security & Privacy” to dynamically change the C2CNet ID.

2. **IPv6 over ingress**: This sub-module enables IPv6 over the lower layer technology provided by an ingress interface and allows to attach other IPv6 nodes behind the GeoNet OBU or the GeoNet RSU. In the vehicle, this sub-module enables MNNs to be attached to the in-vehicle network served by the MR; on the roadside it allows to attach CNs to the roadside network served by the AR.

3. **Routing**: This sub-module is in charge of selecting the interface where incoming packets from an ingress or egress interface should be forwarded to. This decision is made according to routes recorded in the forwarding table and populated either statically or dynamically from instructions received from sub-modules 'IPv6 over C2CNet” and “IPv6 over ingress”, and from modules “3A: Mobility Support” and “3C: Multicast”.

Not all sub-modules are implemented in all IPv6 nodes; in addition sub-modules function differently on different IPv6 nodes (see Section 5.2 “IPv6 Architecture Components”).

In addition to these sub-modules, there may be other egress interfaces supported in the GeoNet RSU or GeoNet OBU, e.g. 2G/3G. Since this support is optional and irrelevant to IPv6 GeoNetworking, no sub-modules are presented on the diagrams nor are they specified in any GeoNet document.

6.3.2 Module 3B: Mobility Support

This module is needed for all Internet-based scenarios (IXi) indicated in Section 4 “Communication Scenarios”. Implemented in GeoNet OBU nodes only, it maintains Internet connectivity and provides session continuity to the GeoNet OBU nodes (MR) and in-vehicle IPv6 nodes (MNNs) attached to ingress interface of the GeoNet OBU. It contains two sub-modules:

1. **NEMO** (NEtwork MObility): Required for ubiquitous Internet connectivity, this sub-module is in charge of maintaining globally reachable IPv6 addresses for all nodes in the vehicle and to maintain Internet connectivity at the GeoNet OBU through the C2CNet egress interface when GeoNet RSUs or other nearby GeoNet OBUs are able to provide Internet access over the GeoNet domain.

2. **MCoA**: (Multiple Care-of Address Registration): Required for media-diversity, this sub-module is in charge of maintaining Internet access simultaneously through multiple egress interfaces while managing network mobility. Effective support of non-C2CNet egress interfaces and the selection criteria of the appropriate egress interface to be used for sending out a given packet is out of scope of the GeoNet project and is not detailed further (otherwise, we would have added a sub-module "IPv6 over non-C2CNet egress" in module "3A: IP Forwarding" and the routing sub-module would have be extended with functions for interface selection). This feature is nonetheless required for compatibility with standardised ITS architectures (ISO CALM [ISO-21217]) as the GeoNet OBU may be equipped with several egress interfaces, one of which being a C2CNet interface.

6.3.3 Module 3C: Multicast

Implemented in all IPv6 nodes, this module acquires group membership information, it determines if there are listeners on its interfaces for a given multicast group and feeds module "3A: IPv6 Forwarding" with the necessary information to update the routing table. GeoNet extends the classical IP multicast scope to also consider a geographical area as an additional valid scope. By doing this, in addition to sending multicast packets aimed at being received by a set of receivers within the scopes defined in [RFC4291] (e.g., interface, link, site, global, etc.), IPv6 nodes can send multicast packets to a set of receivers within a well-defined geographical area. Note that this is very important, since vehicular applications do require the ability of addressing recipients on particular locations. The current IP addressing and routing architecture does not provide such a feature without any modification or extension. As for processing geocast packets, current multicast functions shall be used.

6.4 C2CNet Layer Modules

This layer is responsible for GeoNetworking. Modules in this layer communicate with other layers through SAPs "C2C-IP", "MNG-C2C" and "C2C-LL".

6.4.1 Module 2.5A: Geo-position Calculation

Implemented in all GeoNet OBUs and RSUs, this module is responsible for calculating the position information to be used for GeoNetworking. This modules is also responsible for geographical relevance check.

6.4.2 Module 2.5B: Geo-routing

Implemented in all GeoNet OBUs and RSUs, this module is in charge of forwarding packets from a source to a destination based on geographical information such as position or velocity. It is composed of following sub-modules:

1. **GeoUnicast:** This sub-module delivers a packet to a given node in a certain geographic location.

2. **GeoBroadcast:** This sub-module delivers a packet to all nodes within a certain geographic area.

3. **GeoAnycast:** This sub-module delivers a packet to at least one node (any node) within a certain geographic area.

4. **TopoBroadcast:** This sub-module delivers a packet to all nodes located up to a certain distance in terms of hops.

5. **Store and forward:** This sub-module stores the packet locally for a defined period of time when the forwarding of the packet is not possible. A buffered packet is extracted from the buffer when conditions for forwarding are met.

Geo-routing resolves the C2CNet neighbour(s) for a given destination based on geographic location of communication peers. It performs the following functions:

1. **C2CNet packet generation**: a C2CNet packet is generated when receiving an IPv6 packet from the IP layer together with the C2CNet ID of the IP next hop,

2. **C2CNet next forwarder determination**: Given a C2CNet packet to send, coming from either i) egress interface or ii) IP layer, this function selects among the C2CNet neighbours the one which will take care of forwarding the packet toward the destination. This selection is done based on the geographic location of communication peers (source, forwarder and destination locations).

3. **Store and forward**: In case there is no C2CNet next forwarder available, it stores the packet locally and forwards it later when a conditions are met.

6.4.3 Module 2.5C: Location Management

Implemented in all GeoNet OBUs and RSUs, this module manages location information among communication peers. It is composed of following sub-modules:

1. **Beaconing**: This sub-module exchanges the location information such as geographic position or velocity among communication peers, especially C2CNet neighbours, with beaconing messages.

2. **Location table**: This sub-module is used to record locally the location information of neighbours and other potential destination nodes.

3. **Location service**: This sub-module resolves the geographic location of a communication peer when location table has no valid entry for it.

6.5 Upper Layer Modules

This is an upper layer for IPv6 including the application layer. Applications must be GeoNet-aware in order to exploit the GeoNetworking capabilities; some information about the geographic area where the packets shall be transmitted to (GeoDestination) must be exchanged between the application layer and the C2CNet layer. For this purpose, the GeoNet-aware applications may interact with module “0A: Geo-destination” via SAP MNG-UL.

Furthermore, there are generic upper layer processing tasks, which must be applied to received data through the IP-UL SAP. For the purpose of performing these common processing tasks, Application Layer Support libraries should be provided to GeoNet-aware applications. The following are examples of such tasks:

- Receiver side message filtering, for example to distinguish vehicles driving into an intersection – i.e. towards destination coordinate – from vehicles driving out of it;

- Information aggregation for combining GeoBroadcast with same information content – i.e. same type of sensor information – originating from different sources

The definition of the application primitives is specific to each application and is out of scope of the GeoNet project.

6.6 Lower Layer Modules

The Lower Layer modules provide a platform independent interface to the PHY/MAC or LLC layer. In that way the implementation of GeoNet modules is independent of the used medium or interfaces. The Lower layer modules are platform specific, therefore they must be implemented for each platform the GeoNet protocol stack shall be ported to.

6.6.1 Module 2A: Egress Interface

Implemented in all GeoNet OBUs and RSUs this lower layer specifies the physical network interface for communicating with other GeoNet OBUs and RSUs. Only ETSI ITS G5 and IEEE 802.11p are considered in the scope of the GeoNet project, but other media could be supported likewise.

The GeoNet protocol stack should work on different platforms with ETSI ITS-G5 and IEEE 802.11p compliant hardware devices provided by different vendors. Additionally there is a high likelihood that different ITS protocol stacks and operating systems are used on these platforms. Well defined interfaces are thus needed in order to render the implementation of the algorithms independent in two ways: Hardware platform independent and independent from the ITS protocol stack.

ITS communication architectures in Europe and worldwide are under standardisation. Although there are significant effort to harmonise standards, differences are expected due to national regulations especially on PHY/MAC OSI layers. The Module 2A “Egress Interface” allows easy adaptation of the GeoNet protocol stack with respect to both different platforms and evolution of the international standards. Within the GeoNet protocol stack there is no need to take care of special packet formats. The development can instead concentrate on highly efficient algorithms and high performance implementation.

Module 2A “Egress Interface” unifies the access to the GeoNet protocol stack. This adaptation allows the use of diverse Logical Link Control mechanisms with the same GeoNet implementation. The SAP for the unified access is referred to as 'C2C-LL' SAP.

6.6.2 Module 2B: Ingress Interface

This lower layer specifies the physical network interface linking to other nodes on the same subnet. For well-known ingress interfaces such as Ethernet, existing specification can be used without modification. No further specification is required, and standard behaviour is expected. Any technology such as Ethernet or IEEE 802.11 and State-of-the-Art LLC implementations can be used. The specification of this module is thus out of scope of the GeoNet project. This module communicate with the IP layer through SAP IP-LL.

6.7 Service Access Points (SAPs)

This section outlines the functions to be performed by SAPs (Service Access Point) between layers. SAPs are named after two keywords designating the two layers involved. UL and LL stands for Upper Layer and Lower Layer respectively. The exact LL and UL layers are not indicated precisely because the GeoNet project is only working on the networking capabilities. These SAPs are just indicated, but not further detailed.

6.7.1 SAP IP-UL between IP Layer and Upper Layer

This SAP provides two functions:

- a function for module “3A: IP Forwarding” to receive all the parameters needed to construct an IPv6 packet header given a payload. In particular, it should instruct module 3A to construct an IPv6 unicast, IPv6 multicast or IPv6 anycast packet.

- a function for module “3A IP Forwarding” to transmit up into upper layers a payload and possibly IPv6 destination and source address.

6.7.2 SAP C2C-IP between IP Layer and C2CNet Layer

This SAP provides:

- a function for module “3A: IP Forwarding” (i.e. sub-module “IPv6 over C2CNet”) to transmit an IPv6 packet and all the parameters needed by module “2.5B: Geo-routing” to forward the IPv6 packet until its destination. In particular, it should transmit the C2CNet ID of the IP next hop. For IPv6 multicast packets, the IP layer must provide the C2CNet layer with the necessary GeoDestination information to GeoBroadcast the packet in a specific geographical area.

- a function for module “2.5B: Geo-routing” to deliver the payload (IPv6 packet) of a C2CNet packet up to module “3A: IP Forwarding” an IPv6 packet. (i.e. sub-module “IPv6 over C2CNet”).

6.7.3 SAP IP-LL between IP Layer and Lower Layer

This SAP provides two functions:

- a function for sub-module “IPv6 over Ingress” from module “3A IP Forwarding” to transmit a payload in the form of an IPv6 packet and all the parameters needed by module “2.B: Ingress Interface” to construct a packet. In particular it should transmit the MAC address of the IP next hop.

- a function allowing module “2B: Ingress Interface” to deliver a packet to module “3A IP Forwarding” (more precisely to sub-module “IPv6 over Ingress Interface”).

6.7.4 SAP C2C-LL between C2CNet Layer and Lower Layer

This SAP provides three functions:

- a function allowing module “2.5B Geo-routing” to deliver a C2CNet packet and all related control parameters needed by module “2.A: Egress Interface” to transmit the packet over the air.

- a function allowing module “2.5B Geo-routing” to transmit control parameters to module “2.A: Egress Interface” to configure the egress interface.

- a function allowing module “2A: Egress Interface” to deliver a C2CNet packet to module “2.5B Geo-routing”.

6.7.5 SAP MNG-IP between Management Layer and IP Layers

This SAP provides a function allowing module “3A: IP forwarding” to be informed by module “OB: Security & Privacy” about the newest C2CNet ID to be used for generating the newest IPv6 addresses in forthcoming communications.

6.7.6 SAP MNG-C2C between Management Layer and C2CNet Layer

This SAP provides three functions:

- a function allowing module “OB: Security & Privacy” in the Management Layer to transmit the newest C2CNet ID to be used by the C2CNet Layer in order to maintain privacy.
- a function allowing the C2CNet Layer to request module “0A: Geo-Destination” in the Management Layer to provide the geographical area bound to given a GeoDestination identifier.
- a function allowing the C2CNet layer to provide module "0A: Geo-Destination" in the Management Layer with information about neighbouring nodes. Receiving this information then allows the compilation and publication of location awareness information by this module.

6.7.7 SAP MNG-UL between Management Layer and Upper Layer(s)

Though the specification is out of scope of the GeoNet project, SAPs between the Management Layer and Transport and Application Layers might be necessary, particularly for GeoAware applications to determine to which geographical area a packet shall be transmitted or to receive neighbour location awareness information.

6.7.8 SAP MNG-LL between Management Layer and Lower Layer(s)

SAP between the Management Layer and Lower Layers is necessary but is out of scope of the GeoNet project. This SAP is used to initialise the IEEE 802.11p interface in startup phase and set default values for such parameters as channel (frequency), data rate and transmit power. The specification of this SAP is out of scope of GeoNet as it is mostly operating system and hardware provider specific.

6.8 GeoNet OBU: Enhanced IPv6 Mobile Router (MR)

This section presents the functional modules for the GeoNet OBU, i.e. the combination of the IPv6 functions of an IPv6 mobile router and the GeoNetworking functions of a C2CNet

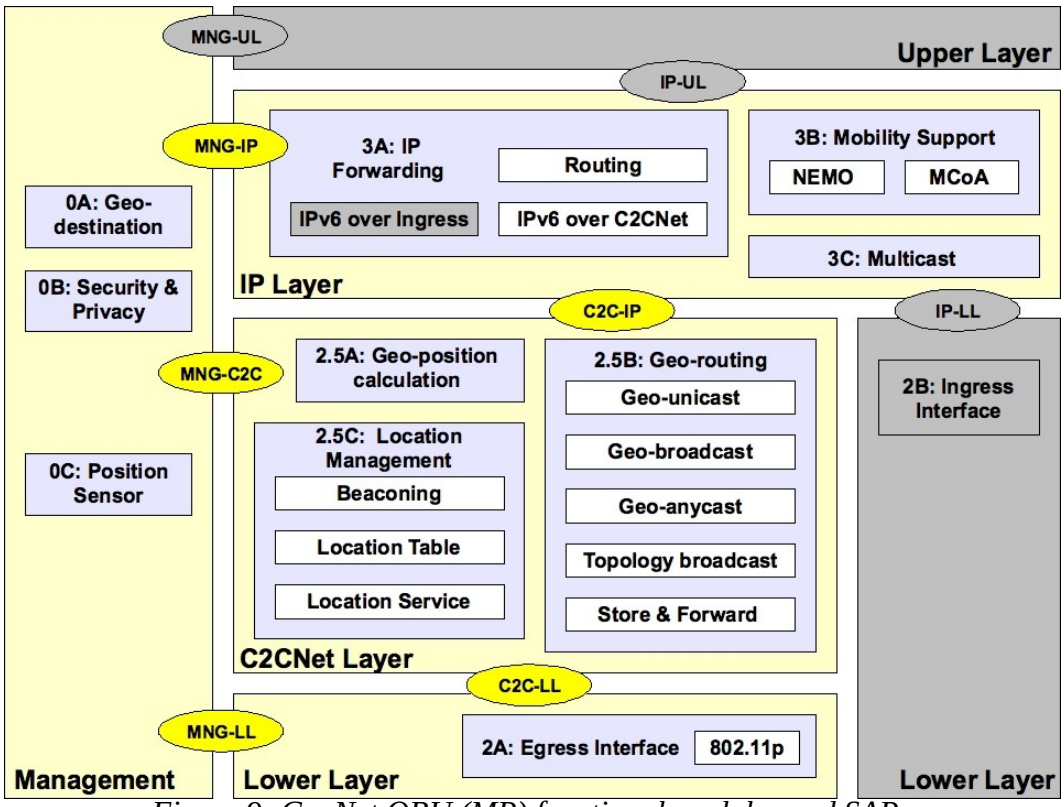

Figure 9: GeoNet OBU (MR) functional modules and SAPs

OBU. The relationship between modules is shown on Figure 9. Module and SAPs in grey (dark) are optional.

The GeoNet OBU shall implement all the C2CNet layer modules and all the management layer modules for GeoNetworking. At the IPv6 layer, it must implement all modules too, including the module “3B: Mobility Support” in order to maintain IPv6 sessions. The implementation of the sub-module “IPv6 over ingress” in module “3A: IP forwarding” and the module 2B “Ingress Interface” is necessary only when a physical interface (e.g. Ethernet) is present in order to attach MNNs. Implementation of the upper layer modules and SAPs is only necessary for GeoNet OBU / MR functioning as an IPv6 application communication end-point.

6.9 GeoNet RSU: Enhanced IPv6 Access Router (AR)

This section presents the functional modules for GeoNet RSU, i.e. the combination of the IPv6 functions of an IPv6 access router and the GeoNetworking functions of a C2CNet RSU. The relationship between modules is shown on Figure 10. Modules and SAPs in grey (dark) are optional.

The architecture of the GeoNet RSU is almost the same as in the case of a GeoNet OBU. At the C2CNet layer they look alike but they act differently at the IPv6 layer. An important difference is the lack of the module “3B Mobility Support”. A less visible but no less

important difference is that the AR does not behave like a MR on its IPv6 C2CNet egress interface where it has to behave as an access router serving GeoNet OBUs. The operation of IPv6 over C2CNet is thus different at the GeoNet OBU and GeoNet RSU.

The implementation of the sub-module “IPv6 over ingress” in module “3A: IP forwarding” and the module 2B “Ingress Interface” is necessary only when a physical interface (e.g. Ethernet) is present in order to attach other IPv6 nodes. Implementation of the upper layer modules and SAPs is only necessary for GeoNet RSU / AR functioning as an IPv6 application communication end-point.

The GeoNet RSU may provide access to the Internet. If that is the case, it has to announce this capability to the GeoNet OBUs. If so, it may comprises an additional interface (could be a wired or a 3G egress interface) unless another router on the link reachable via its ingress interface does.

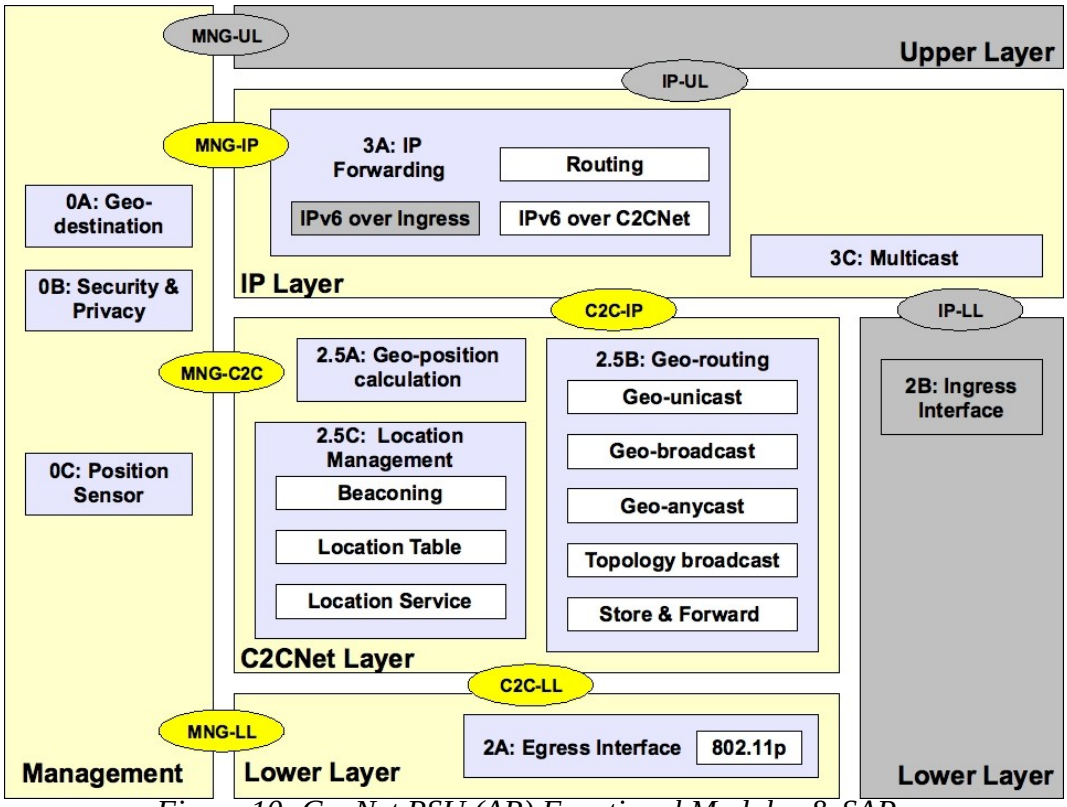

Figure 10: GeoNet RSU (AR) Functional Modules & SAPs

6.10 GeoNet-aware Nodes: Enhanced IPv6 Nodes

This section presents the functional modules for GeoNet-aware IPv6 nodes. It applies to all IPv6 nodes, either in the vehicle (MNNs), the roadside or in the Internet able to process (i.e. produce or consume) geocast IPv6 packets. The relationship between modules is shown on Figure 11.

The most important difference with GeoNet OBU and GeoNet RSU is that GeoNet-aware nodes do not implement C2CNet modules. At the IP layer, they do not implement module "3B: Mobility Support" (unless they are themselves mobile nodes, which is not linked with GeoNet capabilities and thus is omitted on the diagram). In the context of GeoNet, they are standard IPv6 nodes with multicast capabilities[2] and needs no special treatment. They may be slightly modified in order to be able to run geocast applications (i.e. they become GeoAware). In particular, they may implement the Management Layer if specific GeoDestination treatment is required by the application. The difference between legacy IPv6 nodes and GeoNet-aware nodes is the implementation of this new Management layer.

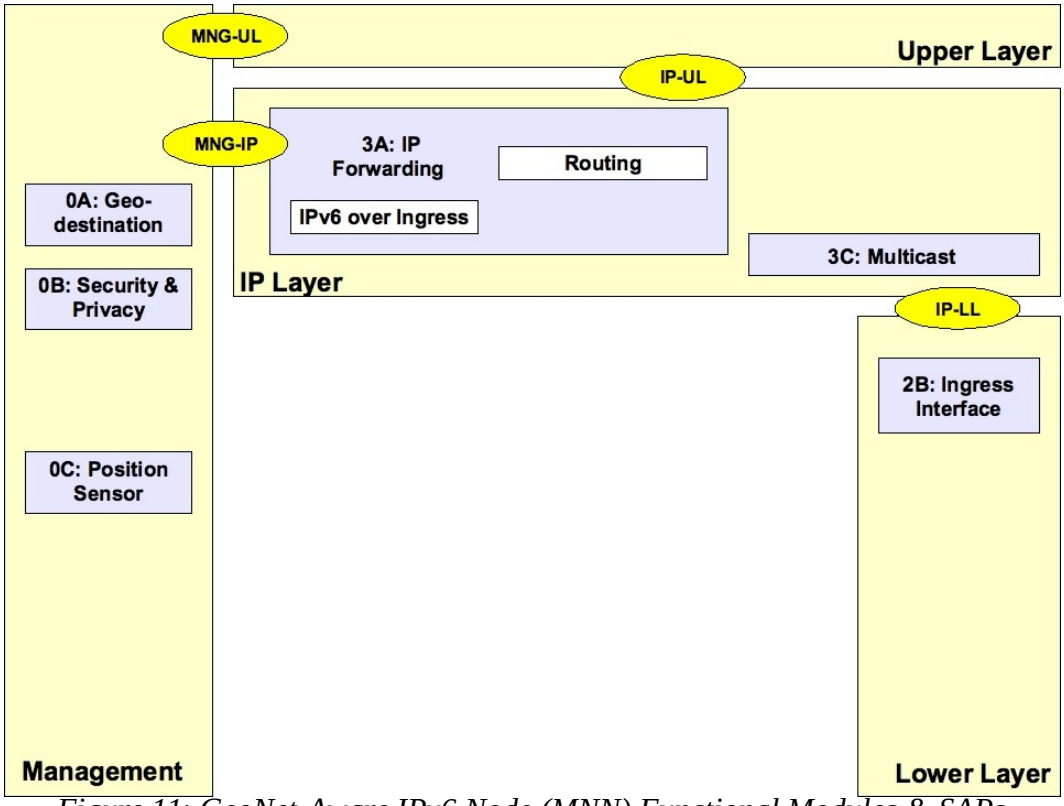

Figure 11: GeoNet-Aware IPv6 Node (MNN) Functional Modules & SAPs

2 All IPv6 nodes have multicast capabilities

7. GeoNet Domain & IPv6 Packet Delivery

In this section we define IPv6 end-to-end packet delivery over the C2CNet layer. We first define the notion of GeoNet domain, C2CNet link and in-vehicle IPv6 subnetwork. We then briefly sketch the IPv6 end-to-end packet delivery mechanism in the GeoNet domain, i.e. IPv6 over C2CNet over IEEE 802.11p environment.

7.1 In-vehicle IPv6 Subnetwork

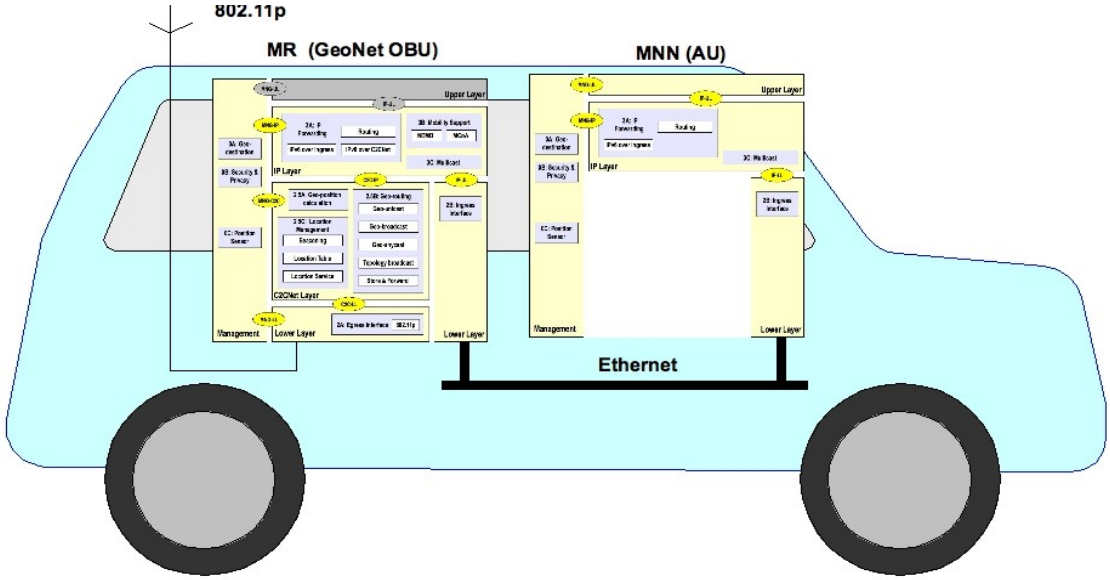

Figure 12: Example Implementation of IPv6 In-Vehicle Network With GeoNetworking Capabilities

Figure 12 provides an illustration of a particular implementation of the GeoNet architecture within a vehicle where the GeoNet OBU serves as a gateway to other IPv6 nodes attached to an in-vehicle Ethernet link. Details of the content of the MR and MNN boxes are illustrated in Section 6 in Figure 9 and Figure 11 respectively for the GeoNet OBU (MR) and GeoNet-aware nodes (MNN).

7.2 GeoNet Domain

Besides the definition of layers composing the IPv6 GeoNetworking architecture, another important element of the architecture is the definition of the wireless communication link for transmitting IPv6 packets between the vehicles (GeoNet OBUs) and the roadside (GeoNet RSUs).

Typically, GeoNet OBUs and RSUs are forming a particular case of vehicular ad-hoc network (VANET). From now on we will refer to this VANET as the **GeoNet domain** (see Annex D for terminology and Figure 13 for an illustration).

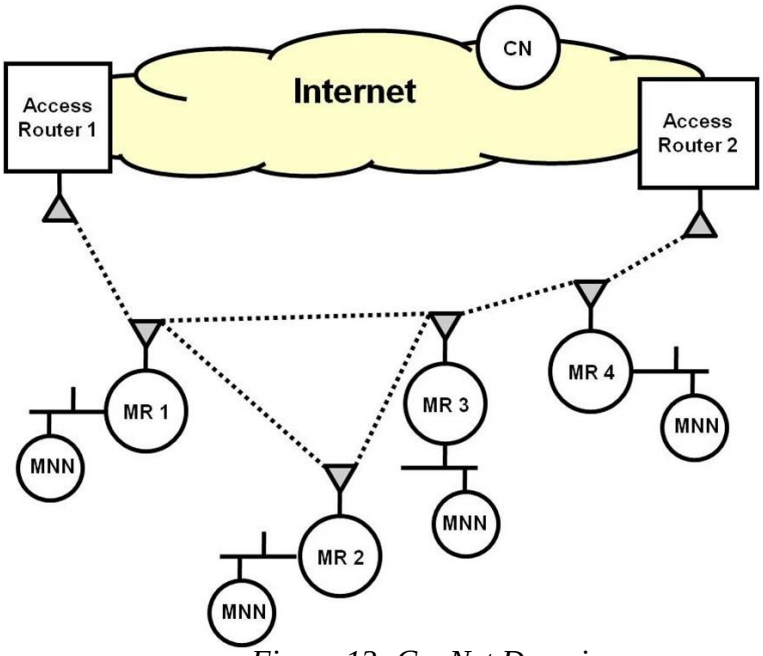

Figure 13: GeoNet Domain

7.3 IPv6 C2CNet Link

All GeoNet OBUs and GeoNet RSUs in the GeoNet domain form an IPv6 subnetwork and are reachable on a single IPv6 link, which we refer to as the **IPv6 C2CNet link**. GeoNet OBUs and RSUs attach to this IPv6 link through an egress interface referred to as the **C2CNet egress interface**. The nature of the actual physical interface, i.e. IEEE 802.11p is hidden from the IP layer. The IPv6 C2CNet link is indeed a virtual IPv6 link. It can be seen as a new type of broadcast media with embedded GeoNetworking and multi-hop capabilities provided by the C2CNet layer. It corresponds to a geographically-scoped area. Actual communication between two GeoNet OBUs on this link may thus occur over **multiple C2CNet OBUs** (see Annex D for terminology) at the layer below IPv6. As such, at the IPv6 layer of the GeoNet OBU, a GeoNet RSU appears to be directly reachable over the C2CNet link (i.e. under the wireless coverage area of a GeoNet RSU) although the packet is actually forwarded by a number of intermediate hops (other GeoNet OBUs, or even C2CNet OBUs not implementing an IPv6 stack). This is illustrated on Figure 14 showing the IP layer view of the C2CNet link. Details of the content of the different boxes entitled MR, AR and MNN are illustrated on Figure 9, Figure 10 and Figure 11 respectively for the GeoNet OBU (MR), GeoNet RSU (AR) and GeoNet-aware nodes (MNN).

IPv6 packets are encapsulated into C2CNet packets as they would into Ethernet packets on an IPv6 Ethernet link. This is illustrated on Figure 15 where two types of communication are illustrated:

- Communication between IPv6 nodes (MNN/AU) attached to two distinct GeoNet OBUs over multiple C2CNet OBUs forming the IPv6 C2CNet link;

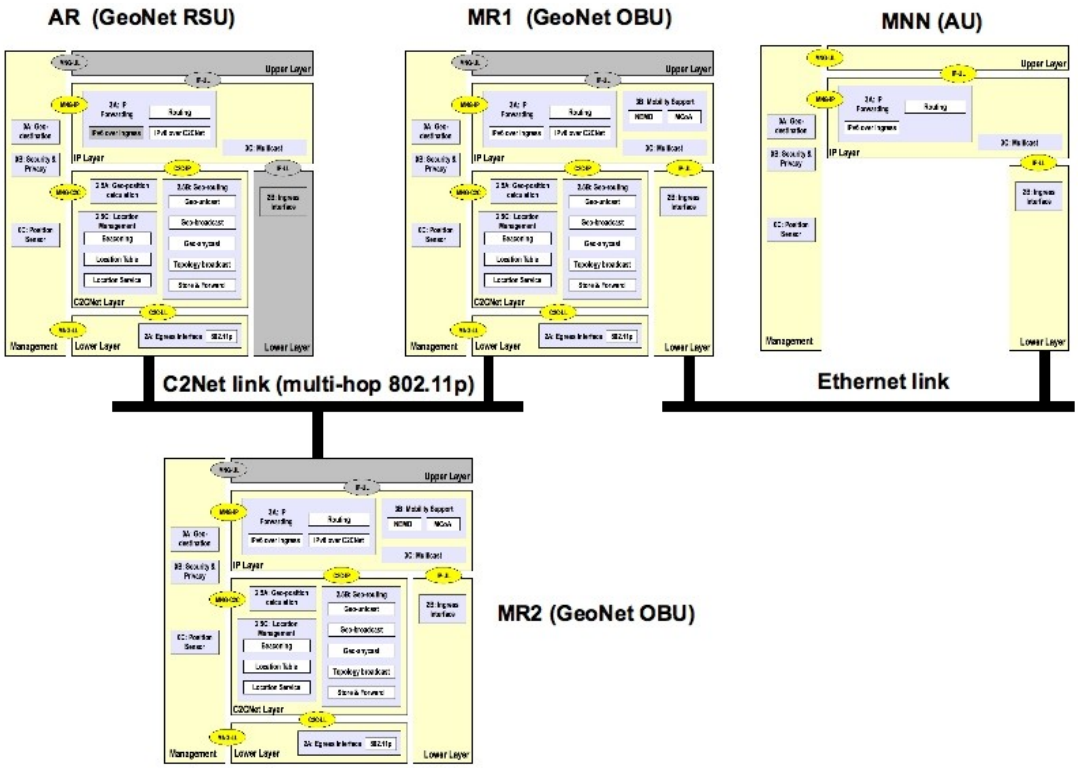

Figure 14: IP Layer View of the C2CNet Link

- Communication between an IPv6 node (MNN/AU) attached to a GeoNet OBU and an IPv6 node (CN) located within the Internet over multiple C2CNet OBUs forming the IPv6 C2CNet link attached to the Internet through a GeoNet RSU acting as an IPv6 access router.

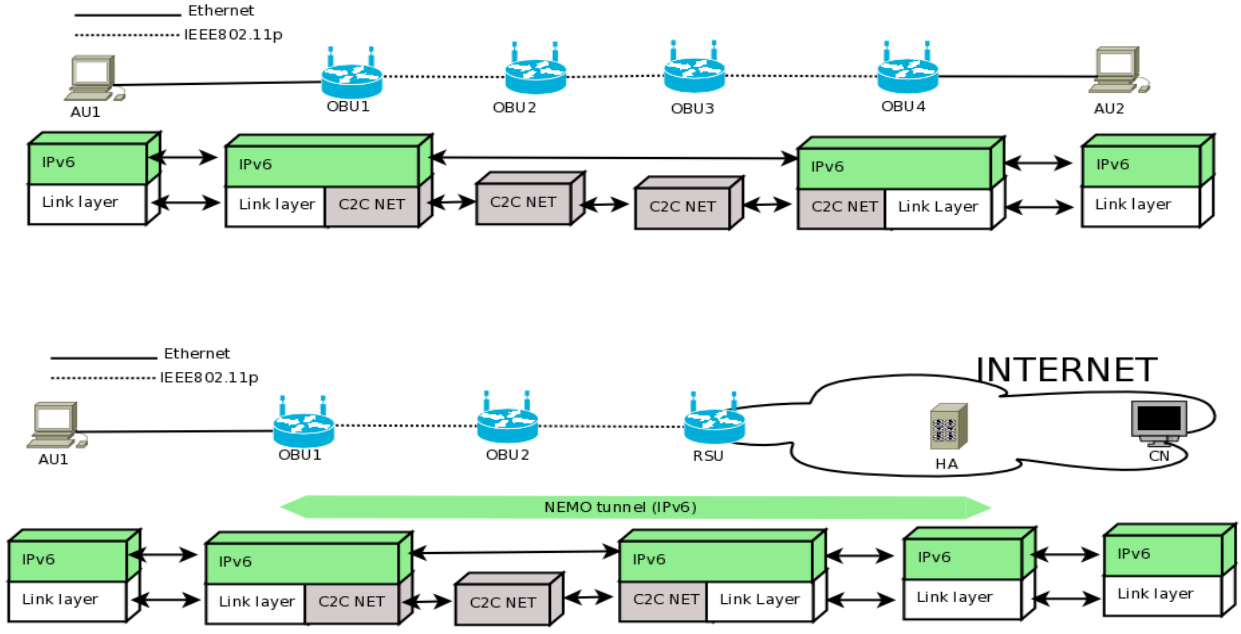

Figure 15: Vehicle-based and Internet-based Communications

The geographic boundary of the service area of GeoNet RSUs could be a maximum radius around the GeoNet RSU. The value of this radius must be fixed statistically or dynamically and could vary from GeoNet RSU to GeoNet RSU.

7.4 Entities involved in Packet Delivery

A packet is generated at the IP source node, enters the GeoNet domain at the C2CNet source, is then forwarded to the C2CNet neighbour, the IP next hop where it exits the GeoNet domain and finally the IP destination node, in that order. So, IPv6 end-to-end packet delivery involves five entities: 1) IP originator; 2) C2CNet source; 3) C2CNet neighbour; 4) IP next hop and; 5) IP destination. This is shown in Figure 16 which illustrates an Internet-based unicast scenario (IUi as defined in Section 4) where an IPv6 node in the vehicle is communicating with an IPv6 node in the Internet.

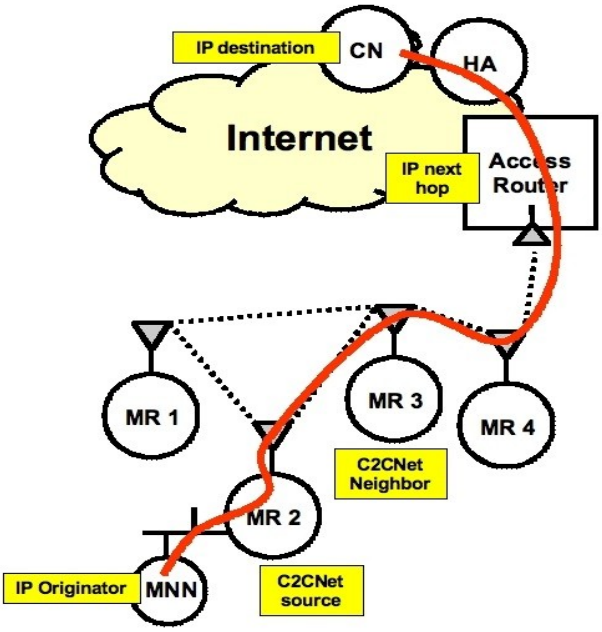

Figure 16: Entities Involved in IPv6 Packet Delivery

7.4.1 IP Originator

IPv6 originator can be a GeoNet node within the GeoNet domain (such as MR, AR), an IPv6 node attached to a GeoNet node (e.g. MNN) or an IPv6 node within the Internet infrastructure outside the GeoNet domain. The IPv6 originator runs an application and generates an IPv6 packet with a suitable IPv6 header.

7.4.2 C2CNet Source

The C2CNet source is the first GeoNet node implementing a C2CNet layer that the IPv6 packet generated by the IP originator passes through. It is either a MR (GeoNet OBU) or

an AR (GeoNet RSU). This is where the IPv6 packet generated from the IP originator enters the GeoNet domain. The C2CNet source adds C2CNet and IEEE 802.11p headers with suitable address and identifier.

7.4.3 C2CNet Neighbour

C2CNet neighbours are the nodes which can communicate directly with one another over the wireless link (IEEE 802.11p link in the context of the GeoNet project). Take notice that C2CNet neighbour is different from the neighbour on the IP C2CNet link.

Upon generating a C2CNet packet, the C2CNet source chooses a C2CNet neighbour and forwards the packet to the C2CNet neighbour in an IEEE 802.11p frame. The chosen C2CNet neighbour is designated by the destination MAC address in IEEE 802.11p frame.

7.4.4 IP Next Hop (C2CNet Destination)

IP next hop is the next hop from an IP viewpoint. It is the end node to which the packet is delivered by the C2CNet forwarding mechanism. The IP next hop is the destination from the C2CNet viewpoint. Take notice that the C2CNet neighbour is the next hop in IEEE 802.11p viewpoint.

If a destination is reachable through C2CNet forwarding mechanisms, the destination is the IP next hop. If not, an access router is the IP next hop.

IPv6 packets are encapsulated with a C2CNet header and the IP next hop is designated by the destination C2CNet identifier recorded in the C2CNet header. the packet reaches the IP next hop, all intermediary nodes only check the packet's C2CNet header and ignore its IP header. Only the IP next hop consults IP header to make a forwarding decision.

7.4.5 IP Destination

The IPv6 destination is the node to which IP packets are delivered and designated by the destination IPv6 address in the IPv6 header.

7.5 Packet Encapsulation

Application data is encapsulated in IPv6, C2CNet and IEEE 802.11p header in that order and each header designates a different entities (see Figure 17).

The IPv6 originator generates an IPv6 packet with destination IPv6 address. The C2CNet source encapsulates the packet with C2C header with IP next hop's C2C ID and encapsulates it once more with 802.11p header with C2CNet neighbour's IEEE 802.11p MAC address as shown on Figure 17.

Take notice that IEEE 802.11p header designates the C2CNet neighbour, C2CNet header the IP next hop and IPv6 header the final destination.

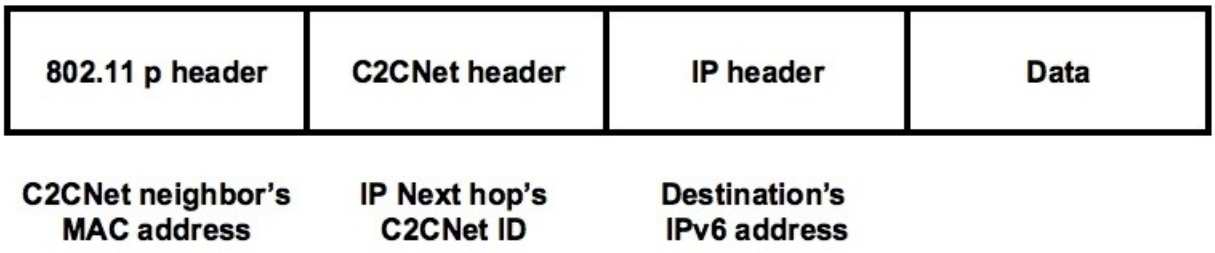

Figure 17: Packet Encapsulation

7.6 Main Tasks in Packet Delivery

For packet delivery over C2CNet, 5 operations are needed, i) IP next hop determination, ii) IP address resolution, iii) Geographic location resolution, iv) C2CNet neighbour determination and v) C2CNet address resolution.

This is a conceptual presentation and actual implementation may perform several operations at the same time.

IP next hop determination and IP address resolution can be combined into one operation, i.e. to find a C2CNet ID of the IP next hop from a given destination IPv6 address.

Also C2CNet neighbour determination and C2CNet address resolution can be combined into one operation, i.e. to find the IEEE 802.11p MAC address from a given (destination) C2CNet ID and its geographic location.

7.6.1 IP Next Hop Determination

This operation is to find IP next hop's IP address from a given destination IPv6 address. It is performed at the C2CNet source, at the IP layer.

The operations is closely related with on-link determination, i.e. determine whether a destination is directly reachable through C2CNet forwarding mechanism or not. If a destination is on-link, its IP next hop is the destination itself. If a destination is off-link, its IP next hop is an AR.

7.6.2 IP Address Resolution

The operation is to find a given node's C2CNet ID from its IPv6 address. It is performed at the C2CNet source, at the IP layer.

7.6.3 Geographic Location Resolution

The operation is to find a given node's geographic location from its C2CNet ID. It is performed at the C2CNet layer.

7.6.4 C2CNet Neighbour Determination

The operation is to find a C2CNet ID of a C2CNet neighbour to forward a packet from a given (destination) C2CNet ID and its geographic location. It is a GeoNetworking operation performed at all intermediary nodes, at the C2CNet layer.

7.6.5 C2CNet Address Resolution

The operation is to find a given node's IEEE 802.11p MAC address from its C2CNet ID. It is performed at all intermediary nodes. It concerns the relation between IEEE 802.11p and C2CNet layer.

7.7 GeoNet Packet Forwarding Example

In this section, we present how an IPv6 packet is delivered in the GeoNet domain. A packet is generated from originator, enters the GeoNet domain at the C2CNet source, is then forwarded to the C2CNet neighbour, IP next hop and finally destination in that order.

For example, in Figure 16 a packet is originated at MNN and delivered to a corresponding node (CN) across an access router (AR). Here MNN is the IPv6 originator, MR2 the C2CNet source, MR3 the next C2CNet neighbour, access router (AR) the IP next hop and the CN the final IPv6 destination. Note that since Internet connectivity is maintain by NEMO, the packets would first have to transit via the IPv6 Home Agent (HA) before reaching the CN. For simplicity, this is not detailed.

Step 1 : Procedures at the IPv6 originator, MNN

- First MNN runs an application and generates an IPv6 packet with the destination IPv6 address of CN.
- The IPv6 packet is delivered to MR2 through IP forwarding mechanism.

Step 2: Procedures at the C2CNet source, MR2

- MR2 receives the IPv6 packet from MNN.
- From the destination IPv6 address of CN, MR2 i) finds out that the AR is the IP next hop and ii) gets AR's C2CNet ID though IP next hop determination.
- From the C2CNet ID of the AR (IP next hop), MR2 resolves its geographic location.

- With the IP next hop's C2CNet ID and its geographic location, MR2 finds i) a suitable C2CNet neighbour to forward the packet, i.e. MR3, and ii) its C2CNet ID through C2CNet neighbour determination (it mostly perform position-based routing.)
- From C2CNet ID of MR3, MR2 finds MR3's IEEE 802.11p MAC address through C2CNet address resolution (the information is mostly obtained from beaconing).
- MR2 encapsulates the IPv6 packet having the IPv6 destination address of CN within C2CNet header having the C2CNet ID of AR as destination and C2CNet ID of MR2 as source.
- MR2 encapsulate this C2CNet packet once more within IEEE 802.11p header having IEEE 802.11p MAC address of MR3 as destination.
- MR2 sends the packet within IEEE 802.11p frame to MR3.

Step 3: Procedures at the C2CNet neighbour, MR3

- MR3 accepts IEEE 802.11p frame because the frame has MR3's IEEE 802.11p MAC address as destination.
- MR3 decapsulates the IEEE 802.11p frame and finds a C2CNet packet inside.
- Because C2CNet header has AR's C2CNet ID as destination, MR3 decides that the packet is not for itself and should be forwarded further.
- From the C2CNet ID of the AR (IP next hop), MR3 finds i) a suitable C2CNet neighbour to forward the packet, i.e. MR4 ii) its C2CNet ID through C2CNet neighbour determination and iii) its IEEE 802.11p MAC address through C2CNet address resolution.
- MR3 re-encapsulate the C2CNet packet once more within IEEE 802.11p header having IEEE 802.11p MAC address of MR4 as destination.
- MR3 sends the packet within IEEE 802.11p frame to MR4.

Step 4: Procedures at an intermediary node, MR4

- Procedures at MR4 is exactly same as the ones in MR3.
- MR4 decapsulates the IEEE 802.11p frame and finds a C2CNet packet inside.
- Because C2CNet header has AR's C2CNet ID as destination, MR4 decides that the packet is not for itself and should be forwarded further.

- From the C2CNet ID of the AR (IP next hop), MR4 finds i) a suitable C2CNet neighbour to forward the packet i.e. AR, ii) its C2CNet ID through C2CNet neighbour determination and iii) its IEEE 802.11p MAC address through C2CNet address resolution.

- MR4 re-encapsulate the C2CNet packet once more within IEEE 802.11p header having IEEE 802.11p MAC address of AR as destination.

- MR4 sends the packet within IEEE 802.11p frame to AR.

Step 5: Procedures at the IP next hop i.e. AR

- AR accepts IEEE 802.11p frame because the frame has AR's IEEE 802.11p MAC address as destination.

- AR decapsulates the IEEE 802.11p frame and finds a C2CNet packet inside.

- Because the C2CNet header has AR's C2CNet ID as destination, AR (precisely C2CNet layer of AR) determines that the packet is for itself.

- AR decapsulates C2CNet header and finds an IPv6 packet.

- Because the IPv6 header has CN's IPv6 address as destination, AR (precisely the IP layer of AR) determines that the packet is not for itself and should be forwarded further.

- AR uses standard IP forwarding mechanism to send the packet to CN.

Step 6: Procedures at the destination, CN

- CN receives the IPv6 packet.

- Because the IPv6 header has CN's IPv6 address as destination, CN determines that the packet is for itself.

- CN decapsulates the packet and sends it upward in the layers.

Annex A: Contributors

The following people have contributed to this GeoNet document, by alphabetical order:

Carlos J. Bernardos – IMDEA Networks

Maria Calderon – IMDEA Networks

JinHyeock Choi – INRIA

Thierry Ernst – INRIA

Yacine Khaled – INRIA

Andras Kovacs – Broadbit

Massimiliano Lenardi – Hitachi Europe

Wilfried Lohmann – Lesswire

Hamid Menouar – Hitachi Europe

Carsten Schulze – Lesswire

Wenhui Zhang – NEC

Annex B: Security & Privacy Threat Analysis

This annex provides an analysis of security and privacy of vehicular communications in the context of the GeoNet architecture. The goals of this annex are multi-folded:

1. **Generic V2X security and privacy threats:** the goal here is to provide an overview of the main security and privacy concerns of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications in vehicular networks, from a generic point of view (i.e. not assuming the GeoNet architecture). The work performed in related EU projects, such as [SeVeCOM] and [PRECIOSA] is taken as input.

2. **GeoNetworking security and privacy threats:** the purpose is to provide an overview of the main security and privacy concerns of vehicular communications in GeoNetworking architectures. Here, the goal is to analyse what are the issues caused by the use of geographical routing and addressing. Input from SeVeCOM and the Car-to-Car Communications Consortium (C2C-CC) [C2CCC] is considered.

3. **IPv6 and IPv6 mobility security concerns:** this part deals with the main security and privacy issues originated by the use of IPv6 and IPv6 mobility protocols in vehicular communication scenarios. This analysis is done from a pure IP viewpoint, i.e., no particular layer-2 technology nor any VANET architecture is assumed.

4. **GeoNet security and privacy:** this is the main outcome of this security work, in which the purpose is to identify, describe and analyse those specific security and privacy issues that are raised by the combination of IPv6 and GeoNetworking protocols (the key aim of the GeoNet project). This is the main goal of Task 1.5, since these are the issues that are specific to the GeoNet architecture and scenarios, and therefore special attention should be paid to them. This work is of utmost importance to the specification work, since the outcome of the security and privacy threat analysis is a set of security requirements that should be met by the solutions designed within GeoNet. Additionally, once the solutions' design is completed, the security of the proposed mechanisms should be analysed as part of the specification work itself. This would result in a security compliance check and the identification of potential open issues left open for future work.

We next devote one section for each of the previously described goals. Note again that the final goal of this analysis is to identify security and privacy issues specific to the GeoNet architecture, while providing a broad overview of other security concerns affecting the GeoNet architecture. These issues not specific to the GeoNet architecture should be addressed by more generic solutions.

B.1 Generic V2X Security and Privacy Threats

This section summarises those security and privacy issues that are general to any V2X (V2I and V2V) communication scenario and, therefore, of interest to GeoNet. V2X scenarios have some common characteristics that make security and privacy both very important and hard to tackle:

- *The communication medium is wireless and shared by multiple users*. There is no physical protection and isolation, thus facilitating multiple kind of attacks (e.g., eavesdropping, spoofing). Without proper care, a malicious user may get access to information, impersonate users/nodes (spoofing) and even modify data in transit. Additional security mechanisms need to be provided as a mean of privacy protection/isolation.

- *Communications might be multi-hop.* Information might need to transit through intermediate nodes – acting as forwarders – to reach its intended destination. Traversing multiple hops increases the complexity and makes the design of security solutions harder, since there are multiple potential points where security needs to be tackled. Besides, communication source and destination are not in direct reachability, what introduces some trust issues with the intermediate nodes.

- *Privacy is critical.* The nature of the vehicular scenario increases even more the importance of privacy in the communications, not in terms of data privacy, but also location privacy. Users making use of vehicular communication facilities do not want to be exposed to location tracking attacks [Papadimitratos2008, Ma2008].

- *Safety is one of the killer-applications*. Given that safety is considered to be one of the key applications of vehicular communications, the system must be invulnerable to on-purpose or accidental attacks, since human life would be at risk. Besides, vehicular communications may be used to control critical embedded devices – that might even autonomously control vehicles –, so its proper operation must be guaranteed.

From the above we can extract the main security requirements of any generic V2X communication scenario. First, it is needed to ensure **data integrity**, that is modification or injection of false information must be prevented. There are many mechanisms proposed to provide data integrity, such as the use of encryption, amongst others.

Second, **data** and **node authentication** is also needed. On the one hand, communication nodes should be sure about the identity of their peers. On the other hand, mechanisms that guaranteed that only authorised nodes can participate in the communications are also needed. Public Key Infrastructure (PKI)-based solutions might be used to provide data and node authentication.

Third, as we have already highlighted, **privacy** should be guaranteed, and in particular location tracking should be prevented. Here, the most accepted mechanism in the

research literature is the use of *pseudonyms*, which are anonymous, short-lived identifiers. The basic idea is to provide vehicles with multiple pseudonyms, so each vehicle alternates among them in time and space, therefore making more difficult location tracking attacks.

Fourth, **routing** must be **secure**. The creation and maintenance of the ad-hoc routes to locally exchange traffic between vehicles composing the GeoNet domain, is a critical issue from the security point of view. This task is performed by ad-hoc routing protocols, which still suffer from many vulnerabilities, mainly due to the unmanaged and non centralised nature of ad-hoc networks. Typical exploits against existing ad-hoc routing protocols may be classified into the following categories [Sanzgiri2005]:

- *Modification attacks.* A malicious node can cause redirection of data traffic or Denial-of-Service (DoS) attacks by introducing changes in routing control packets or by forwarding routing messages with falsified values.

- *Impersonation attacks*. A malicious node can spoof the identity of a legitimate node, and therefore steal its identity, and then perform this attack combined with a modification attack. The main problem of these attacks is that it is difficult to trace them back to the malicious node.

- *Fabrication attacks*. A malicious node can create and send false routing messages. This kind of attack can be difficult to detect, since is not easy to verify that a particular routing message is invalid, specially when it claims that a neighbour cannot be reached.

B.2 GeoNetworking Security and Privacy Threats

This section summarises those security and privacy issues that are exclusive of GeoNetworking-based V2X architectures, i.e. based on geographic routing and addressing. The GeoNet architecture builds on top of the C2C-CC protocol stack, and therefore these security considerations are also relevant to GeoNet.

GeoNetworking-based protocols enable different types of communications, such as GeoBrroadcast (broadcast/multicast over a particular geographic destination region), GeoUnicast (position-based unicast communication) and GeoAnycast (anycast over a particular geographic destination region). Besides, topological flooding (TopoBroadcast) based on the TTL (Time To Live) is also possible. A particular case of topological flooding is beaconing (flooding over 1 single hop), which is used intensively by geographical routing protocols (as well as by several safety applications).

Based on the above, several problems that need to be tackled can be identified [SeVeCOM]:

- *Secure beaconing*. Since these packets are not relayed, a reasonable level of security can be achieved by signing them. This provides sender authentication and

integrity protection. Moreover, beacons should carry a timestamp that prevents replaying them at a later time. Special attention should be paid in order to avoid wasting wireless channel bandwidth due to the use of very sophisticate and expensive cryptographic functions [IEEE1609.2].

- *Secure topological broadcast and geocast*. In this case, as opposed to the previous one, packets need to traverse several hops, so it is not sufficient to just sign the messages at the source (i.e. the sender), since there is information that is modified in transit (e.g., the TTL). For example, for TTL-based flooding, if the TTL field is not properly protected against unauthorised modification, a malicious node could increase the TTL causing more network load. Additionally, there may be certain applications that require the identity of the last forwarder node to be included in the packets.

- *Secure geographic routing*. Since these protocols are based on the position of the destination and the neighbours, the critical parts from the point of view of security are (in addition to guaranteeing the integrity and authenticity of routing messages): securing the beaconing, ensuring that claimed positions are accurate (see next) and securing the location service.

- *Falsified position claims*. Attackers may try to forge position information in the beacons. This is a hard to solve problem, that might be tackled by using plausibility checks.

- *Securing location service*. For GeoUnicast communications, a location service is expected to provide a binding between the identifier and the geographic position of the destination. Therefore, securing that binding is critical.

- *Privacy.* We have already mentioned the importance of privacy in vehicular communications. The use of GeoNetworking protocols, due to its intensive use of geographical information, exacerbates this problem.

B.3 IPv6 and IPv6 Mobility Security Concerns

This section summarises those security and privacy issues that appear because of the use of IPv6 and IPv6 mobility solutions in vehicular scenarios. Since GeoNet architecture is based on IPv6 these security considerations are also of interest to GeoNet.

Most of the problems described in Annex B.1 are applicable to the IPv6 layer. For example, it might be needed to provide data integrity at the IP level. Analogously, the solutions to tackle that are basically the same that were pointed out there. Following the same example, in order to provide data integrity, encryption features of IPsec [RFC2401] can be used.

There are also some security vulnerabilities in the IPv6 protocol. One of interest for vehicular communications is how to secure Neighbor Discovery [RFC4861]. Neighbour Discovery is used to perform many critical operations in IP, such as address resolution, movement and reachability detection, etc. The Internet Engineering Task Force (IETF) chartered a Working Group (WG) – called SEcure Neighbor Discovery (SeND) – to work on this [RFC3971, RFC4581].

IPv6 mobility mechanism introduce additional security issues. The hardest ones are those related to Route Optimisation (RO). In GeoNet, each vehicle deploys an in-vehicle network. The NEMO Basic Support (NEMO BS) protocol [RFC3963] is used to enable network mobility support. Nodes of the in-vehicle network configure their IPv6 addresses from an IPv6 prefix – called the Mobile Network Prefix (MNP) – that is topologically meaningful in a remote attachment point (the Home Network). The GeoNet OBU plays the role of the Mobile Router (MR), which is in charge of managing the mobility of the entire network. NEMO BS forces data packets to follow a sub-optimal route between the MR and the Home Agent (HA) serving the Home Network, even in case of local V2V communications. In order to overcome that problem, a NEMO Route Optimisation solution is needed [Baldessari2009]. So far, there is no standardised solution yet, but any potential NEMO RO mechanism should consider the security during the design phase. For example a V2V NEMO RO has to tackle the following type of attack:

- *Prefix ownership attacks*. Devices within a vehicle form a mobile network, sharing a prefix (the Mobile Network Prefix), which is managed by the Mobile Router of the vehicle. It is necessary to provide Mobile Routers with a mechanism that enables them to mutually verify that a Mobile Router actually manages the Mobile Network Prefix it claims to (i.e. it is authorised to forward/receive packets addressed from/to that MNP). Otherwise, a malicious node would be allowed to spoof (“steal”) a certain prefix and get all the traffic addressed to this prefix from other MRs connected to the ad-hoc network (GeoNet domain).

B.4 GeoNet Security and Privacy Requirements

This section focuses only on the security requirements posed by IPv6 communications using geocast capabilities (i.e. C2CNet). It should be noted that – as we have explained in the previous sections – there are a number of issues that are specific to the GeoNetworking layer (C2CNet). They are assumed to be solved at this particular layer, namely among others:

- Authentication of communication nodes;
- Integrity and confidentiality;
- Trustworthiness check of network header (e.g., plausibility checks of position and speed);

- Detection of misbehaving users (e.g., sending false data) and proper measures against them;

- Anonymity, that is, no information that could identify a node can be intercepted by other nodes.

As we stated above, we have identified some specific issues raised by the combination of IPv6 and C2CNet GeoNetworking (IPv6 GeoNetworking). These are the following:

- **Privacy:** By privacy two different concerns are widely understood: profiling (IP privacy) and tracking (location privacy). While the former (profiling) refers to revealing information that could be used to analyse and gather sensitive user data, the latter (tracking) is concerned with the problem of revealing roaming, which we define here as the process of a vehicle moving from one network to another with or without ongoing sessions. In GeoNet we exclusively focus on location privacy, since IP privacy is a general IP issue, non particular to IPv6 GeoNetworking. Since location privacy may be tackled at different layers, it might be possible that location privacy needs to be addressed at different levels of the protocol architecture. Therefore, how IPv6 and GeoNetworking are combined may impact on the privacy vulnerabilities.

- **Revealing geographic location from the IPv6 address used as communication identifiers:** The geographic position of a vehicle should not be inferred from the IPv6 address configured by the vehicle (OBU/AU). In particular, a communication peer located in the Internet (i.e. a Correspondent Node) should not be able to infer the location of a vehicle from the IPv6 address that is visible to this node.

- **Secure binding between the IPv6 address and the geocast (C2CNet) layer identifier:** This binding should be secured to prevent e.g., IP packets from being delivered to a wrong recipient and avoid redirection attacks. In particular, these problems would appear if a vehicle fails to obtain the legitimate C2CNet ID associated to a particular IPv6 address. For example, in case the binding between the IPv6 address and the C2CNet ID requires some signalling, special care needs to be taken in order to properly secure it, so a third malicious node cannot interfere in the process, injecting a wrong C2CNet ID, and therefore originating a redirection attack.

- **IPv6 address spoofing:** In non geocast networks, IP spoofing cannot easily be performed (ingress filtering techniques would prevent that) unless the attacker is on-path or is attached to the same link as the spoofed node. Besides, in a GeoNetworking-based vehicular network, the link concept is blurred and therefore a malicious node does not need to be within physical media coverage of the target node to perform this type of attack. So, this particular issue deserves special attention in the GeoNet architecture.

Annex C: Related Work

This annex presents related work performed on GeoNetworking and corresponds to Tasks 1.1, 1.2 and 1.3 of the GeoNet project, that is studying past work on IPv6 mobility and geographic routing and addressing performed on one side within ITS communities (i.e. applies to ITS communication architectures) and on the other side within the IETF community (not specifically designed to apply to ITS).

The availability of efficient location system receivers, numerous calculation techniques of the relative coordinates and the need to design an effective and a scalable network are the main reasons for geographical information usage in vehicular networks. The main challenge is to integrate the geographical location into the current design of addressing and routing.

Thus, several studies have dealt with geographical routing and addressing, both in infrastructure and infrastructure-less (ad-hoc) communication modes. In the infrastructure communication mode, the main contributions are on the matching of IP address and geographical information. Therefore, even routing mechanisms must be redefined by considering the geographical information, especially in the infrastructure-less mode.

C.1 Geographical Addressing

Although geographical information is still lacking in IP addressing, its usage is already studied, especially in cellular networks. According to previous works, the extension of IP addressing with geographical information could be achieved with three main approaches 1) in application-layer 2) purely IP extension 3) in sub-layer or network layer (e.g. C2CNet layer).

One of the main contributions, on geographical addressing, is [RFC 2009]. The authors identified three approaches to integrate geographic location into addressing mechanism, which relies on logical addressing as follows: 1) Application-layer solution using extended DNS (see also [RFC1712]), 2) GPS-Multicast and 3) Unicast IP routing extended to deal with GPS addresses.

The application-level approach extends DNS servers with a geographic information database. A new level domain is added – geo - for this purpose. The second and third levels represent respectively states and counties, and the last one represents polygons of geographic coordinates. Geographic address is resolved to a set of IP addresses of nodes covering the whole destination area. The packet is sent, by unicast fashion to all resolved IP addresses of the nodes or by multicast after all resolved nodes are asked to temporarily join a multicast group for this purpose. Nodes register their new location with the DNS server whenever they change their location. The DNS server would accordingly update the mapping for the node's IP address. While it appears to be a feasible approach, it is not clear how scalable such a solution would be. When numerous hosts move quickly, as in

ITS context, from one point to another, it would be daunting to update the location mapping for each of them.

With the GPS-Multicast approach, smallest addressable units have been introduced, called atoms. Each atom and partition (area with many atoms or partitions) is mapped to a multicast address, which is used for the first level of routing from the sender to the receiver. Each node joins all multicast groups for atoms and partitions that intersect its range. The sender determines the multicast address of the message destination and puts the original polygon specification into the packet content. The exact matching is done using the polygon specification in level two between node and the destination. However, this approach can represent a limited number of area and shapes.

The last approach is the integration of geographic addresses into routing decisions [Navas2001, Navas1997]. In this approach, three components are considered for geographic routing: GeoRouters, GeoNodes and GeoHosts. GeoRouters are in charge of transmitting a packet from a sender to a destination. They know their services area and exchange this information with other routers. Then, they are arranged in a hierarchy with small service areas in order to enhance efficiency. GeoNodes store incoming packets, with geographical information, during their lifetime and multicast, periodically, them to their cell. GeoHost is a daemon located on all hosts with capability to receive and send packets.

Routing works as follows: sending a packet involves the following three steps: 1) sending, 2) shuttling between routers, and 3) receiving. To send a packet, the GeoHost is queried in order to obtain the GeoNode IP address. Then, the packet is forwarded to the GeoNode, which forwards the packet to the local GeoRouter. The latter determines whether the destination polygon area and its own service area intersect with one another. If they areas intersect with one another, a copy of the packet is sent to the parent router. In case there is no intersection, the GeoRouter checks its child node's service area and sends a copy if they intersect with one another. After that, GeoRouters deliver a packet to the responsible GeoNodes. Finally, the GeoNodes deliver a packet to all users in the destination area. This second part of the routing between GeoNode and destination could be performed in the same way for all three approaches. It could be based either on application or on multicast filtering. With application filtering the GeoNode uses a multicast address to forward the packet, which additionally includes the GPS address. Matching is performed on the application layer. On the other hand, in multicast filtering, matching is performed on the IP layer. The GeoNode sends a list of all available packets, their geographic destination regions, and their assigned temporary multicast group addresses on a well-known multicast group address. Clients inside a destination area join the temporary multicast group on which the payload packet is later sent by the GeoNode.

Another way to extend IP addressing with geographical information, could be considered as purely geographic-based addressing, is introduced in [Vare2004]. They present location-based protocol between network nodes, named GPIPv6. Authors deal with two separate entities: source and destination. Source enables any IPv6 compliant network node to signal position information in parallel with other data, whether destination provides IPv6 compliant method. Notice that both option types can be used either in Destination options header or in Hop-by-Hop header. In the same way, [Hain2008] introduces a new

approach, not exactly related to GeoNetworking, to embed the position information into IPv6 address by defining a specific type of unicast address prefix. This, in purpose to facilitate scalable Internet routing when sites attach to multiple service providers. In conjunction with [RFC3306] a specific capability for Multicast groups, to target group members in a geographic region, could be defined by these unicast prefixes. They show also 44 bits can represent a geographic position within 6.4 m error bound.

[Choi2008, Baldessari2006, Baldessari2009] propose some architectures to enable IP communication in multi-hop communication in the ad hoc domain, i.e. in the GeoNet domain and over the C2CNet layer if we consider applicability to the GeoNet architecture. A C2C layer tailored for vehicular environments and relying on position-based routing, defines a separate C2C header with a separate C2C identifier. The C2C header is planned to carry the source C2C identifier, the destination C2C identifier, the source geographic location and the destination geographic location. C2C-CC also requires IPv6 support for its system to run such applications as infotainment [Baldessari2009]. For these reasons, [Baldessari2008] takes advantage of the availability of geographical information in the C2C layer and emulate a geographically defined Ethernet link within the C2C header. Packet forwarding is performed in the C2C layer and won't go up to IP layer. Also, [Baldessari2006] introduces a Mobile IPv6 Proxy to support network mobility that maintain the mobile node attached to the network from the ad hoc network characteristics. Instead of fragmenting the VANET in several links, authors introduce one, shared geographically-scoped link per RSU. [Choi2008] performs basic IPv6 protocols such as Neighbor Discovery and Stateless Address Auto-configuration. This solution enables IP configuration and IP packet delivery procedures without link-scope multicast. Vehicles can configure global IPv6 address and, with the address, communicate with peers on and off-VANET.

On the other context, geographical information privacy, the Geopriv working group [RFC3693] is focused on how geographic location could be both securely and privately provided for needed services. For this, [RFC4119, RFC3693] describe an object format for carrying geographical information on the Internet. This location object extends the Presence Information Data Format (PIDF), which was designed for communicating privacy-sensitive presence information and which has similar properties. This location object identifies and encapsulates pre-existing location information formats, and for regulating the location information distribution over the Internet by providing adequate security and policy controls.

C.2 Geographical Routing in Vehicular Ad-hoc Networks

In the previous section, we introduced the usage of geographical information for the addressing mechanism. However, in this section, we deal with routing and therefore present the well known location-based solutions for mobile networks and particularly for vehicular networks. Take notice that a standard solution in ad hoc networks and VANET is lacking.

Geographical-based routing protocols could be divided into two main families: Geocast protocols (e.g. LBM, GAMER [Maihöfer2004]) in which messages are sent to a defined geographical area, and those in which messages are sent to a single node (e.g. LAR, DREAM, GPSR [Mauve2001]).

Generally, the Geocast protocols use a directional broadcast to reach the destination area: messages are sent to nodes that are in the direction of the destination area. The geocast protocols address all the mobiles belonging to an area. To the contrary, the unicast protocols address a single node.

Geocast approach. LBM protocol [Maihöfer2004] avoids to flood the entire network by defining a forwarding area that includes at least the destination region and a path between the sender and the destination region. Outside the forwarding area, the packet is discarded. The forwarding area can also be defined by the coordinates of the sender, the destination region, and the distance of a node to the center of the destination region. GAMER protocol [Maihöfer2004] adapts dynamically the size of the forwarding area according to the current network environment.

Several studies were dealing with improvements or adaptation of geocast protocols for the VANET context. In [Maihöfer2003], upon receiving the geocast message inside the destination region, nodes start an election process. The elected node stores the message and delivers it periodically or on request. Several works were dealing with improvements or adaptation of geocast protocols for the VANET environment. In [Maihöfer2003], geocast solutions are adapted for the VANET context. The initial sender of a geocast message uses a geocast routing protocol to deliver the message for the first time. Inside the destination region, all nodes receive the geocast message and start the election process. The elected node stores the message and delivers it periodically or on request. In [Legner2002], the author uses the digital map and the mobility of vehicles to improve the geocast approach in VANET. In [Harshvardhan2006], a distance-based approach is used to define relay node and angle based-algorithm to determine implicit acknowledgement. The VTRADE protocol [Sun2000] uses the velocity vectors and last positions in order to classify neighbours vehicles in different groups and select the most appropriate one for the message retransmission. The UMB [Korkmaz2004] protocol adapts RTS/CTS mechanism to make a directional broadcasting. This mechanism is named RTB/CTB (Request To Broadcast/Clear To Broadcast).

The unicast protocols address a single node instead of all those belonging to an area [Mauve2001]. In the unicast approach, the position of the destination is known either from a location management service, or by flooding in the expected destination area. In case of a full-duplex communication, the receiver can inform the sender of its new position.

The unicast approach can be divided in two main families: greedy forwarding [Finn1987, Karp2000] and directional forwarding [Ko1998, Basagni1998]. In the greedy forwarding, a node selects the closest to the destination neighbour as the next hop. On the other hand, in the directional forwarding approach, the messages are sent to the nodes situated in the same direction to the destination. Among the most known protocols in both families, we can quote LAR [Ko1998] and DREAM [Basagni1998] for the directional forwarding family,

and GPSR [Karp2000] for the greedy forwarding approach. LAR [Ko1998] relies on a flooding for the route discovering (on-demand approach) while DREAM [Basagni1998] maintains a In GPSR protocol [Karp2000], some control messages are exchanged in the neighbourhood in order to define the retransmitter. In [Mo2006], MURU protocol is based on the path quality prediction. In [Lochert2003], the authors propose a GSR protocol, that combines geographical routing and digital map information to build an adapted knowledge of road environment. GSR needs to know the city topology as it is provided by digital street map. The same authors also propose in [Lochert2004] GPCR protocol, which appears as an enhancement of GPSR by using a digital map. A-STAR [Liu2004] considers a variability of vehicles density between roads by integrating traffic awareness and using rated maps statistically or dynamically. This awareness is performed in order to identify an anchor path with high connectivity for packet delivery. In [Mo2006, Granelli2006, Namboodiri2007, Naumov2007, Menouar2007], some adaptations of positions-based solutions are proposed. The authors take into account the position and the direction of movement of vehicles. Note also that CAR [Naumov2007] can be considered as an improvement of a location-based solution, by avoiding (or decreasing) the frequent destination discovery process. It works on the path connection maintenance between source and destination.

Take notice that the geographical information could be used in the broadcast mechanism. In broadcasting approach each node receiving a message retransmits it to the neighbouring nodes. This ensures that as many nodes as possible receive the message. Generally, upon receiving a message, each node makes a decision whether it will forward the packet or not. In some cases, neighbourhood parameters are needed, whose evaluation requires more control messages consuming more bandwidth when the dynamic increases.

In the probability-based broadcast algorithms [Alshaer2005], the decision relies on some random polling involving the neighbourhood. The retransmission decision could be relied on the node's positions [Alshaer2005, Benslimane2004]. Whenever a node retransmits a message, it adds its own location in the message. It then computes the additional coverage area it could cover itself by retransmitting the message. Similarly, in the direction-based broadcast algorithms, the broadcasting decision is improved by using the nodes trajectory or a digital map [Sun2000, Korkmaz2004].

Also, the broadcast decision can rely only on the cluster heads [Little2005]. The nodes can estimate the message utility to decide which message should be retransmitted first [Wischhof2005a, Wischhof2005b], in order to minimise the bandwidth consumption. The nodes can also take the broadcast decision without neighbourhood knowledge, with the so-called content-based routing [Ducourthial2007]. In this approach, the relays and receivers are selected by means of conditions including in the messages: only the nodes that fulfil the conditions will retransmit the messages or pass by the message to their application layer.

Another improvement in geographical-based routing is the store and forward mechanism, where the messages move forward to the destination by means of node's movements. Hence, a node may carry messages until it meets their destinations [Kosch2002, Allard2005]. The message propagation can rely on epidemic or random schemes

[Vahdat2000] or can rely on subgraphs of the entire network. Such a structure is similar to a backbone in fixed networks, but needs to evolve in dynamic networks. The evolutions of the structure can be controlled as in [Li2000] or [Chatzigiannakis2001] with the so-called support-based routing. Some optimisations can be performed when the context is known [Davis2001]. For instance, in [Zhao2006], the authors exploit the predictable vehicles mobility.

Annex D: Terminology & Acronyms

The terminology used in this document to define the GeoNet architecture is divided into three main families: GeoNet newly defined terms, IPv6 terms and generic networking terms.

D.1 GeoNet Terms

- **Application Unit (AU):** An in-vehicle or road-side entity and runs applications that can utilise the OBU's or RSU's communication capabilities, respectively. Examples of AUs are i) a dedicated device for safety applications like hazard-warning, ii) a navigation system with communication capabilities, iii) a nomadic device such as a PDA that runs Internet applications.

- **GeoAware application**: an application able to transmit data to a specific GeoDestination.

- **GeoNet domain:** an ad-hoc domain, also referred to as Vehicular Ad hoc Network (VANET), which is composed of GeoNet nodes (i.e. GeoNet OBUs, GeoNet RSUs) and C2C nodes (i.e. C2CNet OBUs and C2CNet RSUs) and their attached nodes.
-
- **GeoNet nodes**: nodes implementing GeoNet extensions, i.e. nodes implementing the C2CNet layer or the Management layer or both.

- **GeoNet-aware nodes**: IPv6 nodes able to process IPv6 GeoNetworking packets but not implementing C2CNet layer features.

- **GeoNet OBU (On-Board Unit):** A C2CNet OBU which implements IPv6 basic operations and C2CNet layer capabilities. It is an IPv6 router with at least an egress interface (GeoNet interface) and an ingress interface serving other IPv6 nodes. A GeoNet OBU is likely equipped with other network devices in order to allow communications with an infrastructure network. A GeoNet OBU acts as an IPv6 Mobile Router or a VANET IP router.

- **GeoNet RSU (Road-Side Unit)**: A C2CNet RSU which implements IPv6 basic operations and C2CNet layer capabilities. It is an IPv6 router with at least one egress interface (C2CNet interface) and one ingress interface serving other IPv6 nodes. A GeoNet RSU is likely equipped with other network devices in order to allow communications with an infrastructure network. A GeoNet RSU can act as an IPv6 Access Router or a VANET IP router.

- **GeoDestination**: a destination corresponding to a specific geographic area e.g. “all vehicles in 1km range” or “all vehicles located in an area defined by latitude and longitude”.

- **IPv6 GeoNetworking**: the combination of C2C-CC's GeoNetworking together with IPv6 into a single protocol architecture.

- **C2C-CC**: CAR 2 CAR Communication Consortium is a non-profit organisation initiated by European vehicle manufacturers, which is open for suppliers, research organisations and other partners. The CAR 2 CAR Communication Consortium is dedicated to the objective of further increasing road traffic safety and efficiency by means of inter-vehicle communications. [1]

- **C2CNet nodes:** nodes implementing C2CNet layer functions, i.e. C2CNet OBUs and C2CNet RSUs.

- **C2CNet OBU (On-Board Unit)**: a physical device located in a vehicle and responsible for Vehicle-to-Vehicle and Vehicle-to-Infrastructure communications. It also provides communication services to AUs and forwards data on behalf of other OBUs in the GeoNet domain. A C2CNet OBU must implement C2CNet layer capabilities and is equipped with at least a network device for short range wireless communications based on IEEE 802.11p* radio technology. The C2CNet OBU acts as a VANET non-IP router.

- **C2CNet RSU (Road-Side Unit)**: a physical device located at fixed positions along roads and highways, or at dedicated locations such as gas station, parking places, and restaurants. A C2CNet RSU must implement C2CNet layer capabilities and is equipped with at least a network device for short range wireless communications based on IEEE 802.11p* radio technology. A C2CNet RSU is likely equipped with other network devices in order to allow communications with an infrastructure network. The C2CNet RSU acts as a VANET non-IP router.

- **C2CNet address resolution**: Finding a neighbour's MAC address.

- **C2CNet ID**: unique ID to identify a C2CNet node.

- **C2CNet interface**: an IPv6 network interface attached to the C2CNet link.

- **C2CNet layer**: Maintains the information about communication peers by using location-based routing, beaconing and location service. The layer is seen as a link layer from the point of view of IPv6.

- **C2CNet link:** a virtual link with multi-hop GeoNetworking capabilities on which all GeoNet OBUs and GeoNet RSUs in a GeoNet domain are able to communicate at the IPv6 layer.

- **C2CNet neighbours**: Nodes which can communicate directly with one another over the wireless link, i.e. IEEE 802.11p.

- **C2CNet neighbour determination**: Finding a C2CNet neighbour's, to which a packet is to be sent.

- **C2CNet packet**: A specific packet format used by C2CNet layer. Forwarded by using position based routing with the information in C2CNet header.

D.2 IPv6 Networking Terms

- **Legacy IPv6 node**: An IPv6 node that conforms to RFC 4294 (IPv6 Node Requirements) and functions without additional IPv6 networking capabilities. In IPv6 GeoNetworking, legacy IPv6 nodes must continue to function and interact with GeoNet nodes.

- **IPv6 mobile network**: An IPv6 subnetwork - or an entire set of IPv6 subnetworks moving as a unit - which dynamically changes its IPv6 point of attachment to the Internet and thus its reachability in the topology.

- **IPv6 Access Router**: An IPv6 router residing on the edge of an Access Network and connected to one or more Access Points. The Access Points may be of different technology. An Access Router offers IP connectivity to Mobile Nodes, acting as a default router to the Mobile Nodes it is currently serving. The Access Router may include intelligence beyond a simple forwarding service offered by ordinary IP routers.

- **IPv6 Mobile Router (MR)**: An IPv6 router capable of changing its point of attachment to the network, moving from one link to another link.

- **IPv6 Mobile Network Node (MNN)**: Any IPv6 node (host or router) located within an IPv6 mobile network, either permanently or temporarily.

- **IPv6 Correspondent Node (CN)**: Any IPv6 node (host or router) corresponding with a vehicle or roadside IPv6 node.

- I**Pv6 neighbours**: IP nodes on the same GeoNet link.

- **Mobile Network Prefix (MNP)**: A bit string that consists of some number of initial bits of an IP address which identifies the entire mobile network within the Internet topology.

- **Care-of-Address (CoA)**: An IP address associated with a mobile node while visiting a foreign link; the subnet prefix of this IP address is a foreign subnet prefix.

- **Home Address (HoA)**: An IP address assigned to a mobile node, used as the permanent address of the mobile node.

- **Home Agent (HA)**: A router on a mobile node's home link with which the mobile node has registered its current care-of address.
- **Binding Update (BU)**: A message indicating a mobile node's current mobility binding, and in particular its care-of address.

D.3 Generic Networking Terms

- **Ad hoc network:** Communication network which is set up by the communication nodes (peer-to-peer) without any pre-installed fixed infrastructure.
- **V2V (Vehicle-to-Vehicle) communication**: Communication between two vehicles.
- **V2I (Vehicle-to-Infrastructure) communication**: Communication between a vehicle and the infrastructure.
- **I2V (Vehicle-to-Infrastructure) communication**: Communication between the infrastructure and a vehicle.
- **Unicast**: A means of transmitting a message from one source to one specific destination.
- **Multicast**: A means of transmitting a message from one source to several destinations.
- **Anycast**: A means of transmitting a message from one source to one un-specified destination.
- **Broadcast**: A means of transmitting a message to all nodes connected to a network. Normally, a special address, the broadcast address, is reserved to enable all the devices to determine that the message is a broadcast message.
- **GeoNetworking**: Network service that utilises geographical positions and provides ad hoc communication without the need for a coordinating communication infrastructure (definition taken frol [ETSI-TS-102-636-3])
- **Geocast**: A means of transmitting a message to a designated geographical area. GeoBroadcast and GeoAnycast are geocast communication means.
- **GeoBroadcast**: A means of transmitting a message from one source to all nodes located within a certain geographical area. The area is defined by the sender and transmitted with the data packet control information.

- **GeoAnycast**: A means of transmitting a message from one source to one un-specified destination located within a certain geographical area. The area is defined by the sender and transmitted with the data packet control information.
- **GeoUnicast**: A means of transmitting a message from one source to one specific destination located within a certain geographical area.
- **TopoBroadcast**: Refers to the routing protocol which, based on network topology information, routes data from a source node to all nodes located at a specific distance, in terms of hops.
- **1-Hop Broadcast**: To send a data packet to all direct neighbours of a node. No further forwarding of that data packet is applied.
- **Beacon**: Network Layer control data packet which is sent periodically in broadcast mode and which includes control data used to build up the neighbour table.
- **Geo-routing**: Geographic position and movement information of vehicles are used to route data.
- **SAP**: Service Access Point (SAP) is an identifying label for network endpoints used in OSI networking.
- **Communication scenario**: A class of transactions distinguished by characteristically different handling at the protocol layers in GeoNet scope.
- **Location**: Position of a node and time at which this position was taken.
- **Location Table**: Table which location data of other nodes is stored.
- **Neighbour Table**: Table which includes data on neighbouring nodes, e.g. identifier and position of that node.
- **Transmission Interval Control (TIC)**: Mechanisms to control the periodic messages' rate in order to reduce network congestion.
- **Transmission Power Control (TPC)**: Mechanisms to control the messages' transmission power in order to reduce network congestion.
- **IP next hop**: Next hop from an IP point of view.
- **IP next hop determination**: Find IP next hop's IP address from a destination IP address.
- **GPSR**: Makes greedy forwarding decisions using only information about immediate neighbours. The greedy forwarding consists on selecting as next forwarder the neighbour which is the closest to the destination. When a packet reaches a region

where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region.

- **IEEE 802.11p**: Is a draft amendment to the IEEE 802.11 standard to add wireless access in the vehicular environment (WAVE). It defines enhancements to 802.11 required to support Intelligent Transportation Systems (ITS) applications. This includes data exchange between high-speed vehicles and between the vehicles and the roadside infrastructure in the licensed ITS band of 5.9 GHz (5.85-5.925 GHz). IEEE 1609 is a higher layer standard on which IEEE 802.11p is based.

- **ITS-G5:** Is the functionality of an ITS Station as defined in [ETSI-ES-202-663] for physical layer, medium access control sub-layer and extensions to handle parameters of these layers, including the related management. ITS-G5 distinguishes several frequency ranges in European ITS frequency band.

- **ITS-G5A:** Is the operation of ITS-G5 in European ITS frequency bands dedicated to ITS for safety related applications in the frequency range 5,875 GHz to 5,905 GHz as defined by [ETSI-ES-202-663]

- **ITS-G5B:** Is the operation of ITS-G5 in European ITS frequency bands dedicated to ITS non- safety applications in the frequency range 5,855 GHz to 5,875 GHz as described by [ETSI-ES-202-663]

Annex E: References

[Allard2005] G. Allard, P. Jacquet, and B. Mans. “Routing in extremely mobile networks“. In *Proceedings of 4th Annual Mediterranean Ad Hoc Networking Workshop*, Île de Porquerolles, France, 2005.

[Alshaer2005] H. Alshaer and E. Horlait. “An optimized adaptive broadcast scheme for inter-vehicle communication“. In *IEEE Vehicular Technology Conference*, Stockholm, Sweden, 2005.

[Baldessari2006] R. Baldessari, A. Festag, A. Matos, J. Santos, and R. Aguiar. “Flexible connectivity management in vehicular communication networks“. In *Proc. of the WIT*, Hamburg, Germany, 2006.

[Baldessari2008] R. Baldessari, A. Festag, W. Zhang, and L. Le. “A MANET-centric solution for the application of NEMO in VANET using geographic routing“. In *Proc. of th Weedev*, Austria, 2008.

[Baldessari2009] R. Baldessari, T. Ernst, A. Festag, M. Lenardi. “Automotive Industry Requirements for NEMO Route Optimization“. Internet-Draft (draft-ietf-mext-nemo-ro-automotive-req-02). Internet Engineering Task Force, January 2009. Work in progress

[Basagni1998] I. Basagni, S. Chlamtac and V.R. Syrotiuk. “A distance routing effect!ç algorithm for mobility (DREAM). In *Fourth annual AModuleCM/IEEE International Conference on Mobile Computing and Networking*, Dalas, Texas, USA, 1998.

[Benslimane2004] A. Benslimane. “Optimized dissemination of alarm messages in vehicular ad-hoc networks (VANET)“. In *7th IEEE International Conference*, Toulouse, France, 2004.

[C2CCC] Car 2 Car Communication Consortium ““C2C-CC Manifesto“. Version 1.1. http://www.car-to-car.org. August 2007.

[Chatzigiannakis2001**]** I. Chatzigiannakis, E. Nikoletseas, and P. Spirakis. “An efficient communication stChorategy for ad-hoc mobile networks“. In *15th International Conference on Distributed Computing (DISC)*, London, UK, 2001.

[Choi2008] J. Choi, Y. Khaled, M. Tsukada, and T. Ernst. “IPv6 support for VANET with geographical routing“. In *Proc. of the ITST*, Pukhet, Thailand, 2008

[COMeSafety2008] European ITS Communication Architecture - Overall Framework - Proof of Concept Implementation. Draft Version 2.0, COMeSafety Specific Support Action, October 2008.

[Davis2001] J. Davis, A. Fagg, and B. Levine. “Wearable computers as packet transport mechanisms in highly-partitioned ad-hoc networks“. In *5th IEEE International Symposium on Wearable Computers (ISWC)*, Washington, DC, USA, 2001.

[Ducourthial2007] B. Ducourthial, Y. Khaled, and M. Shawky. “Condseeitional transmissions, a strategy for highly dynamic vehicular ad hoc networks“.

[ETSI-ES-202-663] ETSI “Intelligent Transport Systems; European profile standard on the physical and medium access layer of 5 GHz ITS” ETSI ES 202 663 V<0.0.6> Draft for member approval, October 2009.

[ETSI-TR-102-698] ETSI. “Intelligent Transport Systems (ITS); Vehicular Communications; C2C-CC Demonstrator 2008; Use Cases and Technical Specifications”, ETSI TR 102 698 V1.1.1, June 2009.

[ETSI-TS-102-636-2] ETSI. “Intelligent Transportation Systems (ITS); Transport & Network: Vehicular Communications; GeoNetworking and Data Transport; Part 2: Scenarios for GeoNetworking”. ETSI, V0.3.1 Work in Progress, September 2009.

[ETSI-TS-102-636-3] ETSI. “Intelligent Transportation Systems (ITS); Vehicular Communications; GeoNetworking and Data Transport; Part 3: Network Architecture”. ETSI, V0.5.9 Work in Progress, September 2009.

[ETSI-TS-102-636-6-1] ETSI. “Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking and Data Transport; Part 6: Transmission of IPv6 Packets overs GeoNetworking Protocols”. ETSI, Work in Progress, December 2009.

[ETSI-TS-102-665] ETSI. “Intelligent Transport Systems (ITS); Vehicular Communications; Architecture”. ETSI, Work in Progress, December 2009.

[Finn1987] G. Finn. “Routing and addressing problems in large metropolitan-scale internetworks“. Technical Report ISI/RR-87-180, Information Sciences Institute, Mars 1987.

[GeoNetD1.1] GeoNet. “Preliminary GeoNet Architecture”. GeoNet Deliverable D1.1, February 2009.

[GeoNetD2.2] GeoNet. “Final GeoNet Specification”. GeoNet Deliverable D2.2, January 2010.

[GeoNetD4.1] GeoNet. “GeoNet Conformance Test Plan and Results”. GeoNet Deliverable D4.1, January 2010.

[GeoNetD5.1] GeoNet. “GeoNet Emulation Environment Results” GeoNet Deliverable D5.1, January 2010.

[GeoNetD7.1] GeoNet. “GeoNet Experimentation Results” GeoNet Deliverable D7.1, January 2010.

[Granelli2006] F. Granelli, G. Boato, and D. Kliazovich. “MORA: a movement-based routing algorithm for vehicle ad hoc networks“. In *1st IEEE Workshop on Automotive Networking and Applications 2006*, California, USA, 2006.

[Hain2008] T. Hain. “An IPv6 Geographic Global Unicast Address Format“. Internet Draft, January 2008.

[Harshvardhan2006] Harshvardhan P.J. “Distributed robust geocast: A multicast protocol for inter-vehicle communication“. Master's thesis, Dep. of Electrical and Computer Engineering, NCSU, 2006.

[IEEE1609.2] IEEE “Trial-Use Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages”. IEEE 1609.2.

[ISO-21210] ISO TC204 WG16. “Intelligent Transport Systems – Communication for Land Mobiles (CALM) – IPv6 Networking”. ISO FDIS specification 21210, ISO, October 2009. Work in progress.

[ISO-21217] ISO TC204 WG16. “Intelligent Transport Systems – Communication for Land Mobiles (CALM) – Architecture”. ISO FDIS specification 21217, ISO, October 2009. Work in progress.

[Karp2000] B. Karp and H.T. Kung. “GPSR: Gready perimeter stateless routing for wireless networks“. In *Proceedings of MobiCom'00*, pages 43-54, Boston, MA, USA, 2000.

[Ko1998] Y.B. Ko and H.T. Kung. “Location-aided routing (LAR) in mobile ad hoc networks“. In *Fourth annual ACM/IEEE International Conference on Mobile Computing and Networking*, pages 66-75, Dalas, Texas, USA, 1998.

[Korkmaz2004] G. Korkmaz, E. Ekici, F. Ozguner, and U. Ozguner. “Urban multi-hop broadcast protocol for inter-vehicle communication systems“. In *the 1st ACM international workshop on Vehicular ad hoc networks*, Philadelphia, PA, USA, 2004.

[Kosch2002] T. Kosch. “Technical concept and prerequisites of car-to-car communication“. Technical report, BMW Group Research and Technology, 2002.

[Legner2002] M. Legner. “MAP-based geographic forwarding in vehicular networks“. Master's thesis, Stuttgart University, 2002.

[Li2000] Q. Li and D. Rus. “Sending messages to mobile users in disconnected ad-hoc wireless networks“. In *6th annual international conference on Mobile computing and networking (MOBICOM)*, 2000.

[Little2005] T.D.C. Little and A. Agarwal. “An information propagation scheme for VANETs“. In *8th International IEEE Conference on Intelligent Transportation Systems*, Vienna, Austria, 2005.

[Liu2004] G. Liu, B. Lee, B. Seet, C. Foh, and K. Lee. “A routing strategy for metropolis vehicular communications“. *In Proc. International Conference on Information Networking*, pages 533-542, 2004.

[Lochert2003] C. Lochert, H. Hartenstein, J. Tian, H. Fler, D. Herrmann, and M. Mauve. “A routing strategy for vehicular ad hoc networks in city environments“. In *IEEE Intelligent Vehicles Symposium*, Ohio, USA, 2003.

[Lochert2004] C. Lochert, M. Mauve, H. Füssler, and H. Hartenstein. “Geographic routing in city scenarios“. In *Proceedings of ACM MOBICOM*, Philadelphia, PA, USA, 2004.

[Ma2008] Z. Ma, F. Kargl, and M. Weber, “Pseudonym-on-demand: a new pseudonym refill strategy for vehicular communications,” in WiVeC 2008, Calgary, Canada, September 2008.

[Maihöfer2003] C. Maihöfer, W. Franz, and R. Eberhardt. “Stored geocast“. In *13th Fachtagung Kommunikation in Verteilten Systemen (KiVS), InformatikAktuell*, Leipzig, Germany, 2003.

[Maihöfer2004] C. Maihöfer. “A survey of geocast routing protocols“. *IEEE Communications Surveys and Tutorials*, 6, 2nd quarter 2004.

[Mauve2001] M. Mauve, J. Widmer, and H. Hartenstein. “A survey on position-based routing in mobile ad hoc networks“. *IEEE Network Magazine*, November/December 2001.

[Menouar2007] H. Menouar, M. Lenardi, and F. Filali. “Movement prediction-based routing (MOPR) concept for position-based routing in vehicular networks“. In 1st IEEE International Symposium on Wireless Vehicular Communications (WiVec'07), Baltimore, USA, October 2007.

[Mo2006] Z. Mo, H. Zhu, K. Makki, and N. Pissinou. “MURU: A multi-hop routing protocol for urban vehicular ad hoc networks“. In *3rd Annual International Conference on Mobile and Ubiquitous Systems: Networks and Services*, California, USA, 2006.

[Namboodiri2007] V. Namboodiri and L. Gao. “Prediction based routing for vehicular ad hoc networks“. *IEEE Transactions on Vehicular Technology*, 56(4):2332-2345, November 2007.

[Naumov2007] V. Naumov and TR. Gross. “Connectivity-aware routing (car) in vehicular ad hoc networks“. In *IEEE INFOCOM*, Anchorage, Alaska, USA, 2007.

[Navas2001] J.C. Navas. *“Geographic routing in a datagram internetwork“*. PhD thesis, 2001.

[Navas1997] J. Navas and T. Imielinski. *"G*eoCast - Geographic Addressing and Routing". In *Proceedings of the 3rd annual ACM/IEEE MobiCom*, New York, NY, USA, 1997.

[Papadimitratos2008] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communications: Design and architecture," IEEE Communications Magazine, vol. 46, no. 11, pp. 100–109, November 2008.

[PRECIOSA] EU Project PRECIOSA (Privacy Enabled Capability in Co-operative Systems and Safety Applications). http://www.preciosa-project.org

[RFC1712] C. Farrell, M. Schulze, S. Pleitner, and D. Baldoni. "DNS encoding of geographical location", November 1994. RFC 1712. Status: Experimental

[RFC2009] T. Imielinski and J. Navas. "GPS-Based Addressing and Routing". RFC 2009 (Experimental), November 1996.

[RFC2401] S. Kent and R. Atkinson. "Security Architecture for the Internet Protocol". RFC 2401, Internet Engineering Task Force, November 1998.

[RFC3095] C. Bormann et al. "Robust Header Compression (ROHC): Framework and four : RTP, UDP, ESP, and uncompressed". RFC 3095, Internet Engineering Task Force, July 2001.

[RFC3306] B. Haberman and D. Thaler. "Unicast-Prefix-based IPv6 Multicast Addresses". RFC 3306 (Proposed Standard), August 2002. Updated by RFCs 3956, 4489.

[RFC3693] J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J. Polk. "Geopriv Requirements". RFC 3693 (Informational), Internet Engineering Task Force, February 2004.

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

[RFC3971] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander. "SEcure Neighbor Discovery (SeND)". RFC 3971, Internet Engineering Task Force, March 2005.

[RFC4119] J. Peterson. "A Presence-based GEOPRIV Location Object Format". RFC 4119 (Proposed Standard), Internet Engineering Task Force. December 2005

[RFC4581] M. Bagnulo, J. Arkko. "Cryptographically Generated Addresses (CGA) Extension Field Format". RFC 4581, Internet Engineering Task Force, October 2006.

[RFC4861] T. Narten, E. Nordmark, W. Simpson, and H. Soliman. “Neighbour Discovery for IP version 6 (IPv6)”. RFC 4861, Internet Engineering Task Force, September 2007.

[RFC4862] S. Thomson, T. Narten, and T. Jinmei. “IPv6 Stateless Address Autoconfiguration“. RFC 4862, Internet Engineering Task Force, September 2007.

[RFC5648] R. Wakikwawa, V. Devarapalli, G. Tsirtsis, T. Ernst, K. Nagami. “Multiple Care-of Addresses Registration”. RFC 5648, Internet Engineering Task Force. October 2009.

[Sanzgiri2005] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, Authenticated Routing for Ad Hoc Networks, IEEE Journal On Selected Areas In Communications 23 (3) (2005) 598–610.

[SeVeCOM] EU Project SeVeCOM (Secure Vehicular Communication). http://www.sevecom.org

[Sun2000] M. Sun, W. Feng, T. Lai, K. Yamada, H. Okada, and K. Fujimura. “GPS-based message broadcasting for inter-vehicle communication“. In *International Conference on Parallel Processing*, Washington, DC, USA, 2000.

[Vahdat2000] A. Vahdat and D. Becker. “Epidemic routing for partially connected ad hoc networks“. Technical Report CS-200006, Computer Science Dpt, Duke University, 2000.

[Vare2004] J. Vare, J. Syrjarinne, and K-S Virtanen. “Geographical positioning extension for IPv6“. In *Proc. of the ICN*, Guadeloupe, 2004.

[Wischhof2005a] L. Wischhof and H. Rohling. “On utility-fair broadcast in vehicular ad hoc networks“. In *2nd International Workshop on Intelligent Transportation*, Hamburg, Germany, 2005.

[Wischhof2005b] L. Wischhof and H. Rohling. “Congestion control in vehicular ad hoc networks“. In *IEEE International Conference on Vehicular Electronics and Safety*, Xi'an, Shaanxi, China, 2005.

[Zhao2006] J. Zhao and G. Cao. “VADD: Vehicle-assisted data delivery in vehicular ad hoc networks“. In *25th Conference on Computer Communications (INFOCOM)*, Barcelona, Spain, 06.