CAR 2 CAR Communication Consortium

Manifesto

Overview of the C2C-CC System

Report name C2C-CC Manifesto

This document summarizes the main building blocks for a
CAR 2 X Communication System
as it is pursued by the CAR 2 CAR Communication Consortium.

Document status	Public
Version number	Version 1.1
Date of release by the Technical Committee	28th August, 2007

Revision Chart and History Log

Releases:

Version	Changes	Editor	Date of TC-Release	New Version
	First release	See list of contributors in this document	21st May 2007	1.0
	Notation of CAR 2 CAR, CAR 2 X, etc.	Heyms	28th August 2007	1.1

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 About This Document

This document summarizes and describes the main building blocks of the CAR 2 X Communication System as it is pursued by the CAR 2 CAR Communication Consortium (C2C-CC). “CAR 2 X” means interactions among cars, between cars and infrastructures, and viceversa. It provides interested readers with an introduction to CAR 2 X communications. It is intended to be a living document which will be complemented according to the progress of the work of the C2C-CC. One main objective of this document is to give insight into ongoing and upcoming activities, such as public funded projects which target to contribute to the C2C-CC specifications, an overview on ongoing work and results achieved so far. In addition, this document provides concepts and technologies that have been developed or identified by the C2C-CC and assessed as necessary building blocks to be proposed for a standard.

1.2 CAR 2 CAR Communication Consortium

The goal of the CAR 2 CAR Communication Consortium is to standardize interfaces and protocols of wireless communications between vehicles and their environment in order to make the vehicles of different manufacturers interoperable and also enable them to communicate with road-side units.

The mission and the objectives of the CAR 2 CAR Communication Consortium are

- to create and establish an open European (possibly worldwide) industry standard for CAR 2 CAR Communication Systems
- to guarantee inter-vehicle operability
- to enable the development of active safety applications by specifying, prototyping and demonstrating the CAR 2 CAR system
- to promote the allocation of a royalty free European-wide exclusive frequency band for CAR 2 CAR applications
- to push the harmonization of CAR 2 CAR Communication standards worldwide
- to develop deployment strategies and business models to speed-up the market penetration

The CAR 2 CAR system shall provide the following top level features:

- automatic fast data transmission between vehicles and between vehicles and road side units

- transmission of traffic information, hazard warnings and entertainment data
- support of ad hoc CAR 2 CAR Communications without need of a pre-installed network infrastructure
- the CAR 2 CAR system is based on short range Wireless LAN technology and free of transmission costs

Ad hoc CAR 2 CAR Communications enable the cooperation of vehicles by linking individual information distributed among multiple vehicles. The so-formed Vehicular Adhoc Network (VANET) works like a new 'sensor' increasing the drivers' range of awareness to spots which both the driver and onboard sensor systems otherwise cannot see.

The CAR 2 CAR system electronically extends the driver's horizon and enables entirely new safety functions. CAR 2 CAR Communications form a well suited basis for decentralized active safety applications and therefore will reduce accidents and their severity. Besides active safety functions, it includes active traffic management applications and helps to improve traffic flow.[1]

1.3 C2C-CC Demonstration Event in 2008

The C2C-CC plans to host a major demonstration event in late 2008. This event represents an opportunity for research projects and individual companies to exhibit their achievements towards politics, potential customers and general public. In detail, this event is intended to publicly demonstrate

- beneficial use cases,
- project interoperability,
- functionalities, and
- technical issues

of different European and national projects dealing with Vehicle 2 Vehicle (V2V or C2C) and Vehicle 2 Infrastructure (V2I or C2I) communications (collectively "C2X Communications"). The demonstration will also show that the different technical concepts for C2X Communication developed in Europe converge and can be harmonized in a European standard (or better worldwide standard) within a reasonable timeframe.

[1] Note that the term "CAR 2 CAR Communication" in the context of the C2C-CC always includes "CAR 2 Infrastructure Communication". The latter refers to communication from cars to regular IEEE 802.11 a/b/g systems (e.g. Hotspots, WLAN Access Points) and to road side units as part of the C2C-CC System. Both, CAR 2 CAR and CAR 2 Infrastructure Communications are also referred to CAR 2 X Communications.

1.4 Conventions and Terms

A list of terms defined by the C2C-CC and used in this document can be found in the appendix (Section 10.1).

The document uses some keywords, such as *shall* and *may*, that need to be interpreted correctly. The keyword *shall* indicates that a definition or item is mandatory. The keyword *may* means that a feature is optional.

2 Scenarios

C2X Communication enables a great number of use cases in order to improve driving safety or traffic efficiency and provide information or entertainment to the driver. The C2C-CC C2X system has been and will continue to be designed based on the use case requirements. This section serves to introduce example use cases and shows how the use cases imply certain requirements to the system.

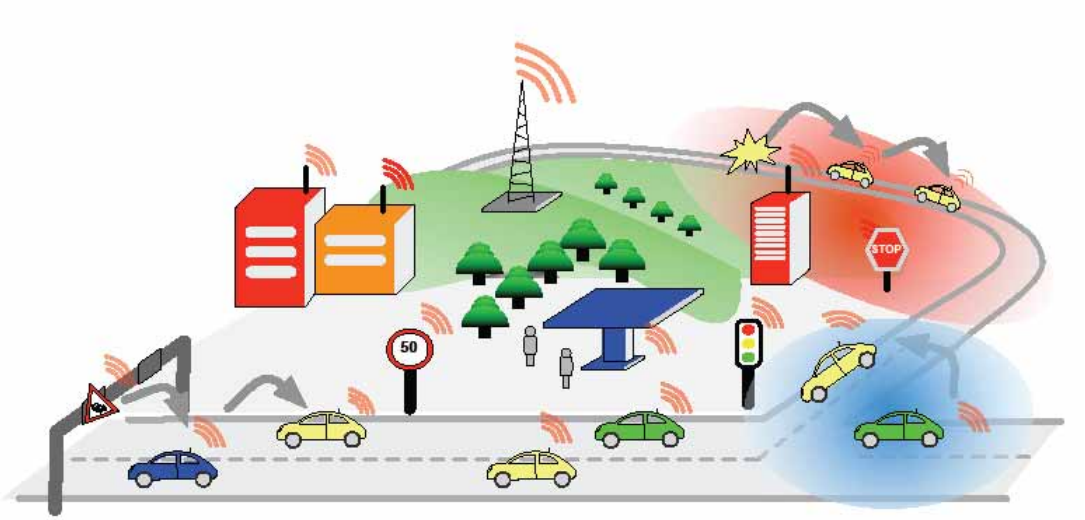

Figure 1 The system requirements are derived from various use cases

As shown in Figure 1 several actors are involved in C2X Communication. Those actors are:

- the drivers, which benefit from the system by receiving warning messages and route recommendations,
- road operators, who receive traffic data and are therefore enabled to control the traffic in a more efficient way,
- hotspot and Internet service providers, who can attach vehicle communication systems e.g. at gas stations.

In the following, several safety and non-safety use cases are exemplarily described.

2.1 Safety

Safety use cases are those where a safety benefit exists when the vehicle enters into a scenario applicable to the use case. In this section, we exemplarily introduce three safety use cases and describe their operation. In general, a variety of requirements can be derived from the description provided.

2.1.1 Cooperative Forward Collision Warning

Typical causes of rear-end collisions are driver distraction or sudden braking ahead of a following vehicle. In all regions of the world, rear-end collisions cause a significant percentage of all accidents. The Cooperative Forward Collision Warning use case provides assistance to the driver primarily to avoid rear-end collisions with other vehicles. During normal driving, the equipped vehicles anonymously share relevant information such as position, speed and heading. In order to predict an imminent rear-end collision, each vehicle monitors the actions of its own driver and the position and behavior of all other nearby vehicles. When the vehicle detects a critical proximity, the vehicle warns the driver via visual, auditory, and/or haptic displays. Thus, the driver will have enough time to intervene and avoid a crash. In addition to wireless communications, object detection sensors might be used to identify vehicles that are not equipped with wireless communication.

As described above, the Cooperative Forward Collision Warning use case requires:

- the ability for all vehicles to share information with each other over a distance of approximately 20 to 200 meters in order to predict a rear-end collision,
- accurate relative positioning of the vehicles,
- vehicles to trust the information they receive from other vehicles,
- reasonable market penetration in order to have a safety impact.

2.1.2 Pre-Crash Sensing/Warning

The Pre-Crash Sensing/Warning use case addresses the next step beyond the Cooperative Forward Collision/Warning use case. Here, the assumption is that a crash is unavoidable and will take place. Similar to the Cooperative Forward Collision Warning use case use case, this use case requires that all vehicles periodically share information from neighboring vehicles to predict a collision. Once a collision is no longer avoidable (i.e., no possible way to steer or brake to avoid the crash), the involved vehicles engage in fast and reliable communication to exchange information such as more detailed position data and vehicle size. This extra information provided to both vehicles enables an optimized usage of actuators such as air bags, motorized seat belt pre-tensioners, and extendable bumpers.

As described above, the Cooperative Forward Collision/Warning use case requires:

- the ability for all vehicles to share information with each other over a distance of approximately 20 to 100 meters in order to predict an unavoidable crash,
- accurate relative positioning of the vehicles,
- vehicles to trust the information they receive from other vehicles,
- reasonable market penetration in order to have a safety impact,
- a fast and reliable connection between two vehicles in case an unavoidable crash is detected.

2.1.3 Hazardous Location V2V Notification

The Hazardous Location V2V Notification use case utilizes the network of vehicles to share information that relates to dangerous locations on the roadway, as for instance slippery roadways or potholes. Thereby, a major issue is the generation of information about the driving condition at a specific location. For instance, a vehicle that experiences an actuation of its ESP (Electronic Stability Program) system, the vehicle retains information about the location and shares its knowledge with other vehicles in the surrounding area. Vehicles that receive the information either provide it to the driver or use it to automatically optimize its chassis or safety systems. The relevant information can be shared with any number of vehicles over an area, limited only by the current density of equipped vehicles. In addition to the case where the information is created in a vehicle, information from external service providers can be accessed via a roadside unit and propagated through the vehicular ad hoc network in the same manner.

As described above, the Hazardous Location V2V Notification use case requires:

- vehicles to trust the information originated by other vehicles,
- vehicles to trust the information originated by roadside units,
- reasonable market penetration in order to have a safety impact,
- the ability for vehicles to share information about a specific geographic area through multiple-hops,
- the ability to evaluate and track the validity of the information shared through multiple-hops.

2.2 Traffic Efficiency

Traffic Efficiency use cases are those meant to improve efficiency of the transportation network by providing information either to the owners of the transportation network or to the drivers on the

network. Those use cases primarily leverage the communication network provided by CAR 2 CAR to either create new traffic related information or share existing information in a way that was not feasible without CAR 2 CAR. A more efficient transportation system can result in fewer delays experience by drivers or less road construction and maintenance costs to the owners of the transportation network. Thus, traffic participants benefit from shorter travel times and road operators benefit from reduced expenses to maintain the roadways.

2.2.1 Enhanced Route Guidance and Navigation

The Enhanced Route Guidance and Navigation use cases uses information collected by an infrastructure owner to deliver route guidance information to a driver. Constantly, the infrastructure owner is collecting data and predicting traffic congestion on roadways throughout a large region. When an equipped vehicle travels by a roadside unit which supports the use case, the roadside unit sends the vehicle information regarding current and expected traffic conditions throughout the region, or perhaps, just for the route entered into the vehicle's navigation unit. The vehicle uses this information to inform the driver about expected delays or better routes that might exist due to the traffic conditions. Because this use case is likely to route a number of people around congested areas, the overall transportation system becomes more efficient with the use of alternate routes that are not congested.

As described above, the Enhanced Route Guidance and Navigation use case requires:

- an infrastructure provider to collect and maintain the information on traffic congestion,
- vehicles to trust the information provided by the roadside unit,
- the ability for a roadside unit to offer a service to passing vehicles.

2.2.2 Green Light Optimal Speed Advisory

The Green Light Optimal Speed Advisory use case provides information to the driver in an effort to make their driving smoother and avoid stopping. As a vehicle approaches a signalized intersection, the vehicle receives information regarding the location of the intersection and the signal timing (i.e., number of seconds to switch from green to red light). With this information, the vehicle calculates an optimal vehicle speed using the distance from the vehicle to the intersection and the time when the signal is green. The vehicle notifies the driver of the optimal speed. If the vehicle travels at or near the optimal speed, the traffic signal is likely to be green and the driver will not have to slow or stop the vehicle. The effect of this use case is less stopping on roadways resulting in increased traffic flow and increased fuel economy for equipped vehicles.

As described above, the Green Light Optimal Speed Advisory use case requires:

- a signalized intersection to transmit intersection position and traffic signal phase and timing information for each direction of travel and each lane with individualized signal timing,
- vehicles to trust the information provided by the traffic signal.

2.2.3 V2V Merging Assistance

The V2V Merging Assistance use case allows merging vehicles to join flowing traffic without disrupting the flow of the traffic. When a vehicle enters an on-ramp to a limited access roadway, the vehicle communicates with the traffic that will be adjacent to the vehicle when it attempts to merge into the roadway. The vehicle requests specific maneuvers from the traffic participants in order to allow a safe and non-disruptive merge into the regular traffic. With no objections from the traffic, the traffic will either automatically adjust or will advise drivers in traffic on how to act. With the actions by the merging traffic, the vehicle can enter the traffic flow without major disruptions to the flow. This use case can also be extended to provide a ramp metering service where the merging vehicle is informed when it may proceed on the on-ramp in order to merge into an empty space in traffic.

As described above, the V2V Merging Assistance use case requires:

- the ability for all vehicles to share information with each other over a distance adequate to perform the merging maneuver,
- vehicles to trust the information they receive from other vehicles,
- vehicles to agree on actions in order to allow space for a merging vehicle.

2.3 Infotainment and Others

The category of use cases named Infotainment and Others is meant to capture the remaining use cases which are not directed at Safety or Traffic Efficiency. Many of these use cases interact more directly with the vehicle owner on daily basis providing entertainment or information on a regular basis. Others are transparent to the driver but still perform a valuable function such as increasing fuel economy or allowing diagnostic information to be accessed more efficiently at a service garage.

2.3.1 Internet Access in Vehicle

The Internet Access in Vehicle use case allows for a connection to the Internet. This enables the use of all kinds of common IP based services in the vehicle. Therefore, a multi-hop route to an RSU is established and maintained that acts as an Internet gateway. The multi-hop route is transparently

masked to above layers of the protocol stack and therefore enables almost any IP based protocol and service to be deployed in the vehicles. This use case enables the benefits obtainable with the freedom for the vehicle or driver to access any type of information available on the Internet.

As described above, the Internet Access in Vehicle use case requires:

- the ability for a vehicle to connect to a roadside unit who offers the Internet connection,
- the ability for a vehicle to address Internet servers through the roadside unit,
- the ability to multi-hop messages to a roadside unit from a vehicle when the two cannot communicate directly with one another,
- a dynamic route maintenance that ensures the necessary service quality parameters and resets the multi-hop route when necessary,
- as an alternative scenario, also supported by C2C Communication Systems: To connect to a regular hotspot running IEEE 802.11 a, b, g WLANs.

2.3.2 Point of Interest Notification

The Point of Interest Notification use case allows local businesses, tourist attractions, or other points of interest to advertise their availability to nearby vehicles. In this case, a roadside unit broadcasts information regarding a point of interest such as its location, hours of operation, and pricing. The huge amount of information is filter by the vehicles in a situation adaptive manner and when appropriate presented to the driver. For instance, if the fuel gauge is low, the vehicle could show the driver locations and prices for fueling stations in the immediate area. The benefit of this use case is that advertising becomes more effective in that the audience is within the geographic area and may be more likely to visit than someone listening to an FM broadcast or surfing the Internet hundreds of kilometers away. The benefit to consumers is up-to-date information from a business in the proximity.

As described above, the Point of Interest Notification use case requires:

- vehicles to trust the information originated by roadside units,
- the ability for a roadside unit to broadcast information to surrounding vehicles.

2.3.3 Remote Diagnostics

The Remote Diagnostics use case allows a service station to assess the state of a vehicle without making a physical connection to the vehicle. When a vehicle enters the area of a service garage, the service garage can query the vehicle for its diagnostic information to support the diagnosis of the problem reported by the customer. Even as the vehicle approaches, the vehicles' past history and the customers' information can be retrieved from a database and be ready for the technician to use. If software updates are required, the system can install the updates also without the physical

connection. This use case can reduce the amount of time necessary to serve a customer during a visit to a service garage. This will also result in lower costs for repair and less waiting times for customers.

As described above, the Remote Diagnostics use case requires

- vehicles to establish a trusted and secure connection with a roadside unit at a service garage,
- the ability for a vehicle to identify itself when requested by an authorized requestor.

3 System Prerequisites and Constraints

The C2X Communication System is principally a distributed and self-organizing mobile communication network which is able to cope with intermittent access to the communication infrastructure. As it is well-known for conventional communication systems, standardization of the communication protocols ensures interoperability at the network level. A specific aspect of C2X Communication is the requirement to standardize also active safety applications. A C2X Standard for application need to comprise methods for hazard detection and classification, data structures exchanged among cars, and their interpretation by receiving cars.

The prerequisites and constraints for a successful operating system can be separated in two main groups:

- economical prerequisites and constraints, and
- technical prerequisites and constraints.

In this chapter, we explain and discuss the economical issues followed by the technical issues in detail.

3.1 Economical Prerequisites and Constraints

C2X Communication allows for autonomous exchange of data among vehicles. The CAR 2 CAR Communication Consortium provides a technical platform for a wide range of applications. Among these, safety and traffic flow applications are most appealing, as they hold the potential for improving the traffic situation to an extent that would be difficult to realize with alternative technologies to vehicular communication. Obviously, C2C-CC technology requires a certain distribution in the market before it can show any effect. The required penetration [1] is estimated to

- at least 10 % of all cars for inter-vehicle danger warning applications,
- and about 5 % for traffic information propagation.

One of the economical challenges is the fact that cooperative systems do not constitute an immediate value to the customers. A reluctant introduction may refrain potential new customers from equipping their car with a C2X Communication System, which eventually results in a chicken-and-egg problem. New strategies for the introduction of these systems need to be developed. This issue has been identified and market introduction and business cases will be studied in detail.

A system, which supports only with a certain minimum penetration rate, cannot be deployed. Therefore the C2C-CC communication system supports applications which communicate between vehicles and road-side units. It would also be highly beneficial to support applications which are based on the Internet protocol family in addition to active safety applications. These applications may include general access to the Internet and provide all kind of information delivery to cars' passengers and various comfort functions.

Even in an optimal introduction scenario, where every new car will be equipped with a C2C-CC Communications System from a certain date onwards, older cars without a communication system will remain on roads. In such a case, it will take

- about one and a half years to reach 10% penetration in the field,
- and more than 6 years to reach 50%.

Clearly, the introduction phase until a minimum penetration rate is reached would be even prolongated the lower the equipment rate. As a consequence, the C2X Communication System must be able to work in scenarios with low penetration and high penetration rates.

In order to overcome the hurdle of low penetration rates in the initial phase, the C2X Communication System can provide communication capabilities for Internet protocols and provide Internet services and applications. Another strategy attempts to create a benefit for the vehicle manufactures during production and service with all cars having a wireless interface. The combination of both strategies may re-finance the C2C-CC Communication System.

Yet aanother option for solving the problem of the market introduction of (stand-alone) C2C-CC Communication Systems is based fixed stations and road side units by third parties, e. g. by the government. The infrastructure would allow for a set of applications from the very first car equipped with a C2X Communication System. Examples for such applications are traffic signal violation warning, in-vehicle signing or electronic payment.

In fact, the technical principles and system architecture of the C2X Communication System incorporate communication of cars with fixed stations and road side units. All protocols and parts of the communication system shall therefore take into account the additional stationary nodes, applications and network load.

In summary, only a joint initiative of all European vehicle manufactures, suppliers, scientific organizations and standardization bodies will lead to an economically promising and successful market introduction.

3.2 Technical Prerequisites and Constraints

3.2.1 Anonymity and Data Security

The C2C-CC Communication System enables cars to exchange data. Although some of the applications could rely on simple message propagation in some of the scenarios, other applications and situations are also necessary in which data has to be relayed to one or more specific nodes, identifiable through an identifier. On the other hand, anonymity of the vehicle and its driver must be protected to a level at least comparable to which users of mobile phones feel comfortable with, today. One of the technical approaches to accomplish anonymity is based on the use of temporary identifiers instead of fixed ones.

Furthermore, the importance of privacy is different in European countries due to historic experiences and the legal regulations. In some countries privacy is mandatory due to customer request or by law. In other countries laws enforce the technical capability of driver identification in every situation. Consequently, the C2X System must incorporate the different requirements for anonymity and security across Europe.

For the success of C2C-CC Communication Systems a reliable system with a high availability is of great importance. In case a driver would receive incorrect data several times, the driver would not trust its technical features. Such incorrect data can be caused by malfunctioning or malicious users and can have a severe effect on the C2X System. As a technical pre-requisite, it should not be possible for anyone to send a false data, such as a warning message using a notebook from a position close to the street. A technical approach to accomplish this feature is based on digital signatures and certificates.

Finally, legal questions such as liability issues are currently regarded to be out of scope of the C2C-CC. However, they also represent an important prerequisite, for example in a scenario where a useless or wrong message provokes a change of driving behavior and eventually results in a road accident. It is unclear who might be held responsible in this case. The situation will become even more complicated when co-operative driving applications based on C2C-CC appear in the market.

3.2.2 Effective Protected Frequency Band

For safety applications, the C2X Communication needs to be robust in all situations and ensure a certain quality of service level, e.g. a minimum latency and a maximum reliability when sending, forwarding or receiving messages. This cannot be guaranteed when other non-safety communication uses the same frequency band and consumes a considerable share of the available bandwidth. A

safety critical message must reach all receivers in time, even if a user in another car simultaneously downloads a video from the Internet using a standard WLAN access point.

If the system would use open bands like the ISM, robust communication and the required quality of service cannot be guaranteed. For this reasons, the C2C-CC supports the allocation of an effectively protected frequency band.

The following **Fehler! Verweisquelle konnte nicht gefunden werden.** shows the requested frequency band and channel usage for Europe.

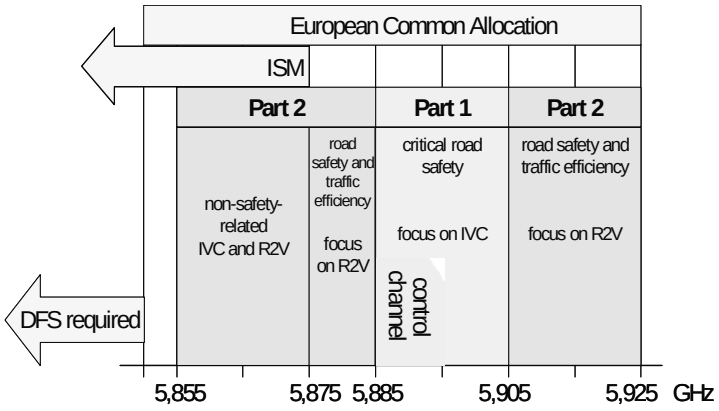

Figure 2 Requested frequencies in Europe (taken from ETSI TR 102 492-2)

The band designated for safety critical applications with focus on (but not limited to) CAR 2 CAR Communication, is located in the band between 5.885 and 5.905 GHz. The allocation process is still ongoing.

The current status of frequency allocation is described in the following documents:

- ETSI TR 102 492-1 V1.1.1 (2005-06) - Technical Report; Electromagnetic compatibility and Radio spectrum Matters (ERM); Intelligent Transport Systems (ITS); Part 1: Technical characteristics for pan-European harmonized communications equipment operating in the 5 GHz frequency range and intended for critical road-safety applications; System Reference Document,
- ETSI TR 102 492-2 V1.1.1 (2006-03) -Technical Report; Electromagnetic compatibility and Radio spectrum Matters (ERM); Intelligent Transport Systems (ITS); Part 2: Technical characteristics for pan European harmonized communications equipment operating in the 5 GHz frequency range intended for road safety and traffic management, and for non-safety related ITS applications; Draft System Reference Document.

3.2.3 Scalability

The C2C Communication System must work in situations with a very small density of road traffic and in situations with a very high traffic density, such as traffic jams or major intersections. These two situations cause different technical challenges. In sparse situations, a car is often out of the transmission range of other cars that potentially could forward data. In dense situations, the data traffic of all cars can exceed the available bandwidth and overload the network. The CAR 2 CAR system has to support and seamlessly scale between both extreme situations.

Also, it can be foreseen that in the market introduction phase very few cars are equipped with C2C Communication Technology (see Section 3.1). In fact, this problem is similar to the two scenarios with opposite traffic densities. Even the first systems introduced in the market must be able to handle situations with high traffic density, because this car might be still in operation even several years after their production.

It is necessary in all cases, that a first generation system is compatible with systems of later generations.

3.2.4 Mandatory Sensor Data

The integration of a C2C Communication System into a car is not addressed by the C2C-CC and is in the responsibility of individual car manufacturer and its automotive supplier. However, a certain set of preconditions must be fulfilled for integration. This mainly comprises the availability of a basic set of sensor data, however quality and security issues also play an important role.

For sensor data which are mandatory for the system, data structures and certain characteristics have to be specified. One prominent example is position data, which are needed by the communication system and by many applications. While for the communication system itself accuracy comparable of those delivered of today's GPS system is sufficient, some applications may need much higher precision. If applications need more accurate position data or positions at more frequent updates, it is the task of the application designer to get this data delivered by in-car systems or off-board servers. It must also be noted that GPS is not compulsory for the C2C-CC System. Any other positioning system that fulfills the requirements may be used instead.

The C2C-CC will specify a data structure (including properties like accuracy, freshness, update rate etc.) which must be supported by each system in each vehicle. The following non-exhaustive list of parameters is regarded as mandatory sensor data, which have to be provided by the in-car system are:

- Position data,
- Vehicle speed,
- Driving direction,

- Hazard warning signal flasher,
- Brake power / vehicle deceleration,
- ABS, ESP and ASR sensors,
- Rain sensor / wiper status.

The first three parameters are required by the C2C-CC Communication System itself and can be utilized by the applications. All other listed parameters are needed for the applications and it is not finally decided if they are mandatory or not. With additional applications possible, there will be more sensor data necessary.

Currently, the method to collect sensor data is regarded to be out-of-scope of the C2C-CC. Sensors might be directly connected to the C2C-CC communication system and the system would read data from a vehicle's internal network. Alternatively, a direct link between the C2X system to an electronic control unit of the car via a suitable interface may exist. The C2C-CC generalizes from this scheme and considers only the properties of the parameters.

4 System Architecture

This chapter describes the C2C Communication System architecture at a high abstraction level. It explains core components and their interaction, the protocol architecture, and main interfaces.

4.1 System Overview

The draft reference architecture of the C2C Communication System is shown in Figure 3. It comprises three distinct domains: in-vehicle, ad hoc, and infra-structure domain.

The **in-vehicle domain** refers to a network logically composed of an on-board unit (OBU) and (potentially multiple) application units (AUs). An AU is typically a dedicated device that executes a single or a set of applications and utilizes the OBU's communication capabilities. An AU can be an integrated part of a vehicle and be permanently connected to an OBU. It can also be a portable device such as laptop, PDA or game pad that can dynamically attach to (and detach from) an OBU. AU and OBU are usually connected with wired connection, but the connection can also be wireless, such as using Bluetooth, WUSB or UWB. The distinction between AU and OBU is logical; they can also reside in a single physical unit.

The **ad hoc domain**, or Vehicular Ad hoc Network (VANET), is composed of vehicles equipped with OBUs and stationary units along the road, termed road-side units (RSUs). An OBU is at least equipped with a (short range) wireless communication device dedicated for road safety, and potentially with other optional communication devices. OBUs form a mobile ad hoc network (MANET) which allows communications among nodes in a fully distributed manner without the need for a centralized coordination instance. OBUs directly communicate if wireless connectivity exists among them. In case of no direct connectivity, dedicated routing protocols allow multi-hop communications, where data are forwarded from one OBU to another, until it reaches the destination. The primary role of an RSU is the improvement of road safety, by executing special applications and by sending, receiving or forwarding data in the ad hoc domain in order to extend the coverage of the ad hoc network. OBUs and RSUs can be seen as nodes of an ad hoc network, respectively mobile and static nodes. An RSU can be attached to an infrastructure network, which in turn can be connected to the Internet. As a result, RSUs may allow OBUs to access the infrastructure. In this way it is possible for AUs registered with an OBU to communicate with any host on the Internet, when at least one infrastructure-connected RSU is available.

In the ad hoc domain, two or more RSUs can communicate to each other directly or via multi-hop communications by means of the same kind of routing protocols used for communications between OBUs and RSUs.

An OBU may also be equipped with alternative wireless technologies for both, safety[2] and non-safety. As shown in Figure 3, an OBU may also communicate with Internet nodes or servers via public, commercial, or private hot spots (HS) (also referred to “WIFI hot spots”) operated individually at home or at office or by wireless Internet service providers.

While RSUs for Internet access are typically set up by with a controlled process by a C2C Communication key stake holder, such as road administrators or other public authorities, public or privately owned hot spots are usually set up in a less controlled environment. These two types of **infrastructure domain** access, RSU and HS, also correspond to different applications types. In case that neither RSUs nor hot spots provide Internet access, OBUs can also utilize communication capabilities of cellular radio networks (GSM, GPRS, UMTS, HSDPA, WiMax, 4G) if they are integrated in the OBU, in particular for non-safety applications.

The infrastructure domain is linked to a PKI certification infrastructure. The Certification Authority (CA) is an entity that issues digital certificates to OBUs and RSUs. These certificates are used in communications among nodes to attest if security credentials belong to a certain node. Their use is intended for an overall security policy, which is out of the scope of this document.

[2] The use of infrared and 60 GHz millimeter-wave based communications for road-safety is complementary to the wireless LAN-like technology and is currently under discussion in the C2C-CC.

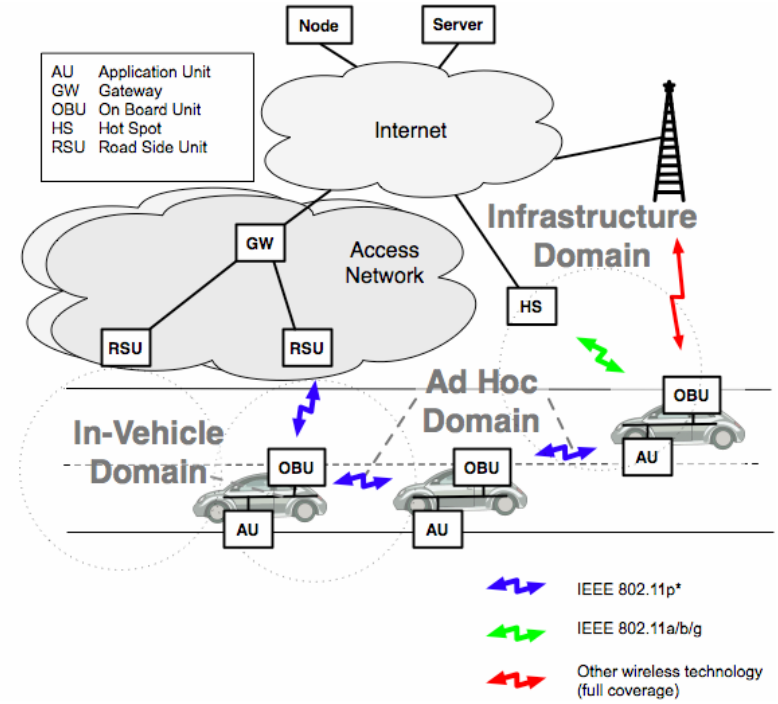

Figure 3 Draft reference architecture

The described draft architecture can be mapped to an abstract reference model as shown in Figure 4, clearly identifying reference entities and reference points.

- Ad hoc communication among vehicles is represented by reference point I1, the communication to road-side units by reference point I2.
- Access to dedicated C2C Service infrastructure happens via reference point I3, whereas in particular commercial services can be accessed via I4. When the same C2C Service infrastructure is accessed via an RSU this happens by reference point I7
- Services of the C2C Operation Support System (C2C OSS) are available at reference point I5, The C2C OSS comprises all functionality, systems and services related to operation of the C2C System, such as authentication, authorization, certificate management, registry databases, service provisioning and general systems management. , Whenever a vehicle also uses commercial telecommunication access networks the respective service provisioning infrastructure may be accessed via reference points I6, and I13, Similarly operational management happens at reference point I8 and I9
- Both C2C OSS and Telco SPP may need to interoperate and provide respective interfaces at reference point I11. Similarly, I10, I12 and I14 are further reference points for discussing interworking of backend components.

Based on this reference model, the relations and interfaces among the subsystems and stakeholders are in discussion within the consortium.

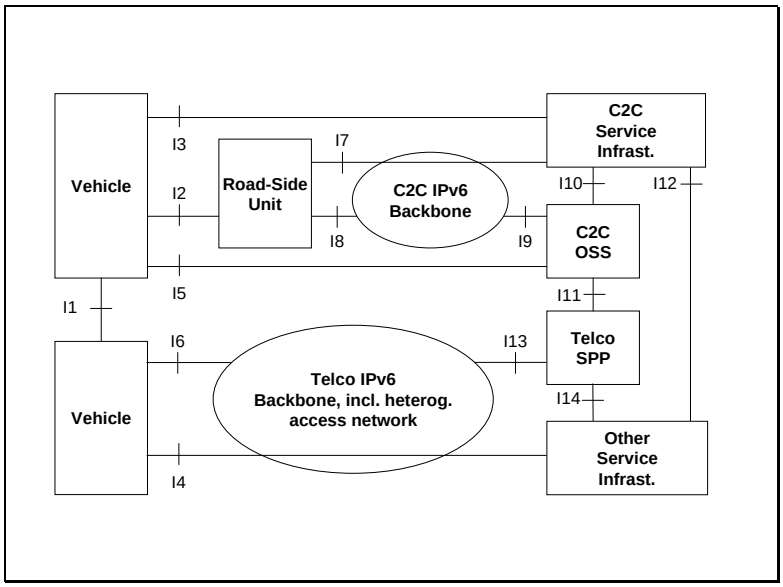

Figure 4: Draft reference model

Based on the reference model (cf. Figure 4) logical interfaces for the reference points are to be specified. Note thate there may be multiple logical/technical interfaces per reference point.

The logical interfaces described herafter focus on the communication sublayers. The core component of the vehicle is the OBU, which hosts the C2C Communication Software and hardware and may host or be connected to in-vehicle application units (AUs).

At reference point I1 communciation interfaes will most probably be based on IEEE 802.11p wireless technology adapted to European conditions (802.11p*). This interface supports all anticipated communication procedures.

At reference points I2 to I6 communication interfaces will most probably be based on IEEE 802.11 a/b/g/n radio technology.

4.2 Basic Communication Principles

Based on short-range wireless communications, the C2C Communication System is founded on two main communication principles:

- It provides a spatial and timely dissemination of information among vehicles. The information dissemination is particularly suited for road safety, but not limited to these applications.

- The C2C Communication System provides a message delivery similar to conventional packet-switched networks in wireless environments to mobile nodes and offers communication types similar to unicast, multicast, anycast, and broadcast in conventional networks, but adapted to vehicular environments.

While conventional communications are typically sender-centric, the C2C Communication System distinguishes between receiver-centric and sender-centric dissemination of information:

- With *receiver-centric dissemination*, a source node detects a hazard by its local sensors and distributes information to its neighbors. Neighbors merge information with their local information state and re-distribute the aggregated information to their neighbor nodes. Spatial and timely distribution of the information is controlled by the receiving node that acts as a forwarder: Upon reception, it determines the relevance of the information for its neighbors and decides whether the information should be re-distributed or not.
- With *sender-centric dissemination*, a source node defines a geographical area and forwards the information to all neighbors. On reception, a neighboring nodes checks whether it is located in the defined geographical area and re-broadcasts the message.

4.3 Architecture Perspective of Individual Components

This section briefly describes the individual components in the C2C Communication System architecture. For every component, its main properties and relations to other components are described. These components can interact in different ways and some examples will be given. The C2C Communication System distinguishes between a basic configuration and extended configuration for OBUs and RSUs. The C2C-CC basic system must include a minimum set of functionalities required to support active safety cooperative applications, while the C2C Communication extended system may include on top of the basic system other functionalities and applications.

The described components are:

- Application unit (AU),
- On-board unit (OBU),
- Road-side units (RSU),
- Other entities outside the scope of the C2C-CC.

4.3.1 Application Units

An Application Unit (AU) is an in-vehicle entity and runs applications that can utilize the OBU's communication capabilities. 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.

An AU can also be built into a vehicle (embedded) and be permanently connected to an OBU. This ensures that a minimal set of applications are always executed in the vehicle. Another type of AUs can dynamically be plugged into the in-vehicle network, for example a passenger's PDA. A portable AU should be automatically configured when connected to an OBU. Similarly an AU can dynamically be removed, for example when a passenger leaves a vehicle. Multiple AUs can be plugged in with a single OBU simultaneously and share the OBUs processing and wireless resources.

The C2C-CC foresees the usage of IPv6 by AUs, even if IPv4 should be implemented and supported in the OBUs for back-compatibility with relatively old portable AUs. This implies that an AU has dynamically configured IPv6 addresses and Internet applications running on an AU can utilize standard interfaces of the IPv6 protocol stack. An AU communicates solely via the OBU, which handles all mobility and networking functions on the AUs' behalf. The distinction between an AU and an OBU is only logical and an AU can be physically co-located with an OBU.

The need for an Application Context Manager is expected. For example if the C2C Communication Network Layer reveals that a vehicle is approaching with high velocity, the relevant safety application would be informed and potentially warns the driver. If the information about approaching vehicles needs to be distributed to multiple applications simultaneously, which use the same information for a different purpose (such as *extended brake light* and *intersection warning*), the context manager could efficiently notify all applications.

4.3.2 On-Board Unit (OBU)

The On-Board Unit (OBU) is responsible for CAR 2 CAR and CAR 2 Infrastructure communications. It also provides communication services to AUs and forwards data on behalf of other OBUs in the ad hoc domain. An OBU is equipped with at least a single network device for short range wireless communications based on IEEE 802.11p* radio technology. This network device is used to send, receive and forward safety-related data in the ad-hoc domain. An OBU can be equipped with more network devices, e.g. for non-safety communications, based on other radio technologies like IEEE 802.11a/b/g/n.

OBU functions and procedures include wireless radio access, geographical ad hoc routing, network congestion control, reliable message transfer, data security, IP mobility support, and others.

An OBU can be categorized as Public Safety OBU when it can execute specific applications authorized to send data with highest priority.

The C2C Communication basic system of an OBU comprises a minimum set of safety applications, the C2C Communication protocol stack with C2C Communication transport and network layer, the radio protocols with the IEEE 802.11p* device, and an interface to the local sensors of the vehicle. Possible extended configuration includes other safety and non-safety applications and optional network interfaces.

4.3.3 Road-Side Unit (RSU)

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

Main functions of a RSU are[3]:

- extending the communication range of an ad hoc network by means of re-distribution of information to an OBU when the OBU enters the communication range of the RSU. This functionality includes the case that a RSU directly forwards data in a wireless multi-hop chain with vehicles. **(**Figure 5)
- possibly running safety applications, such as for Vehicle 2 Infrastructure warning (e.g. low bridge warning work-zone warning), intersection controller, or virtual traffic sign, and act as information source and receiver, respectively (Figure 6).
- possibly providing Internet connectivity to OBUs (Figure 7).

- possibly cooperating with other RSUs in forwarding or in distributing safety information

The case in Figure 5 also represents the basic usage of a RSU, where a RSU provides minimal forwarding functionality. The cases in Figure 6 and Figure 7 are configurations for the extended usage of RSUs.

[3] The order does not imply priority.

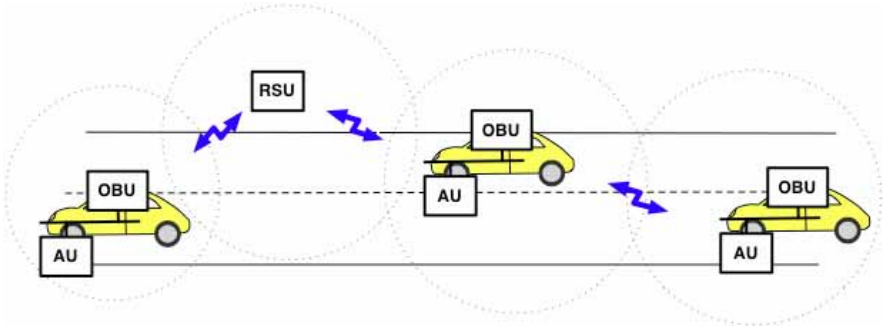

Figure 5 A RSU extends the communication range of OBU by forwarding of data

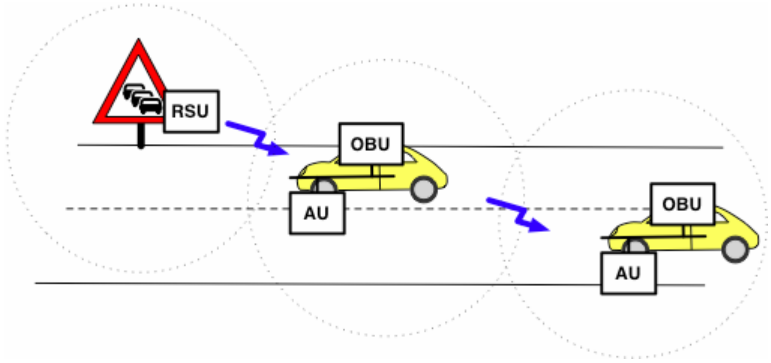

Figure 6 A RSU acts as information source

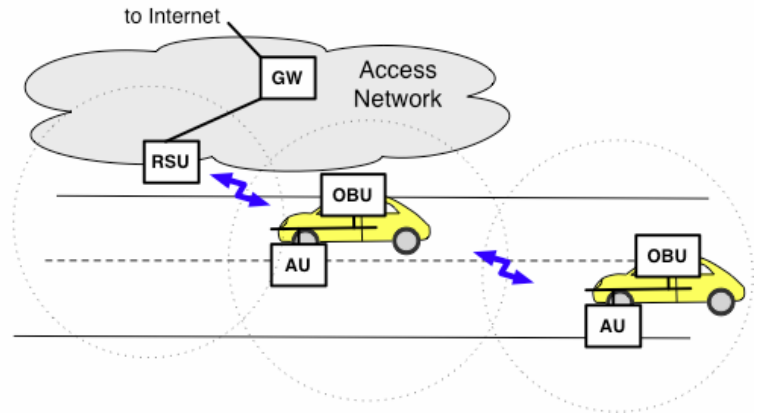

Figure 7 A RSU provides Internet access

4.3.4 Entities Outside the Scope of the CAR 2 CAR Communication Consortium

Numerous network entities, typically as part of the infrastructure domain, are outside of scope of the C2C Communication Consortium. Examples for such entities are public hot spots, instances of a Mobile IP infrastructure like Mobile IP Home Agents in the Internet, application servers, and control centers.

4.4 Layers' Architecture and Related Protocols

The C2C Communication Layers' architecture of an OBU is shown in Figure 8. The C2C-CC principally distinguishes among three basic types of radio wireless technologies: *IEEE 802.11p** wireless technology[4], conventional wireless LAN technologies based on *IEEE 802.11a/b/g/n*, and *other radio technologies* (like GPRS or UMTS). On top of the radio layers MAC and PHY of the specific wireless technologies, the *network layer* provides wireless multi-hop communications based on geographical addressing and routing, and executes functions specific to vehicular communications like congestion control and vehicles' movement dissemination (beaconing).

In eventual implementation, separate MAC layers may be combined into one, and C2C Network may also access certain other radio types.

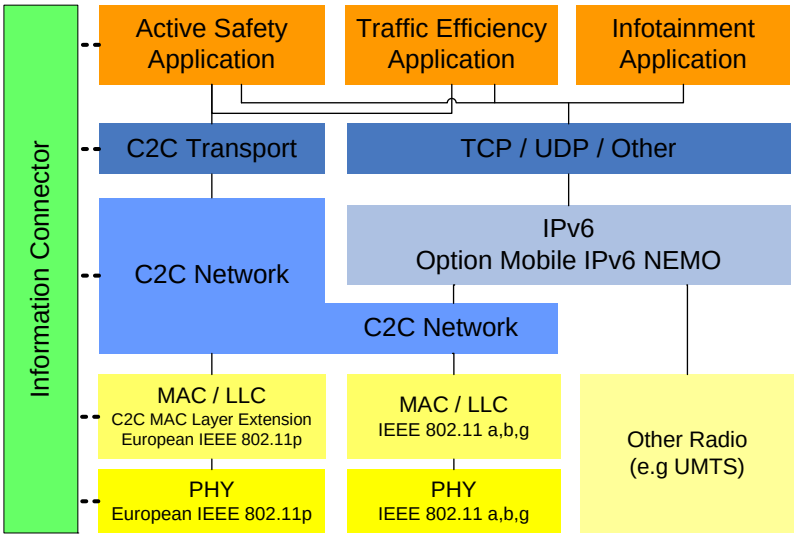

Figure 8 Protocol architecture of the C2C Communication System

As it can be seen in the protocol architecture, non-safety applications use the traditional protocol stack with TCP and UDP (or an alternative transport protocol) over IPv6 and can access wireless multi-hop communications to communicate with other applications in vehicles, road-side unit or Internet nodes. Non-safety applications can also bypass the C2C Communication Network Layer and transceive data via the IEEE 802.11a/b/g network interfaces, for example for direct communications with WIFI hot spots.

[4] IEEE 802.11p* refers to a variant of IEEE 802.11p adapted to the European conditions.

Opposed to non-safety applications, safety applications regularly communicate with the left-side column of the protocol stack via the C2C Communication Transport and Network Layers, and the IEEE 802.11p* physical [2] and IEEE 1609.4 MAC layer extensions as part of the IEEE 1609 standard family [3][4] [5][6]. The C2C Communication *Transport Layer* provides several services to safety applications, such as data multiplexing and de-multiplexing, and may also offer unicast-based connection-oriented, reliable data transfer according to the requirements of the safety applications. A particular additional task of the C2C Communication Transport Layer is to combine data from different applications in order to carry them in the payload of a single packet and deliver them to the applications on the receiving side. The C2C Communication *Network Layer* provides wireless multi-hop communications based on geographical addressing and routing. Main components of the geographic routing protocol executed in the network layer are beaconing, location-service, and forwarding of data packets. Different forwarding schemes are supported for unicast- and broadcast.

Safety applications, however, are not restricted to use the C2C C Transport and Network Layers over the IEEE 802.11p*-based wireless interface. As shown in Figure 8, non-critical safety applications may also transceive data via regular IEEE 802.11a/b/g or other wireless technologies, typically to access servers in the infrastructure domain and sharing the wireless resources with non-safety applications. It is worth noting that applications may use both communication types simultaneously, or in sequence. For example, a safety message can be sent as a geographical broadcast from a RSU in order to warn approaching drivers of a road work zone. This message may include an IP address identifying a server in the Internet which provides additional information about the road work zone. Passengers in the vehicles may then retrieve additional information via conventional IP-based communications from the server.

Another particular module in the OBU's protocol architecture in Figure 8 is the *Information Connector* (IC). Its main task is to provide through a mechanism the cross-layer data exchange among the different layers of the protocol stack in an efficient and well-structured manner. This can be, for example, achieved via a publish-subscribe mechanism that asynchronously informs subscribed instances. This information exchange is dealing with un-interpreted raw data.

4.4.1 C2C Communication Application Layer

The C2C Communication Application Layer provides common application services to application processes, including maintenance of local data bases, sending and receiving procedures of messages, processing of messages and local sensor data of the vehicle, and others. Applications can interact with users (drivers and passengers by human-machine interfaces) and with local sensor data in the vehicle (typically via the CAN-bus interface).

The C2C Communication Basic System comprises a set of applications that are mandatory in every vehicle. Other applications, however, can be installed and executed (extended system).

4.4.2 C2C Communication Network Layer

The C2C Communication Network Layer provides protocols for data dissemination to VANET applications. Due to the limited wireless bandwidth, flooding (i.e. each node forwards any received packet) in a wireless ad hoc network has to be scoped in its range. In the C2C Communication Network Layer the dissemination of safety information can be restricted to an area of relevance defined by the originator of the information. This can be achieved in a way that data packets are relayed towards the target area and once reached the geographical target area are efficiently disseminated to all vehicles inside the target area.

Unicast data packets are forwarded from the source to the destination via multi-hop communications. The routing algorithms defining the path through the vehicular ad hoc network can use nodes' movement and position data to deal with the fast changes in the network topology ("geounicast").

The C2C Communication Network Layer copes with all possible densities of equipped vehicles. In the early morning or at night time the density of vehicles may be low such that an equipped vehicle only sporadically finds other equipped vehicles in its communication range. After a potential full market introduction many equipped vehicles can be close together, for example in a big traffic jam. Efficient dissemination and unicast protocols must work reliably and efficiently in all scenarios. In order to meet the requirements in both dense and sparse vehicle densities, the network layer provides appropriate algorithms and schemes, but it is clear that in the first phase of deployment of C2C-CC systems, a very important role will be played by an efficient supporting ad hoc infrastructure.

The C2C Communication Network Layer defines three data delivery scheme:

- With event-driven *geographical broadcast* data packets are distributed to all nodes within a geographical area efficiently and reliably. Geographical broadcast is mainly intended for applications that simply distribute data within a sharply defined geographic area (packet-centric dissemination). The targeted area can be around the source node, but it can be located far away. In the latter case, the packet is first sent towards the target area. Then, in the target area the packet is flooded in order to disseminate the information.
- With event-driven *single hop broadcast*, a data packet is distributed from one OBU to all its neighboring OBUs and RSUs in direct wireless communication range. Single-hop broadcast is preferred for applications that disseminate information and aggregate the information on every wireless hop (information-centric dissemination).

- The *beacon packets*[5] are a specific case of single-hop broadcast, which are periodically sent by the C2C Communication Network Layer can carry additional application data by means of piggybacking. It is discussed whether beacons could also be broadcasted over 2 or more hops using dedicated multi-hop broadcast algorithms, in particular when active safety application requirements are strict and necessary in highly mobile environments.

Some algorithms can be implemented at the network layer in order to control the network congestion; for example, transmission interval control can be applied for dynamically reducing the network layer beacon rate when the network density is too high. Congestion control mechanism may involve cross-layer aspects, for example the C2C Communication MAC Layer can provide state information of the wireless channel to the C2C Communication Network Layer and applications for congestion control.

4.4.3 MAC/LLC Layer

The specification of the C2C Communication MAC Layer is currently under discussion. This section describes selected design principles that have been identified as fundamental in the C2C Communication Consortium.

The service access point between LLC and the C2C Communication Network Layer shall be specified. The actual LLC functionality might be passive, but the role is to provide uniform access point to network layer.

The C2C-CC MAC layer is based on the IEEE 802.11 MAC protocol as specified in [7] but with many simplifications in the services and some enhancements in the cross-layer integration. The adopted MAC algorithm is the standard *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA).

Power management and roaming (i.e. access point scanning) are not supported. All the IEEE 802.11 services for nodes, including authentication, de-authentication and privacy, except data delivery, are not included. In particular, the C2C Communication MAC Layer defines a single ad-hoc network where all nodes that conform to the C2C-CC standard are members without the need for any association procedure. Therefore, referring to IEEE 802.11 terminology, all nodes are considered a priori members of a single independent basic service set (IBSS).

With respect to congestion control, the C2C-CC has identified as necessary the following features not included in the 802.11 standard:

- The MAC layer should provide the upper layers with information about the current estimated channel load. According to this information, upper layers apply different

[5] Beacons in the context of the C2C Communication are network-layer messages and should not be confused with management frames defined in the IEEE 802.11 standard, which are also referred to as beacons.

strategies to prevent medium congestion (e.g. applications decide depending upon the priority whether they can transmit or not),

- The LLC sublayer should provide the network layer with a per-packet parameters control, in particular regarding the transmission power,
- A client/server interface for channel observation and control commands between the MAC layer and all the upper layers is required,
- The MAC layer should implement a differentiated queuing scheme according to the priority of the message as specified by the applications, e.g. as specified in IEEE802.11e.

4.4.4 Physical Layer[6]

The design principles of the C2C Communication Physical Layer are described in Section 6. From the architectural point of view, the C2C Communication Consortium considers the upcoming IEEE 802.11p (Wireless access in vehicular environments – WAVE) radio technology, directly derived from the IEEE 802.11a one, but with modifications and amendments for adapting it to vehicular environments, like no usage of association/authentication, usage of specific transmit power and of multiple channels with different bandwidth per channel than defined in the IEEE 802.11a standard. However, basic algorithms and modulation schemes are unchanged.

[6] The spectrum proposed by C2C-CC and ETSI is in the frequency range from 5,875 to 5,925 GHz. However, there is no effectively protected bandwidth assigned by ECC to ITS services yet. Therefore, no decision has been taken on spectrum use by C2C-CC so far.

5 Applications

Chapter 2 describes example use cases in order to describe benefits of CAR 2 CAR Communication and indicate its potential with regard to safety, traffic efficiency, and comfort. This chapter covers the complete application range of CAR 2 CAR Communication in the scope of the C2C-CC. Use cases are assigned to six “applications” based on their requirements of security and types of information exchange. Consequently, the applications are defined to provide generic mechanisms for use by any number of use cases. The following describes the requirements and generic mechanisms for each application.

The following sections define the applications and the functionality provided by each application. Currently, the applications are separated with no interfaces between them but with a standardized interface to the transport layer (*C2C-CC Transport* and *TCP/UDP/Others*) and the Information Connector (see chapter 4.4). Control of information in each application shall be done by the vehicle systems.

A basic C2C-CC system shall possess the application instances shown in Table 1 according to the C2C-CC definition. The application instances marked “RSU” and “OBU” below are C2C-CC Roadside Units and on board units respectively. A blank entry indicates that the instance is not required.

Table 1 C2C-CC Basic Application instance requirements for vehicles

Application	Application Instance	Required as C2C-CC Basic*
Vehicle 2 Vehicle Cooperative Awareness	Sender	OBU
	Receiver	
	Vehicle Systems	
Vehicle 2 Vehicle Unicast Exchange	Initiator	
	Responder	OBU
	Vehicle System	
Vehicle 2 Vehicle Decentralized Environmental Notification	Detector	
	Sender	OBU
	Receiver	OBU
	Message Management	OBU
	Vehicle System	
Infrastructure 2 Vehicle (One-Way)	RSU System	RSU
	Sender	RSU
	Receiver	

	Vehicle System	
Local RSU Connection	RSU System	RSU
	Sender	RSU
	Receiver	
	Vehicle System	
Internet Protocol Roadside Unit Connection	RSU Router	RSU
	Client	
	Server	RSU
	Vehicle System	

*Note: OBU = on board unit, RSU = roadside unit

5.1 Vehicle 2 Vehicle Cooperative Awareness

This application supports the requirement for vehicles to share information with each other without any persistent communication link between the vehicles. The general requirements are summarized in Table 2. Vehicles share information by broadcasting or geocasting data to all surrounding vehicles or to vehicles within a geographic region, respectively.

Table 2 General capabilities for V2V Cooperative Awareness

Communication Type	Broadcast, Geocast
Communication Range	300 meters to 1 kilometer
Roadside Units	N/A
Security	V2V Trust

5.1.1 Application Instances

As shown in Figure 9, this application contains three application instances, Sender, Receiver, and Vehicle System.

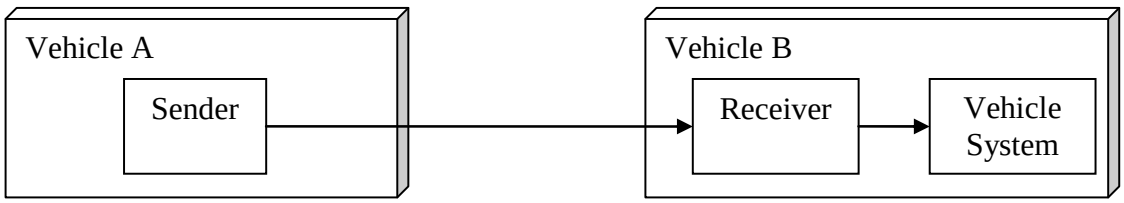

Figure 9 Application Instances for Vehicle 2 Vehicle Cooperative Awareness

5.1.2 Sender

The *Sender* shall:

- consolidate the local vehicle data required by the corresponding use cases
- package the local vehicle data into a message
- use a broadcast or geocast mechanism to send the message to all surrounding vehicles.

5.1.3 Receiver

The *Receiver* shall:

- authenticate messages received from the *Sender*
- decode the messages into remote vehicle data
- evaluate the contents of the messages according to use case requirements.

5.1.4 Vehicle Systems

The output from the *Receiver* is passed to the *Vehicle Systems* application instance. From here, the results of the *Receiver* are acted on as appropriate for the use case.

5.1.5 Messages

The messages for this application will be defined after use case requirements are captured and consolidated.

5.1.6 Example

As an example, the *Cooperative Forward Collision Warning* use case will be described. The Sender application instance should send all data as required. The Receiver application instance will execute an algorithm to assess the threat of the other vehicle with respect to its own vehicle. The algorithm will use data sent by the Sender as well as data from the local vehicle. If the algorithm detects a potential forward collision, the Receiver will communicate this result to the Vehicle System. The Vehicle System will deliver a warning to the driver (e.g., auditory, visual, and/or haptic).

5.1.7 Use Cases

ID 3031: V2V Merging Assistance

ID 4020: Cooperative Forward Collision Warning

ID 1100: Emergency Electronic Brake Lights

ID 2040: V2V Lane Change Assistance

ID 1010: Approaching Emergency Vehicle Warning

ID 4050: Highway/Rail Collision Warning

ID 3101: Wrong Way Driving Warning

ID 2070: Cooperative Glare Reduction

ID 2120: Cooperative Adaptive Cruise Control

5.2 Vehicle 2 Vehicle Unicast Exchange

This application enables a communication link between two vehicles for exchange of information. The application consists of four different phases: *Discovery*, *Connection*, *Maintenance*, and *Closure*. The Discovery Phase is the phase when one of the vehicles decides to connect to another vehicle. This decision process will likely use information from any number of other use cases along with an algorithm for deciding to initiate the next phase. In the subsequent Connection Phase one vehicle initiates a request to the other vehicle to open a connection. The other vehicle must decide whether or not to allow the connection. The Maintenance Phase is when the two vehicles are exchanging data while keeping the connection open. The Closure Phase is when one of the two vehicles decides to stop exchanging data and closes the connection.

The phases listed above have implications on the underlying communication layers and how they behave. For example, a communication link between the two vehicles might require the communication system to use a different communication channel. Details such as these should be transparent to the applications and should be addressed by the lower communication layers.

The general requirements are summarized in Table 3.

Table 3 General capabilities for V2V Unicast Exchange

Communication Type	Unicast
Communication Range	0 meters to 5 kilometers
Roadside Units	N/A
Security	V2V Trust

5.2.1 Application Instances

Figure 10 shows the application instances for Vehicle 2 Vehicle Unicast Exchange. This application should use a lightweight, connection-orientated transport layer protocol which builds a robust reliable communication link between Initiator and Responder (vehicles A & B) within the ad hoc network.

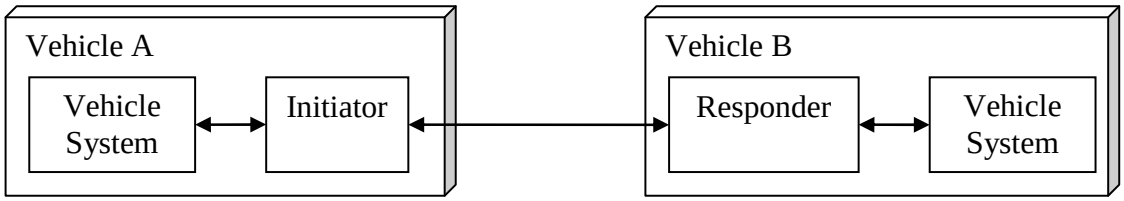

Figure 10 Application instances Vehicle 2 Vehicle Unicast Exchange

5.2.2 Initiator

The Initiator shall utilize information from the communication system and Vehicle System to execute the Discovery Phase.

When the Initiator has identified a vehicle with an available service of interest to its Vehicle System, the initiator shall send a connection request to the communication system for a connection to the Responder.

Once the connection is established, the Initiator shall execute the duplex or bi-directional communications protocol required for the implementation of the use case. This includes packaging of Vehicle System information into messages and sending the messages at the appropriate times.

The Initiator shall request information from and send information to the Vehicle System as appropriate for the use case.

The Initiator may close the connection at any time.

5.2.3 Responder

The Responder shall reply to all connection requests with either acceptance or declination. The decision to accept or decline will likely be enabled by information from the Vehicle System.

When a connection is established with an Initiator, the Responder shall execute the duplex or bi-directional communications protocol required for the implementation of the use case. This includes packaging of Vehicle System information into messages and sending the messages at the appropriate times.

The Responder shall request information from and send information to the Vehicle System as appropriate for the use case.

The Responder may close the connection at any time.

5.2.4 Vehicle System

The Vehicle System shall notify the communication system of the services that it will provide.

The Vehicle System shall interact with the Initiator or Responder to provide the proper information for transmission to support the use case.

The Vehicle System shall receive information from the Initiator or Responder and act appropriately for the use case.

5.2.5 Messages

In general, the messages required are:

- Connection request/acceptance/declination message
- General data exchange message
- Error and flow control messages (to ensure data integrity and delivery)
- Channel closure message

5.2.6 Example

One example of this application is for the use of *Pre-crash Sensing*. The Vehicle System notifies the communication system of support for the Pre-crash Sensing use case. This allows the communication systems of surrounding vehicles to know that the service is available. When the Vehicle System in Vehicle A detects that a collision with Vehicle B is unavoidable, the Vehicle System requests from the Initiator a communication link to Vehicle B. The Initiator knows whether or not Vehicle B supports the Pre-crash Sensing use case by monitoring the list of available services from the communication system. Since Vehicle B supports pre-crash sensing, the Initiator of Vehicle A sends a request to its communication system to open up a connection to Vehicle B. The communication system is assumed to make the connection according to lower-layer standards. Once the connection is established, the Initiator shall issue a request for relevant information (e.g., vehicle mass, bumper height) from the Responder. The Responder will reply with the information which can then be used by Vehicle A to prepare for the unavoidable crash.

5.2.7 Use Cases

ID 3010: Pre-Crash Sensing/Warning

ID 3031: V2V Merging Assistance

ID 3170: Cooperative Vehicle-Highway Automation System (Platoon)

ID 2080: Instant Messaging

5.3 Vehicle 2 Vehicle Decentralized Environmental Notification

This application provides information about events and roadway characteristics that are probably interesting to vehicles or drivers for a certain time in a certain area. Most prominent is the ability of this application to support the Hazard Warning use case. Vehicle 2 Vehicle denotes the main communication link for information dispersal. Information is distributed in a decentralized network of communication nodes without central intelligence. Nevertheless RSUs behave within this information network like standing vehicles. They store, cluster, prioritize, and repeat received information or might add or remove messages. Because the communication mechanisms stay the same the integration of RSUs does not result in another application.

Several characteristics distinguish this Application from others:

- The temporal validity of the information might be much higher than the time needed for forwarding the information in an ad-hoc network (e.g., up to some minutes).
- The distribution area exceeds the communication range of a single-hop system.
- Information about the same event may be originated by numerous originators (e.g. traffic jam end).
- Information may be originated by previously unknown originators.
- Information from various originators or information about various events may have different reliability. The reliability is set by the originator together with the information.
- Information origination and communication links can not be guaranteed.

The first two characteristics indicate that the information should be spread in a network using fast forwarding mechanisms, such as geocast. Additionally, the application must collect and store information in order to distribute it to other vehicles when they are encountered. The latter mechanism is important for vehicles entering the relevant area later on while the information is valid and in order to maintain the information in networks with a low density of equipped vehicles (i.e., no continuous ad-hoc network exists but vehicles meet occasionally and exchange data).

Given the long temporal validity of information for some use cases, high latency given by the distribution algorithms may be acceptable; however it should be reduced if possible.

Information may not be altered by a forwarding communication unit however a forwarding communication unit might dismiss information without forwarding. Information dismissal may occur when:

- A forwarding communication unit identifies information to be implausible due to own information. This requires that the application layer of a forwarding communication unit has to have this information and has to be able to interfere with the further distribution.
- The redundancy of the information exceeds some threshold. This requires that the system maintain a concept of redundancy when information from a number of origins is available.

The general requirements are summarized in Table 4.

Table 4 General capabilities for V2V Decentralized Environmental Notification

Communication Type	Broadcast, Geocast
Communication Range	300 meters to 20 kilometers
Roadside Units	Not required but can aid applications
Security	Originator Trust

5.3.1 Application Instances

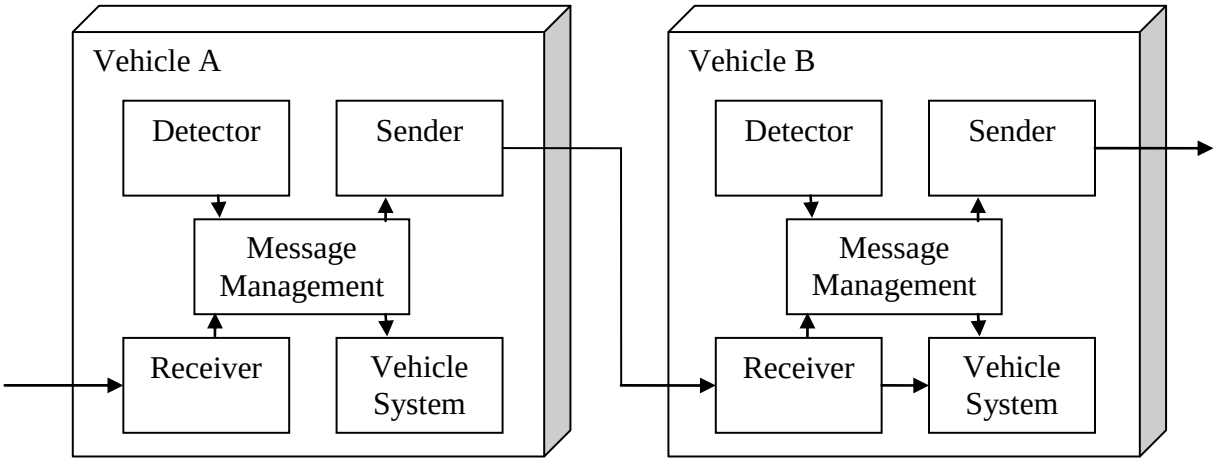

Figure 11 Application instances for Vehicle 2 Vehicle Decentralized Environmental Notification

5.3.2 Detector

The Detector shall:

- detect a mandatory set of hazardous events/locations based on basic vehicle data available in all vehicles (e.g., crash, emergency braking, breakdown / warning lights, traffic jam inflow, fog start = fog light & speed reduction)
- optionally detect additional events and roadway information based on advanced vehicle data (e.g., low friction, obstacle detection, wind, slopes, sharp road bends)
- (for infrastructure systems) detect hazardous events and roadway information from existing infrastructure sensors on the roadway (e.g., induction loops, visibility sensors, wind sensors at bridges)
- detect position of events or information
- compile a message including parameters for distribution (e.g., priority, validity), authentication data (e.g., signature), position, and event or roadway information description using the standardized hazard type scheme

5.3.3 Sender

The Sender shall

- use a broadcast or geocast mechanism to send the message to surrounding vehicles or vehicles in a geographic region.

5.3.4 Receiver

The Receiver shall:

- decode the messages
- check validity (i.e., authentication, expiry, plausibility of distribution parameters) of received messages and dismiss any invalid messages

5.3.5 Message Management

The Message Management shall

- store messages
- cluster messages describing the same event or roadway information based on the standardized hazard type scheme
- identify redundant event detections
- optionally check plausibility of clustered information based on own vehicle data (e.g., high speed at reported traffic jam), dismiss implausible messages, and send negative message
- prioritize clustered information for distribution and pass messages with highest priority to Sender
- identify relevant clustered information for the own vehicle
- pass relevant clustered information to the Vehicle System

5.3.6 Vehicle System

The Vehicle System shall

- prioritize clustered information received from Message Management
- inform or warn the driver of the vehicle early before approaching the position for which information is available

5.3.7 Messages

The messages contain information about events or road conditions. Note that road conditions can be static or dynamic, (e.g., black ice - static, traffic jams - dynamic). Each message contains information about a single event or road condition in order to distribute information independently.

Each message consists of three parts as follows:

- **Parameters for message management**: This information is used for content independent handling of the message. It contains
  - a random message ID which is preferably unique. Because vehicles generate message IDs independently, complete uniqueness can not be guaranteed unless it includes position and time information resulting in very long IDs. Therefore the system has to be robust against ID collisions.
  - message time stamp
  - priority
  - reliability of information set by originator
  - limits of target area
  - expiry time
  - authentication
- **Position information:** The information is needed to cluster information and to identify relevant information for the driver. Therefore, position information of different messages has to be matched and the own driving path has to be matched to the messages. In order to enable this matching, not only the event position is added to the message but also a position trace describing the path leading to the event. This trace information has to be independent from special digital maps. Preferably, matching should be possible without any map.
- **Event and road condition information:** First of all, the event or roadway information is coded using a standardized, extensible scheme. This scheme enables the Message Management to cluster information without knowledge about the meaning. Additionally, some specific information is given that can interpreted only by applications that are able to handle the specific code.

Because basic implementation of some Use Cases might be realized using Vehicle 2 Vehicle Cooperative Awareness or Infrastructure 2 Vehicle (One-Way), the message should be a compatible extension of basic messages used there (i.e., position information event type coding). For example, the Vehicle 2 Vehicle Decentralized Environmental Notification might distribute information about a slow driving vehicle on a highway section in a wide area while Vehicle 2 Vehicle Cooperative Awareness distributes information about the slow driving vehicle to vehicles in the direct vicinity.

5.3.8 Example

Decentralized Floating Car Data and Hazard Warning are the most prominent use cases for Vehicle 2 Vehicle Decentralized Environmental Notification. The Detector detects events like traffic incidents or

dangerous situations. To avoid information loss, the Sender transmits the data to other vehicles for a certain time and within a certain area. Other vehicles receive the information through their Receiver. The messages are stored and presented to the driver (e.g. auditory, visual, and/or haptic) by the Vehicle System. The messages are sent to other vehicles by using the Message Management and the Sender.

5.3.9 Use Cases

ID 1011: Slow Vehicle Warning

ID 6010: Post-Crash Warning

ID 3130: In-Vehicle Amber Alert

ID 6020: Safety Recall Notice

ID 2110: Traffic Jam Ahead Warning

ID 1120: Hazardous Location V2V Notification

ID 6170: Safety Service Point

ID 2160: Decentralized Floating Car Data

5.4 Infrastructure 2 Vehicle (One-Way)

This application supports the communication from roadside units (RSUs) to vehicles without a persistent communication link between vehicles and RSUs. The general requirements are summarized in Table 5.

Roadside units broadcast information to all surrounding vehicles.

Note: Not every communication with infrastructure falls under this application. This application neither builds up a 2-way communication link nor does it receive or forward hazard warnings. This would be done through the application *Vehicle 2 Vehicle Decentralized Environmental Notification* of which a receiver and a sender instance are running on a RSU that is seen as a “fixed position vehicle”.

Table 5 General capabilities for Infrastructure 2 Vehicle (one-way)

Communication Type	Broadcast, geocast
Communication Range	300 meters to 5 kilometers
Roadside Units	Required

Security	Vehicle must trust RSU

5.4.1 Application Instances

As shown in Figure 12, this application contains four application instances: RSU System and Sender on the RSU side, Receiver and Vehicle System on the vehicle side.

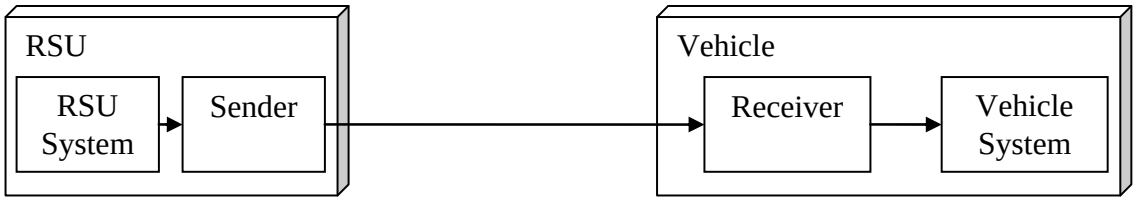

Figure 12 Application instances for Infrastructure 2 Vehicle (one-way)

5.4.2 RSU System

The RSU System may consist of a Human Machine Interface (HMI), communications interface to a larger network, or sensors for configuring the RSU or obtaining real-time data. This application instance may also contain some logic for determining the content of the message to send.

5.4.3 Sender

The RSU Sender shall

- package the data into a message.
- use a broadcast mechanism (broadcast, geocast) to send the message to all surrounding vehicles.

The message type and broadcast mechanism shall be appropriate for the use case being supported.

5.4.4 Receiver

The Receiver shall:

- authenticate messages received from the *Sender*
- decode the messages into remote RSU data
- evaluate the contents of the messages according to use case requirements.

5.4.5 Vehicle System

The output from the Receiver is passed to the Vehicle Systems application instance. From here, the results of the Receiver are acted on as appropriate for the use case.

5.4.6 Messages

The detailed format of the messages is defined within the message protocol specification. The repetition rate varies depending on the message content. Changing content that has to be given to vehicles at the edge of the communication range (e.g., phase information has to be repeated periodically). Fixed content that has to be given to each passing vehicle at least once (e.g., POI notification) can be repeated less frequently.

5.4.7 Example

An example is the broadcast of speed limits. Consider a dynamic speed limit sign showing different limits according to the time of the day or on special occasions like traffic jams. The RSU System will determine the appropriate speed limit according to its internal time table and traffic conditions. The RSU Sender application instance will periodically broadcast a message containing the speed limit. If appropriate, the message will contain additional information regarding the speed limit such as its geographic or directional limits.

The Receiver application instance will compare any geographic or directional limits in the message with the vehicle data to determine if the speed limit applies to the local vehicle. If so, the application instance will compare the received speed limit with the actual vehicle speed. Any speed limit violation will be communicated to the Vehicle System. The Vehicle System will deliver a warning to the driver (e.g., auditory, visual, and/or haptic).

5.4.8 Use Cases

ID 1121: Hazardous Location I2V Notification

ID 6150: Green Light Optimal Speed Advisory

ID 2180: V2I Traffic Optimization

5.5 Local RSU Connection

This application supports use cases where data between a vehicle and a RSU needs to be sent from the vehicle to the RSU or bi-directionally. Once service discovery is complete, the vehicle and the RSU will interact by exchanging messages between each other. The RSU will not directly route messages to another network (i.e., no Internet Protocol routing). However, this application does allow the RSU to be connected to and interact with another network. The general requirements are summarized in Table 6.

Table 6 General capabilities for Local RSU Connection

Communication Type	Unicast
Communication Range	0 meters to 1 kilometer
Roadside Units	Required
Security	RSU/OBU must trust each other

5.5.1 Application Instances

As shown in Figure 13, this application contains four application instances, RSU System, Sender, Receiver, and Vehicle System.

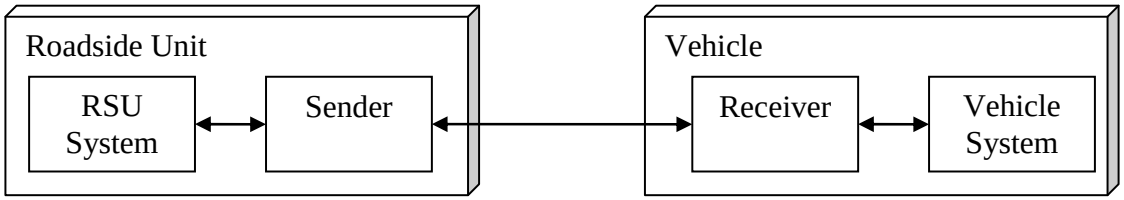

Figure 13 Application instances for Local RSU Connection

5.5.2 RSU System

The *RSU System* may consist of a Human Machine Interface (HMI), communications interface to a larger network, or sensors for configuring the RSU or obtaining real-time data. This application instance may also contain some logic for determining the content of the messages to send.

5.5.3 Sender

The Sender shall:

- authenticate OBU messages
- be readily identifiable as an RSU
- respond to service discoveries
- implement all services listed
- implement a robust communications protocol

5.5.4 Receiver

The Receiver shall:

- authenticate RSU-originated messages
- identify and select RSU(s) suitable for local connection
- initiate Service Discovery with a suitable RSU
- implement a robust communications protocol
- manage connections (e.g., handover) with suitable RSU(s) as required

5.5.5 Vehicle System

The Vehicle System shall provide information to and receive information from the Receiver.

The information transmitted between the two entitites may be used in an interface to the driver.(e.g., auditory, visual, and/or haptic).

5.5.6 Messages

The messages depend on the specific use cases. The detailed format of the messages is defined within the message protocol specification.

5.5.7 Example

Two examples that utilize this type of application have been included below, the Local Directory Fetch and the Emergency Vehicle Signal Preemption, to demonstrate both commercial and safety related use cases.

5.5.7.1 Local Directory (Fetch)

Consider an RSU which contains a large non-volatile memory suitable for storage of information in multiple languages relevant to its locale. Content stored on such an RSU could include local service information, points of interest, mapping data, event information, rich media, etc.

Having identified the presence of an RSU which supports a local directory service, the local directory service client which drives the HMI from the OBU requests a content index or registry from the RSU. Upon receipt of the content index, the local directory service client applies a filter identifying specific content of interest to the vehicle's occupants (e.g., Restaurants – Italian). The local directory service client then requests content from the RSU based on the filter and presents these in an appropriate way to the occupants. Please note that this example includes several steps that apply to this use case.

5.5.7.2 Emergency Vehicle Signal Preemption

Consider an RSU connected physically to a traffic signal controller at an intersection. Such a unit could support a number of traffic signal related use cases including *Signal Violation Warning* or *Signal Preemption*. The following example focuses on a specific use case *Emergency Vehicle Signal Preemption*.

An emergency vehicle (police, fire, ambulance etc.) enters communication range of an RSU and its OBU indicates the presence of an RSU which supports signal preemption. With the emergency vehicle's lights and or siren enabled, the OBU automatically issues a signal preemption request to the RSU. The Vehicle System provides a signal to the driver when signal preemption is granted. Note that since accidents involving emergency vehicles are common, service operators may be required to maintain a log of preemption requests and grants to the RSU in order to determine liability in the event of an accident.

5.5.8 Use Cases

ID 6080: Automatic Access Control

ID 5040: Personal Data Synchronization at Home

ID 3030: Infrastructure-based Cooperative Merging Assistance

ID 5070: Remote Diagnostics

ID 2060: Free-flow Tolling

ID 5100: Drive-through Payment

ID 5070: Remote Diagnostics

ID 6110: Vehicle Computer Program Updates

ID 3010: Signal Violation Warning / Signal Preemption

5.6 Internet Protocol Roadside Unit Connection

This application supports services that are offered to the driver by servers located in the Internet. The communication relies on Internet Protocol (v6) and client-server paradigm. Assuming that the RSU is connected to the Internet and advertises the availability of Internet connection, the vehicle can acquire a valid address and communicate with any node in the Internet. Internet protocol security methods (like IPsec at network layer or HTTPS at application layer) are adopted to secure the communication.

The general requirements are summarized in Table 7.

Table 7 General requirements for Internet Protocol RSU Connection

Communication Type	Unicast
Communication Range	0 meters to full radio range. Can be extended using multi-hop.
Roadside Units	Required
Security	Internet security (IPsec, application layer security)

5.6.1 Application Instances

As shown in Figure 14, application instances for *Internet Protocol RSU Connection* are Receiver and RSU Router in the RSU, Client and Vehicle System on the OBU, and a Server on the Internet.

5.6.2 RSU Router

An RSU offering internet connection shall route Internet Protocol (v6) packets between the vehicle Network and the Internet. Furthermore, the RSU shall advertise the availability of internet connection to the vehicles in its vicinity.

5.6.3 Client

The software running on the OBU consists of a set of clients. Each client is responsible for a service. When the Vehicle System generates a request for a service connection, the responsible client shall check the availability of the connection (as advertised by the RSU). When the connection is available, the client connects to the predefined or advertised server.

5.6.4 Server

Servers required to support each service reside on the Internet. Servers listen for incoming connections on predefined ports. Servers can be centralized or distributed. Server addresses can be predefined or advertised by the RSU. Server ports are predefined according to the service type.

5.6.5 Vehicle System

The Vehicle System shall indicate to the client when a user or any component of the vehicle requests an internet connection. The Vehicle System shall be responsible for relaying information from the *Client* to the user or component requesting the connection.

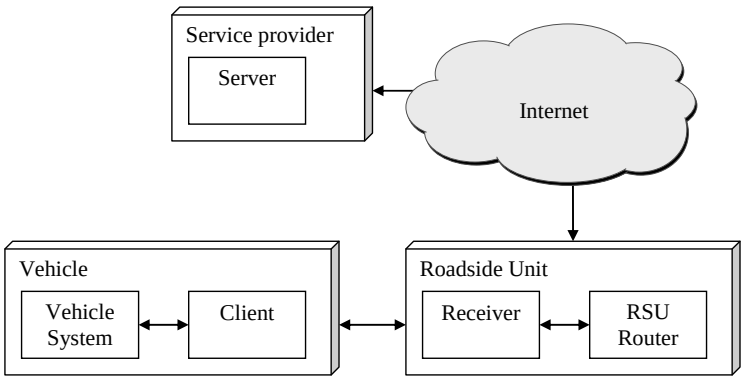

Figure 14 Application instances for Internet protocol Road Side Unit connection

5.6.6 Messages

The RSU advertises availability of an internet connection. Vehicles first acquire the internet connection, then connect to a server on the Internet. Communication takes place using standard Internet Protocol (optionally with mobility support extension) and standard transport protocol (TCP/UDP) on top of it. Following the client-server paradigm, first the vehicle client connects to a server on the internet requesting for a specific service, then, if the service is available and authorized, the communication continues as the service requires.

5.6.7 Examples

5.6.7.1 Real Time Traffic Information

The driver sets the destination in the Vehicle System. The vehicle system activates the client for the service *Real Time Traffic Information*. When internet connection is available, the Client connects to a predefined or advertised Server for traffic information and communicates the selected destination. The Server replies including fastest route, estimated travel duration, gas stations on the path, etc. The Vehicle System shows data to the driver.

5.6.7.2 In-Route Hotel Reservations

The driver sets the destination in the Vehicle System and enables the *In-Route Hotel Reservations* service, also specifying favorite features. The Vehicle System activates the Client for this service. When the internet connection is available, the Client connects to a Server whose address is predefined or advertised by the RSU (typically a local server, e.g. administrated by local tourism agencies). The Server replies including available hotels/restaurants, prices, short description. The driver/passenger can reserve a room specifying a valid identity.

5.6.7.3 Instant Messaging

The driver or passenger who wants to use the service enters credentials into the Vehicle System. When the internet connection is available, the Client connects to a predefined or advertised Server. A chat session can take place with users in the internet (e.g. family/friends at home). Using IP mobility support, the session can continue after moving to a different RSU.

5.6.8 Use Cases

ID 5010: SOS Services

ID 6030: Just-In Time Repair Notification

ID 6100: Media Download

ID 5020: Map Downloads and Updates

ID 6180: Enhanced Route Guidance and Navigation

ID 6200: Fleet Management

ID 2080: Instant Messaging

6 Radio System

6.1 General

In order to enable vehicles and the correspondent infrastructure to exchange data in an adequate manner, design principles such as main requirements, constraints and usage of deployed communication channels are specified in the following sections.

For safety applications considered in C2C-CC, the C2C-CC Radio System should be capable to transfer and receive messages stably under expected European traffic conditions. For example, vehicle speed up to 250 km/h, which might result in relative speed up to 500 km/h, should be supported by the C2C-CC Radio System. In order to fulfil these requirements, these design principles are defined.

In this document the Physical layer and the MAC/LLC layer are counted to the radio system and therefore described in this chapter.

6.2 Application Categories

In the overall scope of this document there are two types of communication channels used by the C2C-CC Radio System:

- dedicated C2C-CC Channels for
  - network control and critical safety applications (control channel CCH),
  - critical safety applications,
  - road safety and traffic efficiency applications, and
  - non-safety related car to roadside and car to car applications
- public channels as specified in the IEEE 802.11a/b/g within the frequency band allowed for Wireless LAN in Europe, in accordance with regional limitations.

In addition, a C2C-CC System may support other radio such as GSM, GPRS, UMTS, HSDPA, WiMax, 4G, which are not further described here.

Among these two types of communication channels, only the *dedicated C2C-CC Channels* are mandatory and the *normal channels* are optional for the C2C-CC Radio System.

Based on the communication channel classification above, the following rules are set:

- The network control and service announcement of the C2C-CC Radio System shall use the control channel, dedicated for network control and critical safety applications.
- Critical safety applications need robust and reliable CAR 2 CAR as well as CAR 2 Roadside Communication. The related data shall be transmitted on the protected dedicated channels for critical safety applications including the channel for network control.
- CAR 2 CAR as well as CAR 2 Roadside Communication for road safety and traffic efficiency applications shall use the corresponding dedicated channels.[7]
- Entertainment/infotainment and Internet access applications are regarded to be add-on services for the C2C-CC Radio System. These add-on services shall only operate on the non-safety related dedicated channels or the public channels. The car to hotspot communication should preferably use the public channels.

6.3 Physical Layer

The following subsections describe design principles only relevant for the *dedicated C2C-CC Channels.* The *public channels* are out of scope of these principles. In general IEEE 802.11p (Wireless Access for Vehicular Environment WAVE) is the technical basis for the C2C-CC Radio System dealing with the *dedicated C2C-CC Channels*.

Regarding the specification of the *public channels*, relevant documents such as IEEE standards should be referred [8][9][10][11].

6.3.1 Frequency Band

The following frequency band allocations for dedicated C2C-CC Channels have been requested at European Telecommunications Standards Institute (ETSI):

- 10 MHz band from 5.885 to 5.895 GHz for network control and critical safety applications (same as WAVE control channel),
- 10 MHz band from 5.895 to 5.905 GHz for critical safety applications,
- three 10 MHz bands from 5.875 to 5.885 GHz and from 5.905 to 5.925 GHz for road safety and traffic efficiency applications, and

[7] The frequency allocation for the dedicated road safety and traffic efficiency applications is still in process.

- two 10 MHz bands from 5.855 to 5.875 GHz for non-safety related car to roadside and car to car applications

For detailed information on the frequency allocation, see ETSI technical reports [12] and [13].

6.3.2 Maximum Transmit Power

Maximum transmit power allowed for the C2C-CC Radio System is 33dBm. The communication range to be achieved by the C2C-CC Radio System is 500 to 1000 m within one-hop in line-of-sight situations. A radio system with lower target communication range may have a reduced maximum transmit power.

6.3.3 Transmit Power Control

Transmit Power Control (TPC) shall be supported. This control scheme should be able to adjust the power per packet under the request of upper protocol layers.

The C2C-CC Radio shall support a dynamic TPC with a minimum transmit power of at most 3dBm.

6.3.4 Data Rates

Data rates of 3/ 4.5 / 6/ 9 / 12 / 18 / 24 / 27 Mb/s shall be supported. The default data rate shall be 6 Mb/s. Algorithms for changing the data rate have not defined yet and should be further discussed by C2C-CC WGs.

6.3.5 Antenna

The design principle on antenna beams has not defined yet. Antennas influences significantly the communication range of the C2C-CC Radio System. Based on experimental results, circular characteristic of the antenna beams seems to be best to achieve the expected performance under assumed traffic situations. At the same time, optimization of antenna characteristics for individual vehicle may be necessary, because the way of antenna installation affects the performance. For example, antennas installed in passenger room or on trunk might result insufficient performance. Best way for the installation will be on the top of roof.

6.3.6 Communication Mode and Frequency Modulation

Half-duplex and broadcast communication modes are believed to be adequate to the applications considered today. OFDM modulation scheme shall be supported.

6.4 MAC/LLC Layer

In general IEEE 802.11p [2] and IEEE1609.4 [6] are the technical basis for the C2C-CC Radio System, and the adopted MAC algorithm is the standard *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA).

6.4.1 Multi Channel Operation

According to IEEE 1609.4, all C2C-CC Radio Systems shall listen to the dedicated control channel during the control channel intervals. These are synchronized to the Coordinate Universal Time (UTC). This scheme is used to ensure, that critical safety messages are received by all devices during the control channel interval.

6.4.2 Dual Receiver Concept

C2C-CC shall support the use of dual receivers.

This concept is aimed to enable the C2C-CC Radio System to receive messages on two dedicated C2C-CC Channels simultaneously.[8] These two messages may originate from different transmitters. The use of dual receivers allows continuing listening to other dedicated channels while listening to the control channel during the control channel interval. This allows safety applications to continue their safety related communication on the other dedicated safety channels during the safety channel interval. Also other applications can continue their communication during the control channel interval, if a second receiver can listen to the control channel. This allows better utilization of the frequency band.

Dual transmitter is optional.

[8] Feasibility of this concept has been studied by computer simulation, and the results show that this concept works fine in terms of criteria such as rejection for adjacent channel signal, and so on. At the same time, some disadvantage of this concept can be identified. Currently, hardware for dual receiver is not available. Even if dual receiver chips would be available, it is expected that these have considerably higher costs than single receiver hardware. The dual receiver concept needs to be further investigated and proven in practical experiments.

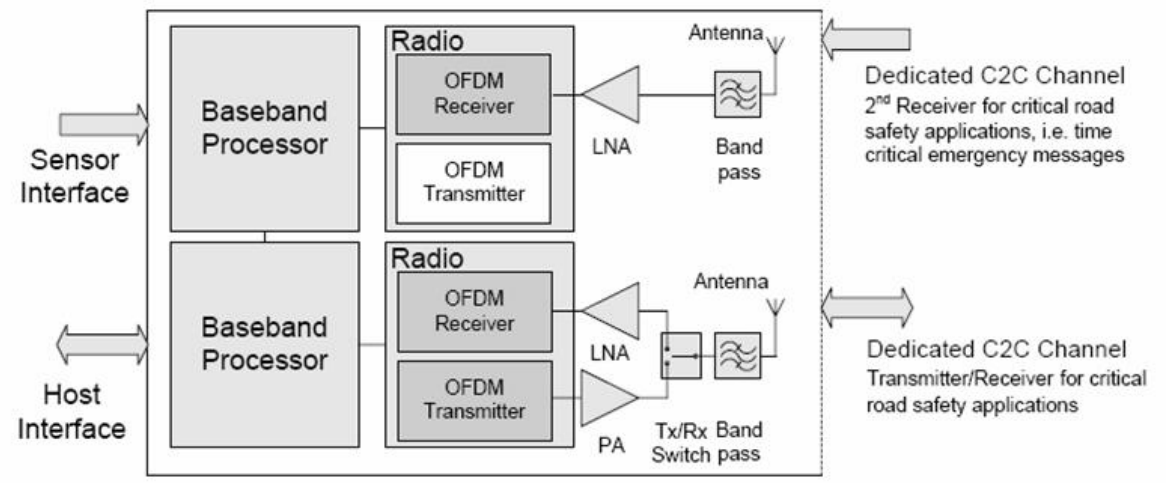

Figure 15 Dual receiver concept

6.4.3 Addresses

A link layer address shall be encoded in IEEE MAC address format.

A node shall support the concurrent use of 48 bit and 64 bit link layer addresses to achieve compatibility with commercial wireless LAN access technologies. For this reason, a C2C Communication Node shall also support the use of universal 48 bit link layer addresses. No assumptions are made herein if this implies to allow simultaneous use or alternative use of both address formats.

To guarantee privacy it seems to be necessary to change the address randomly from time to time. For this reason the following assumptions are made:

- Each C2CC node (on-board units and road-side units) shall be unambiguously referenced by its link layer address (MAC address) while communicating with other C2CC nodes. No assumptions are made about the scope of this unambiguity, since uniqueness may be statistically but not universal.
- A node shall support the use of multiple link layer addresses either sequentially (use one after another) or simultaneously (use at the same time). No assumptions are made herein about the method (algorithm, entity, organization) assigned to generate a link layer address.

In order to achieve a sufficiently large address space for frequently changed random addresses, the use of EUI-48 addresses implies local MAC addresses (universal bit set to “0”), whereas EUI-64 addresses might be either universal (universal bit set to “1”) or local (universal bit set to “0”).

6.4.4 Maximum Message Size, Priorities and Waiting Times

In general it is necessary to avoid channel overload under high traffic conditions and to guarantee low latency times for high priority messages. However up to now no assumptions are made on the maximum message size, priorities and the waiting times for accessing the channel after successful transmissions again.

As different types of data have a different grade of urgency a priority mechanism needs to be adopted. Support of priorities is considered to be mandatory on the dedicated C2C-CC channels (and optional on the normal channels).

According to IEEE 1609.4, IEEE 802.11e is the base for the priorization used in C2C-CC [14].

6.4.5 Logical Link Control

The LLC is required to provide uniform access point to the C2C-CC Network Layer. It could be used to distinguish IP-based and peer to peer communication from C2C-CC specific messages.

7 Communication System

The communication system is a core component of OBUs and RSUs. It provides wireless data transmission, offers communication services to applications, and allows for distributed network coordination. The communication system comprises the network and transport layers in the C2C-CC Protocol Stack on top of the radio system. This chapter describes the communication principles for Vehicle 2 Vehicle and Vehicle 2 Infrastructure communication and briefly explains the tasks and functions of the communication system protocols.

7.1 General Overview

Similarly to packet-switched communication systems, the C2C-CC System defines network and transport protocols, which basically provide the individual transmission of data units among OBUs and RSUs based on short-range wireless technology.

The communication system takes into account the different requirements from applications. Safety applications typically address vehicles in a geographical area and are based on broadcast communication, where data need to be flooded in a geographic target area. These applications have strong demands with respect to reliability and delay. In contrast, non-safety applications, such as mobile Internet access, rely on point-to-point (unicast) communications and have less stringent requirements for reliability and delay.

In the design of the communication protocols, three main aspects specific for vehicular environments are being considered: First, the vehicular communication network lacks a central instance for network organization and coordination, so algorithms and protocols run in a fully distributed manner. Second, the high mobility of nodes results in frequent changes in network topology and could cause considerable transmission overhead for signaling. Third, the data traffic generated by vehicles can exceed the available wireless bandwidth, which can congest the network and result in considerable packet loss and transmission delay.

Due to the primary use of IEEE 802.11-based technology with its short-range communication range, the physical distribution of vehicles on roads and highways has a strong impact on the communication system design. Basically, we distinguish two opposite and challenging network situations, i.e. sparse and dense. In *a dense network situation*, such as cities or major highways with a large portion of equipped vehicles, the data load on the wireless channel is controlled in order not to exceed the

limited wireless bandwidth. In contrast, in *sparse network situations*, such as in the introduction phase of the C2C-CC System or on rural roads with a small density of vehicles, channel saturation is not an issue. Moreover, since vehicles are most likely out of wireless radio range of each other messages could be cached and repeated. The use of enhanced forwarding strategies ensures that vehicles inside the area of influence of a hazard, but not reachable at the time it is detected, will also be notified. Finally, in dense network situations, adapted forwarding strategies are required to be very efficient in terms of overhead while ensuring high reliability to priority messages with the most important payload, i.e., safety-of-life.

The specific aspects of vehicular environments and application requirements have led to the development of communication protocols that are specifically designed for vehicular communication and provide wireless multi-hop communication based on geographical addressing and forwarding. For the dissemination of safety information we identify two main forwarding approaches, *packet-centric forwarding* and *information-centric forwarding*. Packet-centric forwarding refers to the conventional approach for packet-switched communication where the source node breaks the information into data packets and addresses them to a group of network nodes. In vehicular environments, this group typically comprises nodes located in a geographic area. With packet-centric forwarding the responsibility of information dissemination resides on the communication system (more precisely on the network layer) of the forwarder/receiver, where forwarding algorithms attempt to provide efficient and reliable delivery of these packets over potentially multiple wireless hops inside of a geographical area. In contrast, information-centric forwarding does not rely on an end-to-end semantic implemented in the communication system: the safety information issued as single-hop broadcasted by a source node is processed at every receiving node, and afterwards (modified or not) redistributed if required. With information-centric forwarding, therefore, the responsibility of information dissemination resides on the application itself, where it is required that the particular application is installed and executed on every potential forwarder. Both, packet-centric and information-centric forwarding represent two extreme but valid approaches for dissemination of safety information.

In the C2C-CC System, a hybrid approach of packet-centric and information-centric information dissemination for safety applications is applied. Applications can either use the packet-centric or the information-centric approach, or a combination of both. Considering the use cases in Chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**, cooperative forward collision warning is based on information-centric forwarding, whereas hazardous location Vehicle 2 Vehicle notification rather applies the packet-centric dissemination method. The latter example can also apply a combination of both, where the information is disseminated by packet-centric forwarding in a geographic core area with immediate danger for vehicles and using information-centric forwarding beyond the area borders. The combination of both methods ensures that the source node as the originator of an information can determine a minimal geographical area in which the information will be disseminated. Beyond this

region, the forwarders/receivers can decide – depending upon the relevance of the information and network state in its local surrounding – whether to forward an information and optimally aggregate the data. It is worth noting that other methods to combine packet-centric and information-centric forwarding are feasible and are under discussion.

Non-safety applications primarily use the conventional packet-centric approach. If two vehicles communicate and the source node issues a data packet, the communication system is responsible to deliver the data packet to the destination node by means of wireless multi-hop communication. For packet transport beyond the communication range of a single node, intermediate nodes re-forward a data packets on behalf of the source node. For efficiency and scalability, the routing of data packets from source to destination is based on positions. This technique is referred to as *geographical routing* or *position-based routing*.

Non-safety applications may also use broadcast to transmit data. A typical example is consumer advertisements sent by gas stations. Here, the application in the source node determines the geographical area in which the information should be distributed and periodically sends a message. The communication systems then applies forwarding schemes to distribute the data packets to nodes in the geographic area. In comparison to safety applications, the transmitted data of non-safety applications have relaxed requirements for reliability and delay. Forwarding algorithms, in these cases, will operate in “best-effort”-like mode, with low-priority packets and lesser efficiency.

Non-safety applications typically use the Internet addressing scheme and the TCP/IP protocol suite. According to the C2C-CC System Architecture described in Chapter 4, IPv6 packets can be delivered either through the C2C Communication Network Layer or directly on the optional IEEE 802.11a/b/g network interface. In the first case, IPv6 packets (header and payload) are simply encapsulated into C2C Communication Network Headers and transmitted. Therefore, for data generated by applications using the TCP/IP protocol suite a traditional packet-centric delivering is adopted by default. More in detail, for broadcast IP-based communication, some functionalities of the C2C Communication Network Layer can be used to increase efficiency (e.g. distribution to geographical areas, caching and forwarding, efficient flooding). Non-safety applications, however, may also utilize an information-centric approach. As an example, consider an application for road traffic efficiency. When every node periodically informs its direct neighbors of the road traffic status in their vicinity and aggregates the information from other nodes, road traffic information propagates through the network.

The following sections describe the fundamental principles of the communication system, including addressing, forwarding, Internet integration, and support of multiple interfaces. Then, open issues are presented that are considered to be part of the communication system but are currently under discussion in the C2C-CC working groups.

7.2 Design Principles

7.2.1 Geographical Addressing

The C2C-CC System applies a novel addressing scheme that is based on geographical positions. Basically, two types of geographic addresses are defined: First, individual node addresses (like the C2C Communication Network Address) are linked to the physical position of the node. This position is used by forwarding algorithms to transport data packets towards the destination node ("geographical unicast" or "geounicast"). Second, geographical positions are used to define a geographical region based on geometric shapes (such as circles, rectangles, and others). The geographical region can be linked to nodes, either to address all nodes in the region ("geographical broadcast" or "geocast") or to address any of the nodes in the region ("geographical anycast" or "geoanycast").

It is worth noting that a geographical address has a time significance: Due to mobility, the geographical position of a vehicle changes over time. In order to deliver a data packet to an individual node located at a certain geographic position, the position is always linked to a time stamp that allows identifying its freshness. Similarly, a geographic area addresses a group of nodes. Since vehicles can enter and leave the geographical area, the number and identities of the addressed nodes can change.

In addition to addressing, geographical positions are also utilized by many applications. Examples for safety applications are the geographical position at which a hazard (e.g. icy road) was detected, the geographical area in which a hazard information is valid and should be distributed, and the current position of vehicles in its vicinity for extended electronic break light. Also, non-safety applications utilize positions, for example to locate parking lots.

7.2.2 Forwarding Algorithms

Forwarding of data packets is the core function of the C2C-CC System and refers to the process of sending a message to other nodes as part of the routing protocol. In principle, forwarding is based on the concepts for geographical addressing as described in Section 7.2.1.

The C2C-CC System distinguishes among 4 basic forwarding types, i.e. Geographical Unicast, Topologically-Scoped Broadcast (TSB), Geographical Broadcast, and Geographical Anycast. The forwarding types are illustrated in Figure 16 –Figure 19.

- Geographical Unicast is used for unidirectional data transport from a single node (source) to a single node (destination) by means of direct communication or by multiple hops based on C2C Communication specific addresses that include node identifier,

geographical position, and time information (Figure 16).[9]

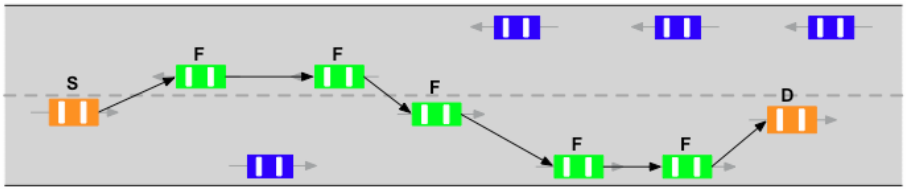

Figure 16 Geographic unicast

- Topologically-scoped broadcast is used for data transport from a single node (source) to all nodes in the coverage scope of the vehicular ad hoc network. In other words, a topologically-scoped broadcast is restricted in the number of wireless hops and it is mapped to a broadcast service at data link layer (Figure 17).

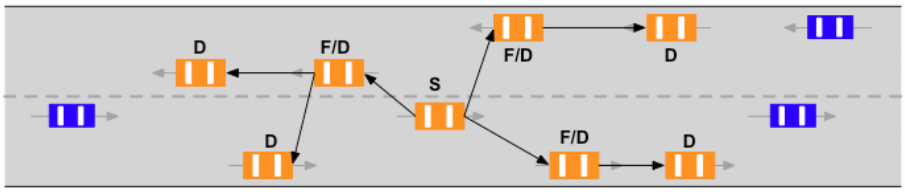

Figure 17 Topologically-scoped broadcast (example with scope = hops = 2)

- Geographically-scoped broadcast is used to transport data from a single node to all nodes within a geographically target area. In contrast to topologically-scoped broadcast, the scope is defined by the geographic region. The geographic region in turn is determined by a geometric shape, such as circle and rectangle (Figure 18).

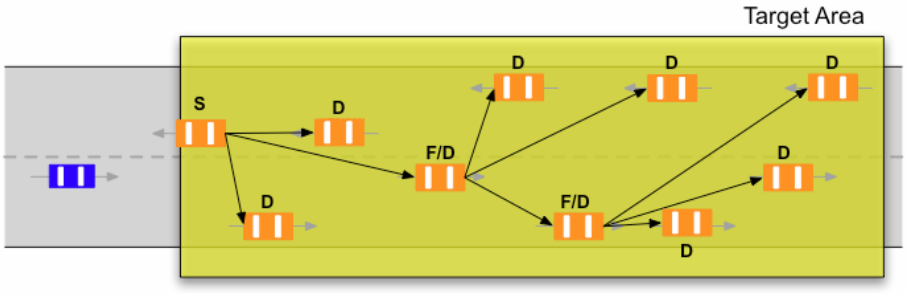

Figure 18 Geographically-scoped broadcast

[9] In the figures, *S* stands for source node, *F* for forwarder, D for destination. *F/D* is both, forwarder and destination.

- Geographically-scoped anycast transports data from a single node to any of the nodes within a geographically area. Compared to geographically-scoped broadcast, with geographically-scoped anycast a packet is not forwarded inside of the geographic area when the packet has reached the area.

For geographically-scoped broadcast, two different scenarios need to be distinguished. In the first case, the source node of a data packet is located inside of the geographical area. This is the common case for safety applications in which a vehicle addresses all others vehicles in the opposite driving direction (e.g. a hazard warning to warn all vehicles driving behind on the same highway up to 2 km range). In the second case, the source node is located outside of the geographic area.[10] In a simple approach, the data packet could be forwarded by geographic unicast towards the target area (see Figure 19). Since the unicast message delivery to the target area may fail, alternative approaches are under discussion.

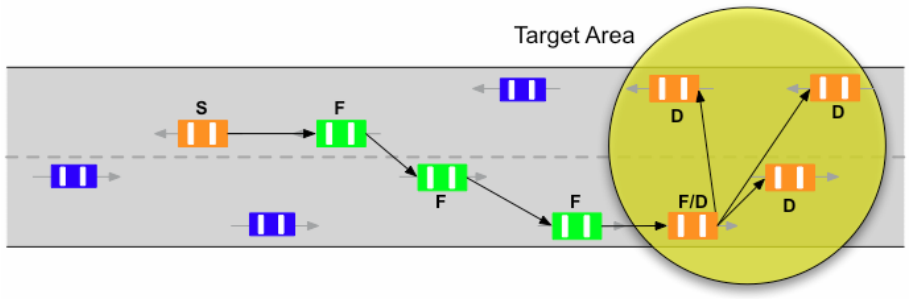

Figure 19 Geographically-scoped broadcast with packet transport towards the target area

Data packets that are periodically sent by every node to inform neighbors on its movement are of particular importance for the C2C-CC System, since many safety applications rely on them. These broadcast packets are potentially sent with a high frequency by every node and can consume a considerable portion of the available wireless bandwidth. They can be regarded as a specific case of topologically-scoped broadcast with a scope of 1 or as a special case of geographically-scoped broadcast with distance (and/or time) constraints, or finally as a mixture of those broadcast protocols.

7.2.3 Transport and Congestion Control

Compared with the network layer protocol, the design of transport protocol for C2C-CC Systems is rather at its initial phase. There is no transport protocol tailored for vehicular networks so far, and it is also very complex to either design new protocols or adapt existing protocols by modifications or

[10] The case of geographical anycast, where the source node is located inside of the geographical area, is not meaningful.

enhancement. The example of TCP indicates the effort to develop a transport protocol. Though it has undergone extensive evolution over the last two decades, it is still subject to improvement and modification to be well suited for today's Internet. The transport protocol for the C2C-CC System will be designed to support the envisaged applications in the vehicular environment. In addition, it should also be flexible to meet possible requirements in the future in order to avoid consequent reengineering. Currently C2C-CC is analyzing the requirements and characteristics of applications as well as special features of the network layer and link layer of the C2C-CC System. Initial results such as design principles and possible approaches are presented and justified in this subchapter and the following subchapter.

In the Internet communication paradigm, services requests from applications are handled by the transport protocols, which issue requests to the network layer, and provide transparent transfer of data between applications. Typical functions of transport protocols include application data multiplexing, error recovery, in-order and reliable transfer, flow and congestion control, etc. Generally saying, transport protocols should provide transparent transport services to applications and should not be linked with any applications semantics. In reality, only very limited transport-related information will be presented to applications, e.g. TCP and UDP follow this rule in that only the port numbers and IP addresses of the source and destination are visible to applications running on top of them.

The requirements and characteristics of the applications and their implications on designing transport protocols are listed below.

- *Types of transport*: Most safety applications and some non-safety applications will use broadcast, while unicast data packet may also be necessary in order to support some non-safety applications. Since broadcast and unicast have distinct requirements and characteristics, the corresponding transport mechanisms will also differ greatly.
- *Error-free transport*: Generally saying, data packets from either safety applications or non-safety applications, irrespective of whether broadcasted or unicasted, require error-free data at the destination. Otherwise, they will be of no use for the applications. Thus, either applications or the transport protocols have to deal with erroneously transmitted data packets.
- *Reliability*: Safety applications have strong demands on reliability in the sense that a broadcast safety message should reach the highest number of intended destinations. Safety applications are typically run on top of broadcast communications. This should not be mixed with the connection-oriented reliable transport mechanism, which requires connection setup before data transfer and acknowledgement of received data.

- *Multiplexing*: It may happen that multiple applications, either safety or non-safety applications run simultaneously between two or a group of communication nodes. In this case, the transport protocols need to multiplex data streams from different applications.
- *Delay constraint and location validity*: Packets from both safety and non-safety application may have a time and space significance, and they will be out-dated or invalid beyond a certain time span or out of a location area. This imposes additional constraints on data buffering, transmission, retransmission, and end-to-end signaling.
- *Priority of data packets*: A natural priority of data packets exists, i.e. packets from safety applications are more important, thus have higher priority than non-safety applications. Packets may also be distinguished according to their priority with more granularity, e.g. depending on their urgency, importance, etc. This implies communication nodes may treat the packets differently when buffering, dropping and forwarding data packets if such information is provided.
- *Forwarding*: Both packet-centric and information-centric forwarding are to be supported. That is, intermediate nodes may update information on the transmission path, thus the end-to-end principle may not apply in the transport protocol design.
- *Data aggregation* from different applications: Typical safety applications have small payload, thus aggregating payload of different applications into one packet and sending it once may reduce network load. Whereas the packet will be disaggregated at the destination. This benefit of data aggregation is justified especially when multiple applications send small payload periodically at a high frequency. Providing this function as the transport layer would free protocols at application layer or middleware from doing this.
- *Application payload size*: Contrary to data aggregation, data from applications may also be too big to be put into one packet on the network layer, thus it has to be disassembled into many packets at the source and assembled at the destination. Packet disassembling, resembling, and in-order delivery are required, and those are typically functions of the transport protocols.

The transport protocols for C2C-CC System also have to deal with the highly varying path characteristics of the vehicular environment. Transmission of data packets in ad hoc networks are well known for the high packet loss rates, long round trip times, short connection durations, high probability of packet reordering, etc. This makes the design of the transport protocols a very challenging task, and it is yet complicated by high moving speeds of communication nodes. The challenges are reflected in several major aspects:

- It is inherently difficult to provide reliable data transport service for both user data and control data in a very dynamic and error-prone communication environment.

- High dynamic network environment makes it hard for the transport service to adapt the changes in the network based on the estimation of the network status or signaling between communication nodes.
- Congestion may happen at any communication hop and it is expensive for a source node to get valuable feedback from networks on the data communication path in order to apply any congestion control mechanisms.
- For broadcast communication, in particular geographical broadcast, the end-to-end paradigm as the basis for a transport protocol can hardly be applied.
- Currently the communication is based on IEEE 802.11 technology, and as reported in the literature, it suffers from a number of issues, such as the well known hidden node problem, the exposed node problem, and unfairness of different nodes at channel access. These problems are harmful for multi-hop communications, and thus pose further challenges on the transport protocols.

Considering the vehicular communication environment, especially the usage of position-based routing protocol, certain features on the network layer and link layer may be utilized by the transport protocols:

- Position-based routing is used as routing protocol, and it provides more functions than those in wired networks such as network layer beacons, the location service, security related services, etc. Moreover, in addition to basic information such as node identities, sequence numbers, and time stamps transferred by beacons, other information may also be included such as transmission power of the source and forwarding nodes. All these information may be utilized by the transport protocols as a part of signaling.
- In case a link is broken, a new route may be found by position-based routing very efficiently and fast on the fly. This may also assist the transport protocols to promptly react to frequent link failures.
- Load control in each wireless hop may be coordinated at the link layer in a distributed and autonomous way, e.g. power control, discarding packet according priority.

The design principles serve the basis for further detailed design of the transport protocols, thus they have to be carefully observed. In the following, some open issues are discussed and possible approaches are justified.

- **Single protocol or multiple protocols**: In the C2C-CC System, safety applications and non-safety applications represent different and challenging requirements which justify the design of different transport mechanisms. This could be realized by either a single protocol which meets

all the requirements, or multiple protocols, which meet the diverse requirements correspondingly.

- **End-to-end principle**: The end-to-end principle may not be feasible or at least has to compromise on application requirements and network characteristics for the following reasons: 1) Information-centric forwarding has to be supported and it is in principle against the end-to-end principle. 2) End-to-end signaling is expensive and even infeasible in vehicular networks. 3) Certain local functions would be beneficial such as local route recovery, local congestion control, etc.
- **Reliability**: Frequently a route may be broken and may never be recovered or replaced. Thus it is very hard and expensive to provide reliable transport service on top of the inherently unreliable network. That means reliable delivery of packets may not be guaranteed, but only be provided as much as possible.
- **Connection-oriented versus connectionless**: Safety applications do need connectionless transport since they are based on broadcast. For non-safety applications, this is an open issue.
- **Transport protocols** should be on the transport layer since: 1) This will hide transport-related details from applications, and not bounded to any application-specific semantics. 2) Transport protocols on application layer may provide certain functions such reliable transport, but other functions such as congestion control may need close interaction with network layer or link layer.
- **Coupling with network and link layers**: Cross-layer signaling is necessary. TCP is based on some metrics such as round-trip-time, packet loss to perform transport functions, and these metrics lose their meaning in ad hoc networks. New metrics from network layer or link layer are needed such as link failure, local traffic congestion etc.
- **Compatibility with TCP/UDP**: Compatibility with TCP and UPD may not be necessary since 1) C2C Communication is a new area, thus new protocols are to be implemented and exclusively used in vehicular networks without considering the TCP/UDP compatibility issue. 2) Legacy applications running on top of TCP/UDP may find their application in case stable connection is assumed to exist. 3) TCP/UDP data packets may also be encapsulated into C2C Communication Network Packets and be tunneled between end points.
- **Fairness**: TCP provides a fair share of bandwidth on a link for concurrent data flows. In the C2C-CC System, fairness should also be part of the transport function. Different from wired networks, ad hoc communication channels have temporal and spatial variations. Thus a fairness criterion has to be redefined.

- **Complexity**: A simple protocol is preferred. It should be easy to implement and test. On the other hand, to distinguish between safety- and non-safety related transport protocols could be beneficial.

7.3 Protocol Design

7.3.1 Network Layer Protocol

The network layer protocol has the following core components (Figure 20):

- The **Location Table** is the central database in a node. The location table maintains a list of other known nodes, either neighbors in a 1-hop distance or non-neighbor nodes. The location table keeps entries as soft-state, i.e. the entries have a certain lifetime and need to be updated, or are removed when the lifetime expires. A location table entry includes a number of information about the particular node, including node network address, MAC address, IPv6 address, geographical position, speed, and heading with time stamp. Flags are used to indicate different states of the nodes, like node type (OBU, RSU, public-safety OBU), availability of Internet access via the node, and others. The location table is updated every time a packet with information about originator and sender of a data packet is received. Applications, in particular for road safety, can rely on location table information, where an efficient and structured approach is needed to distribute the location table information to applications. Plausibility of the Location Table entries should be checked as well. One possible solution caches some of the latest entries related to a node and executes a dedicated algorithms to check plausibility of the ‘trace back’.
- **Packet assembly/disassembly** refers to the generation and processing of a packet header when a packet is sent, forwarded, or received. It includes the access to information of the location table and updating of packet header fields when a packet is forwarded, such as geographical positions, time information, time-to-live value, and priority.
- **Beaconing** is used to advertise the presence of a node to its neighbor nodes. A beacon carries at least the node identifier and its timestamped movement information (position, speed, and heading). A beacon is sent periodically, whereas the interval may vary according to application requirements and the channel load.
- **Forwarding** means re-distribution of a data packet towards the destination, being an individual node or a geographical area. Forwarding is based on different algorithms for

geographical unicast, topologically-scoped broadcast, geographically-scoped broadcast and anycast. A basic algorithm for unicast is *greedy forwarding*, e.g. with the *maximum progress within radius* (MFR) policy. For geographically-scoped broadcast inside of a geographical area, so called *simple flooding with duplication detection* represents a simple approach. More advanced forwarding algorithms are currently under discussion in the C2C-CC working groups.

- **Location service** provides a functionality to locate a certain node by its identifier. The location service is part of the position-based routing protocol, where the source node of a data packet needs to determine the current position of a node first, before the packet is forwarded. The location service is used only when the location table does not have a valid entry for the destination. In principle, the location service is based on a *reactive location search* which allows a node to query the geographical position in an on-demand fashion.
- **Priority handling** offers the assessment of a priority value for a data packet as a measure for the importance/relevance of a packet and the packet processing inside of a node. The processing includes packet classification based on the priority value and applies queuing and scheduling on a per-packet basis. This basically ensures that packets with higher importance/relevance are forwarded with higher priority, while low priority packets can still get a share of the bandwidth.
- **Congestion control** Network congestion occurs when the load of data packets on the wireless channel exceeds the available bandwidth and the network performance degrades. Congestion control is an overall system feature that pertains to all layers, including for example rate limitation for applications. Network layer congestion control comprises a number of mechanisms including priority handling, load indication from wireless channel, transmit power control, packet discard mechanisms, rate control, and others.

The C2C-CC Network Layer has interfaces to upper layers (Service Access Points SAP) to the C2C-CC Transport Layer and to the IP protocol stack. To lower layers, the C2C-CC Network Layer provides SAPs to the different DLC layer of the IEEE 802.11p* interface, IEEE 802.11a/b/g interface, and of other alternative interfaces.

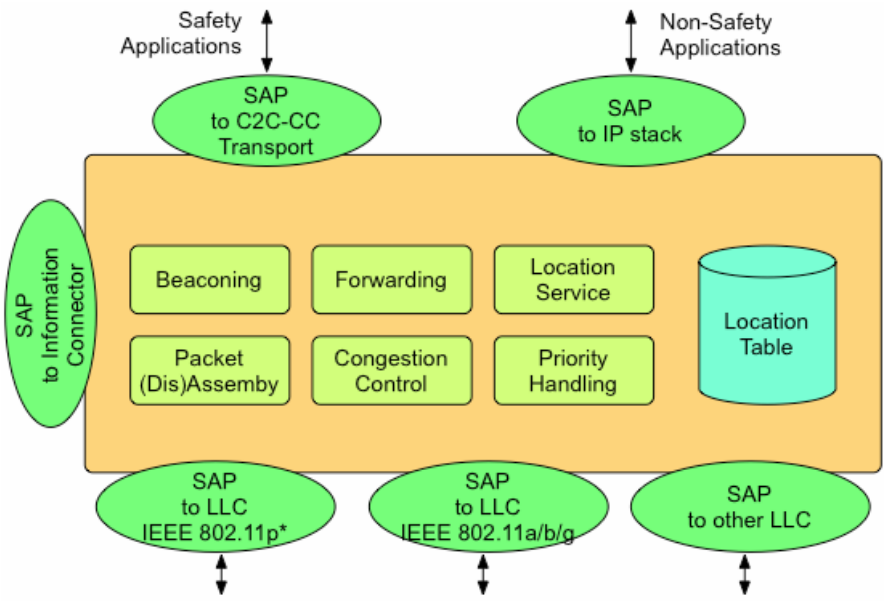

Figure 20 Main components of the C2C-CC Network Layer Protocol

7.3.2 Transport Layer Protocol

TCP is the most prevalent transport protocol in the Internet. It is a connection-oriented reliable protocol typically used by applications that require guaranteed delivery of data. It is well known that TCP is inefficient in wireless networks and is inappropriate for ad hoc networks. To cope with this problem, two approaches are commonly adopted: either to enhance TCP or to design a new TCP-like protocol. Both approaches are not trivial and tend to be more complex than TCP. The application of TCP or TCP-like connection-oriented protocols is mainly limited to non-safety applications. Lacking a suitable transport protocol tailored for vehicular networks, it is not clear whether it is worth developing a TCP-like protocol for non-safety applications.

Safety applications are typically run on top of broadcast communications. Broadcasts are usually built on connectionless transport services, since it is very expensive to guarantee the delivery of broadcast messages. For the C2C-CC System, UDP may be considered as a candidate to support broadcast and also unicast. UDP is a connectionless unreliable transport protocol, and it multiplexes multiple connections by via the source and destination ports, and protects data and protocol headers by means of checksum. Its applicability to the C2C-CC System and possible modifications and enhancements are discussed below.

- Multiplexing connections by means of port numbers can be directly used.
- New mechanisms are needed to ensure more reliable transport of data packets, especially those from safety applications.

- Packet disassembly and assembly have to be enhanced with respect to the specific requirements.
- Checksum of UDP may be disabled or refreshed after each hop in order to support information-centric forwarding.
- Congestion control mechanism is required.

A new protocol, Datagram Congestion Control Protocol (DCCP) is currently being standardized by the IETF. It aims to design a congestion-controlled unreliable transport protocol by resembling TCP but without its reliability function. The protocol was expected to be simple with the initial assumption that unreliable congestion control would be no harder than reliable congestion control. However, it turns out that the protocol is much more complicated than it was expected to be. The reason is attributed to the art of the TCP, i.e. its congestion control, flow control, acknowledgement, reliability are integrated into a seamless whole, whereas a break up of its integrity leads to the redesign of almost every aspect of the transport protocol. Although the protocol has different objectives from those of the C2C-CC System, it sheds light on how congestion control maybe achieved with unreliable transport. Possible mechanisms that can be borrowed from DCCP have to be studied.

In the following reliability and congestion control are discussed. The investigation of further mechanisms is to be done. Finally, the selection and integration of appropriate mechanisms also require very delicate consideration.

Reliable Transport

Reliability may be enhanced at the application layer. For example, Real Time Transport Protocol (RTP) is used in conjunction with UDP to provide end-to-end network transport functions to transmit real-time data over multicast or unicast network services. However, it is not the aim of the transport design to assume any such reliability support from the application layer.

TCP follows the end-to-end approach, where three-way handshakes are used to establish a connection. This might be expensive or even not necessary in vehicular networks. Considering location service provided by position-based routing protocol, for unicast transport, the source of communication may obtain the destination identity and position by either information obtained from beacons or location service. This implicitly indicates that there exists a transport route, and it could serve as some kind of quasi-handshake.

Certain TCP mechanisms such as timeout, retransmission, and Selective Acknowledgement (SACK) are useful. However, these end-to-end mechanisms should also be enhanced by mechanisms at each hop. Possible mechanisms include packet buffering and retransmission at each intermediate node, local route recovery in case link failure or congestion, etc.

Congestion Control

Congestion control may be performed based on the end-to-end paradigm. For end-to-end congestion control, TCP applies window-based method, while many other TCP deviants follow the rate-based approach based on feed back from the network. For the C2C-CC System, rate-based approach appears to be promising. It is straightforward for a source to obtain the load at the local hop and its distance to destination, which is correlated with the number of hops to the destination. It is still subject to further investigation whether these metrics could be used for rate control, and which other metrics may also be used.

Congestion control at each hop is also beneficial since it is easy for an intermediate node to react quickly to local congestion. A possible approach is to classify packet according to their priority, so that each node may forward only packets with high priority in case of congestion. However, this approach requires support applications since each packet has to be marked with its priority. Again, its feasibility and applicability have to be examined.

7.3.3 TCP/IP Protocol Integration

The C2C-CC System provides transport of IPv6 packets (header and payload) enhanced by geographical addressing and forwarding as described in Sections 7.2.1 and 7.2.2. The delivery of IPv6 packets is achieved by encapsulation of IPv6 packets into C2C Network Layer Headers. After encapsulation, the C2C Network Layer Headers are routed and forwarded using the same basic mechanisms used for C2C application data. This mechanism for delivery of IPv6 packets can also be referred to as *"IPv6 in C2C network header tunneling"*, where two communicating nodes use virtual tunnel interfaces that change dynamically their end points.

Important design aspects for the integration of TCP/IP protocols and the C2C Communication Network Protocols are addressing scheme and resolution mechanisms. The following list briefly summarizes related design concepts currently discussed in the CAR 2 CAR Communication Consortium:

- Due to the limited wireless resources, address resolution mechanisms as used in the TCP/IP protocols, like *Address Resolution Protocol (ARP)* and *Neighbor Discovery (ND)* are not applied. A scheme to map IPv6 address into C2C Network Layer Address, and also C2C Network Layer Address into MAC address, will be defined.
- As consequence of the previous statement, vehicles should use only IPv6 addresses with a EUI-64 identifier as host identifier derived from the MAC address. Privacy issues described and addressed in RFC 3041 [15] are strongly alleviated through the use of temporary, changing MAC addresses, which are assigned in a set to every vehicles as part of pseudonyms.

- Because the uniqueness of MAC addresses is assumed by the C2C-CC System for liability reasons, *Duplicate Address Detection (DAD)* is omitted.
- IPv6 stateless and stateful address configuration mechanisms are supported. This is achieved by distributing IPv6 signaling messages using delivery mechanisms provided by the C2C Network Layer.
- For direct communication between vehicles, a predefined IPv6 prefix reserved for the C2C-CC System is used (e.g. belonging to the Unique Local IPv6 Unicast Addresses class as defined in RFC 4193 [16]). For communication with the infrastructure, a globally routable prefix is obtained from an *IPv6 Access Router*.
- Road Side Units can either act as IPv6 Access Routers or as network bridges connected to external IPv6 Access Routers. Different Access Routers are responsible for announcing different network prefixes with global validity. As a consequence, when roaming between Access Routers, vehicles experience network layer handovers.

From the architectural point of view, in the C2C-CC approach the IPv6 layer is not aware of the ad hoc routing in the C2C Communication Network Layer below. This results in a clean separation of roles with functions for ad hoc routing placed in C2C Network Layer and functions for interconnection with an IP-based intra-structure routing placed as usual in the IPv6 layer. The separation also ensures that a solution for IP mobility support can be integrated into the IPv6 layer with minimal implications on the ad hoc routing. In particular, the Network Mobility protocol NEMO, RFC 3963 [17], is the solution considered by C2C-CC to provide session continuity and global reachability. Currently, RFC 3963 requires that a network infrastructure is always reachable and that all data traffic goes through the Home Agent. Extensions to allow data packets to be exchanged directly between vehicles, even if the infrastructure is not reachable, are currently discussed in the IETF, considering also C2C Communication requirements.

As depicted in Chapter 4, the C2C-CC encourages the usage of an additional WLAN network interface implementing a standard IEEE 802.11a/b/g family protocol. This interface can be accessed by the IPv6 layer either directly or through the C2C Communication Network Layer, which provides the same functionalities as for the modified 802.11p interface. Additionally, the 802.11a/b/g interface can be used to connect with public hot spots located at gas stations, parking and commercial areas. These attachment points can optionally implement the C2C Network Layer in order to extend their coverage area by means of wireless multi-hop technology and to exploit geocast message distribution.

7.4 Outlook

While the principles of the C2C-CC System are settled, the C2C-CC working groups currently work on a number of technical aspects, including:

- Enhanced forwarding algorithms,
- Congestion control mechanisms for geographical broadcast,
- Transport protocol design for geographical unicast,
- Support of authentication, integrity and non-repudiation in the communication system,
- Enhanced concepts for integration of ad hoc routing and the IP protocol suite,
- Support of IP mobility solutions in vehicular environments,
- Multi-channel operation with IEEE 802.11p*,
- Spectrum harmonization, and
- IEEE 802.11p and WAVE standardization.

8 Data Security and Privacy

Securing CAR 2 CAR Communication is an indispensable prerequisite for its deployment and real-world use. Three major goals need to be achieved:

- All information communicated in the network must be correct and trustworthy.
- The C2C-CC System must be extremely robust and must not fail to work.
- The C2C-CC System participants' privacy must be ensured.[11]

Beside this technical work, security within the C2C-CC considers various further discussion areas (see Figure 21):

- The goal of the security mechanisms is to ensure acceptance and credibility of the system by the end user, who trusts the system.
- Current standards are to be considered and properly applied to the system design. Where necessary, standards need to be extended or new ones created.
- In addition to pure ad hoc communication, the integration of communication infrastructures and telecommunication platforms into the overall system architecture are to be properly set.
- Thereby, the discussions are driven by commercial requirements conveying business models and operational concepts, partnerships and regulations.
- Legislation aspects need to address privacy, law enforcement and liability questions.

[11] In many cases, VANET applications communicate personal data, such as current location or current speed, which could be used for vehicle / driver profiling.

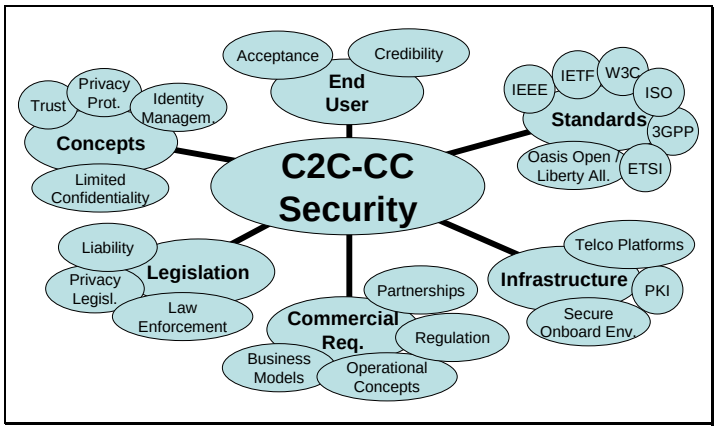

Figure 21 Security discussion areas

From a technical point of view, in order to achieve the first two of the major goals, i.e. trustworthy dissemination of information and robustness, the C2C-CC Network must be protected against different kinds of attacks. Analyzing the threats for this special kind of network, Denial of Service attacks, generating fake messages or tampering with messages need special consideration. It is extremely important to ensure message integrity - a risky driving maneuver based on false message information might be fatal - while sender authentication is not needed in many cases.

For the assistance and collision avoidance types of applications, the C2C-CC Security Solution must still allow low latency communication. This is an important requirement since applying cryptographic methods can create considerable computing overhead. Hence, it is not possible to adopt security protocols involving strenuous verification or interaction processes.

Security mechanisms should normally not surface at the application layer. Of critical importance however is that applications receive from other vehicles or from infrastructure entities information with a certain level of trustability. This, besides integrity (knowing that the message had not been tampered with in an unauthorized way, see above), requires receiving it from a trusted source. While strong sender identification and authentication is not the goal here, it might still be somewhat required and is competing against the goal of driver/vehicle privacy. An anonymized authentication of messages should ideally be possible.

Notably, to establish trust, basically cryptographic measures can be applied as well as means of plausibility checking and cross-verification. It remains to be established, how cryptographic means can be balanced against application algorithms such as plausibility checking. Issues such as radio resource consumption, processing power, hard-ware requirements (e.g. when tamper-proof devices become necessary) will need to be further investigated.

Moreover, applications must not assume that individual vehicles can always be identified by some unique code that is openly communicated. To protect privacy and prevent recording of movement

patterns etc. it should rather be assumed, that means for vehicles to assume dynamic identities and even dynamic certificates for regular over-the-air communication are established.

A potential approach is to rely on the road-side infrastructure. This will be connected to an IPv6 backbone. Vehicles may in a secure way draw leases for temporary IPv6 address assignments and use these randomly assigned IPv6 addresses as temporary identifiers.

A trusted authority, which issues temporary, anonymous, but unique certificates to vehicles, could be the corner stones for a balanced C2C-CC Security Concept.

From these early and rough requirements, work progressed in two directions, a technical and a non-technical direction, both guiding and feeding each other.

On the technology side, some baseline concepts have been drafted, that are currently being actively discussed:

- as vehicles equipped with a C2C-CC System will be periodically geo-broadcasting their position and send beaconing information for network layer purposes, the real identity of the vehicle will be concealed to protect privacy against both, malicious and casual observation or tracking. This means, that permanent identifiers and addresses must not be communicated in clear over the air.
  To the contrary, at all layers from physical to IP/network to application, C2C-CC in-vehicle systems will be using temporarily assigned identifiers. Fixed identifiers should only be used in the occasional situation, where mutual system authentication is necessary, e.g. when obtaining a new set of temporary identifiers.
- to ensure trust in messages, they have to be signed. Signing of messages again has to happen with dynamically assigned, temporary pseudonyms. It is currently under investigation, how frequently pseudonyms will be updated and what the technical mechanisms will be for this procedure. Moreover, it is yet to be decided, which crypto-technology to actually use for these pseudonym signatures.
  In this choice, a number of factors have to be balanced, such as security level, size of signature and bandwidth constraints, processing time and real-time requirements of e.g. safety applications. Currently, RSA and ECC are candidates under investigation.
  Also, process aspects such as which organization will have authority to issue, verify and withdraw pseudonyms are critical and have to be addressed.

On the non-technical side, challenging questions will have to be addressed before being able to even draft applicable security mechanisms.

- What are the business models involved in C2C-CC Systems and which business objects need to be protected against which attacks?

- What are the operational concepts and who will deploy, operate and control the infrastructure?
- Who will issues subscriber modules, if any? When subscriber modules will be issued, how do they differ from e.g. the GSM SIM? What relationship will C2C-CC Systems have with mobile networks, operators, service providers and MVNOs[12]? Are there potential synergies, e.g. on the infrastructure side, that should be exploited when designing C2C-CC Security Mechanisms?
- What regulatory and legal aspects should be foreseen in the future and should be taken into account?

Note, that all these assumptions are still work in progress. A clear favourable solution has not been identified yet and some questions are yet under discussion. The C2C-CC is in liaison with various security activities and open to discussions with and proposals from projects such as SEVECOM[13] or the data security working group of the project NoW – Network on Wheels[14].

[12] Mobile Virtual Network Operators

[13] http://www.sevecom.org

[14] http://www.network-on-wheels.de

9 Summary and Conclusions

The Manifesto represents the first public document released by the CAR 2 CAR Communication Consortium and a first European step towards a standard for vehicular communications. It basically provides an overview of the consortium goals and the technical approach for vehicular communications. On the one hand, the Manifesto brings together the different aspects of the overall C2C-CC System and describes them in a unified view. Consequently, it will be used as a basis for further work by the involved partners. On the other hand, the Manifesto introduces concepts and principles of vehicular communications for those readers who are not directly involved in the design and specification of the CAR 2 CAR Communication Consortium work. In particular, the Manifesto is a basis for discussions between the C2C-CC and other ITS stake holders, such as future and existing R&D projects, standardization bodies and car industry.

The technological approach of the C2C-CC is manifold and comprises of radio, networking and information technology. The combination and integration of these aspects results in a system architecture which regards vehicles as communicating and cooperating network peers. In this architecture, vehicles can communicate with the roadside communication infrastructure and also among each other. The cooperating behavior of vehicles in communication allows the utilization of novel communication principles where a vehicle forms a spontaneous network with other vehicles in its vicinity. Then, a vehicle is not only information source or sink, but also information distributor. Being mainly focused on Wireless LAN as the underling radio technology, the C2C Communication System provides Vehicle 2 Vehicle and Vehicle 2 Roadside Communications. The communication services enable a wide range of applications, ranging from road safety and traffic efficiency, driving comfort and infotainment. While the primary focus of the C2C Communication System remains on Active Safety, it is open and prepared to be integrated into an overall European ITS architecture, which targets at safer, cleaner, and more efficient transport of people and goods.

Founded in 2002, the C2C-CC has established as an important player among the stake holders and as a reference for vehicular communications. The publication of the Manifesto represents a first milestone in creation of the consortium by major car makers and suppliers in Europe and definition of system design and technical principles. The Manifesto is the results of the different C2C-CC working groups that also integrated and harmonized the achievements of the various European and national R&D projects. The identification of missing technical parts and open questions is a particular contribution of the Manifesto which allows the consortium and interested parties to straighten future efforts.

Having finished the 1st phase of consortium creation, definition of the system architecture and of technical principles, the working groups of the CAR 2 CAR Communication Consortium will focus working on detailed system design, definition and specifications of algorithms and communication protocols. As a next step, the CAR 2 CAR Communication Consortium will develop conceptual solutions for the system design issues that are currently under discussion, such as allocation of a protected frequency band for road safety in Europe, potential usage of the IEEE 802.11p / WAVE standard, integration of multiple wireless technologies, data security, congestion control, data transport, and others. These solutions will be harmonized with other emerging worldwide standards that are related to the vehicular communications, such as IEEE 802.11, IEEE 1609, ISO TC 204 WG 16, selected IETF working groups and SAE.

In the future, it is expected that the C2C-CC proposed standard will be the technical basis for European field operational tests (FOTs) for vehicular cooperative systems.

10 Appendix

10.1 Terms and Definitions

Term	WG	Definition
1-Hop Broadcast	*Net*	*To send a data packet to all direct neighbors of a node. No further forwarding of that data packet is applied.*
Access Point		*An access point is a non moving network node that allows access to the car using any IEEE 802.11 standard including the new CAR 2 CAR Communication Standard. An access point can have a connection to other local or global networks, e.g. the Internet. An access point might be private or publicly owned.*
Ad hoc network	*Net*	*Communication network which is set up by the communication nodes (peer-to-peer) without any pre-installed fixed infrastructure.*
Bandwidth	*Phy*	*The difference between the highest and lowest sinusoidal signals that can be transmitted across a transmission line or through a network. It is measured in Hertz (Hz) and also defines the maximum information-carrying capacity of the line or network.*
Basic System	*Phy*	*The Basic System is a special subset of a CAR 2 CAR Communication System. The Basic System includes only functions and components which are required* *1. to forward and route messages as specified in the standard and* *2. to make the car feasible to create and to send warning messages and traffic flow information messages as specified in the standard.* *When buying the car the consumer should not make any decision, the Basic System should be part of the regular equipment. In a car only equipped with the Basic System there is no application visible for the driver, the passengers or the owner.* *The reason for equipping cars just with the Basic System is to reach the required market penetration and to make warning and traffic flow applications running for the consumers that purchased these applications as an option. For these applications additional hard- and software not*

Term	WG	Definition
		part of the Basic System might be necessary.
Beacon	*Net*	*Network Layer control data packet which is sent periodically in broadcast mode and which includes control data used to build up the neighbor table.*
Broadcast	*Phy/Net*	*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.*
CAR 2 CAR Communication Consortium (C2C-CC)	*Sta*	*The CAR 2 CAR Communication Consortium is a non-profit organization initiated by European vehicle manufacturers, which is open for suppliers, research organizations and other partners.*
CAR 2 CAR Communication System	*Sta*	*The communication system specified by the C2C-CC.*
CAR 2 CAR Radio Communication System	*Arch*	*The radio system contains all parts of the CAR 2 CAR Communication System that are used for functions of the physical layer and the data link layer (MAC & LLC). This can be hardware, software and antennas.*
Communication	*Net*	*The exchange of related messages between two communication partners. At least one message has to be sent to a communication partner and at least one response message has to be received from this communication partner*
Destination *(Recipient)*	*Net/App*	*One of those nodes which are addressed by the source of a packet and which will receive the data packet and pass it to the upper layers.*
DSRC	*Phy*	*Dedicated Short Range Communication* *It must be differentiated between the European DSRC and the DSRC in the US. The US DSRC is the basis for the new standard IEEE 802.11p.*
ETSI	*Sta*	*European Telecommunications Standards Institute*
Forwarder	*Net*	*Node which receives a data packet from another node and sends this data packet to a third node*
Geo-Anycast	*Net*	*Forwarding of a message to some arbitrary node inside a geographical area. The area is defined by the sender and transmitted with the data packet control information.*
Geo-Broadcast	*Net*	*Forwarding of a message to all nodes which are located inside a geographical area. The area is defined by the sender and transmitted with the data packet control information.*
Geo-Unicast	*Net*	*Forwarding of a message to one and only one recipient which is addressed by an identifier.*
Hot Spot	*Net*	*In this context a hot spot is the same as an access point*

Term	WG	Definition
IEEE	*Sta*	*Institute of Electrical and Electronics Engineers*
IEEE 802.11p	*Phy*	*IEEE standard for the radio communications between vehicles and between vehicles and infrastructure.*
Information Lifetime	*Net*	*Lifetime of information between origin and last information consumption*
Information Range	*Net*	*Distance between information origin and most distant information consumption (originator of an information to most distant recipient of this information)*
Infrastructure	*Arch/Net/App*	*Infrastructure is the generic term for private or public access points and for traffic infrastructure.*
IP	*Net*	*Internet Protocol.*
ISO	*Sta*	*International Organization for Standardisation, sets world-wide standards for any subject not covered by a specialist agency; now cooperates with the International Electrotechnical Committee (IEC) in the Joint Technical Committee 1 (JTC 1) of IEC and ISO for IT standards.*
Location	*Net*	*Position of a node and time, at which this position was taken*
Location Table	*Net*	*Table, in which location data of other nodes is stored*
Message Lifetime	*Net*	*Time between message generation and oldest possible reception*
Message Range	*Net*	*Distance between originator of a message and most distant recipient*
Neighbor Table	*Net*	*Table which includes data on neighboring nodes, eg. identifier and position of that node*
Originator	*Net*	*See Source*
Physical Transport	*Net*	*To temporary store a data packet inside the computing system of a car with the intention to move it together with the car*
Point-2-Point communication	*Net*	*Communication between two dedicated communication partners.*
Position	*Net*	*Position of a node (e.g. latitude/longitude pair)*
Recipient	*App*	*See Destination*
Source (Originator)	*Net/app*	*A node on which a data packet has been generated, which has to be transmitted to the recipients addressed.*
SAP	*Arch*	*Service Access Point (SAP) is an identifying label for network endpoints used in OSI networking.*

Term	WG	Definition
Standard	*Sta*	*A standard which has been approved pursuant to the statutes of the standards bodies with which the Community has concluded agreements.*
Technical specification	*Sta*	*A specification contained in a document which lays down characteristics required of a product, such as levels of quality, performance, safety of dimensions, including the requirements applicable to the product as regards terminology, symbols, testing and test methods, packaging, marking or labeling.*
Telematics	*App*	*Synthetic word of telecommunication and informatics for covering both disciplines*
Transmission Control Protocol (TCP)	*Net*	*The protocol in the TCP/IP suite that provides a reliable full-duplex message transfer service to application protocols.*
Transmission Interval Control (TIC)	*Net*	*Mechanisms to control the periodic messages' rate in order to reduce network congestion*
Transmission Power Control (TPC)	*Net/Phy*	*Mechanisms to control the messages' transmission power in order to reduce network congestion*
Traffic Infrastructure		*In this context traffic infrastructure are entities with a communication unit that are able to communicate in one or in both directions with the CAR 2 CAR Communication System in a vehicle. Examples are traffic lights or a traffic signs.*
UDP	*Net*	*User Datagram Protocol*
Validity time	*Net*	*Time set by the application describing the time how long a message has to sustain inside the destination area or inside the vehicular network. E.g. a danger warning message can sustain for 15 minutes. It is the task of the CAR 2 CAR Communication System to ensure that new arriving cars receive this message for the validity time*
Vehicle 2 Infrastructure Communication	*Arch/Net*	*Communication between a CAR 2 CAR Communication System and the infrastructure.*
Vehicle 2 Vehicle Communication, CAR 2 CAR Communication	*Arch/Net*	*Communication between CAR 2 CAR Communication Systems*
Wireless LAN (WLAN)	*Phy*	*A wireless LAN or WLAN is a wireless local area network, which links two or more nodes without using wires.Typically, WLAN is based on IEEE 802.11 standard.*

11 Contributors

In alphabetical order.

Roberto Baldessari	NEC
Bert Bödekker	DENSO
Achim Brakemeier	DAIMLERCHRYSLER
Matthias Deegener	OPEL
Andreas Festag	NEC
Walter Franz	DAIMLERCHRYSLER
Andreas Hiller	DAIMLERCHRYSLER
Chris Kellum	OPEL
Timo Kosch	BMW
Andras Kovacs	EFKON
Massimiliano Lenardi	HITACHI EUROPE
Andreas Lübke	VOLKSWAGEN
Cornelius Menig	AUDI
Timo Peichl	ALPINE
Matthias Roeckl	DLR
Dieter Seeberger	DAIMLERCHRYSLER
Markus Strassberger	BMW
Hannes Stratil	EFKON
Hans-Jörg Vögel	BMW
Benjanmin Weyl	BMW
Wenhui Zhang	NEC

12 References

[1] K. Matheus, R. Morich, I. Paulus, C. Menig, A. Lübke, B. Rech, W. Specks, *CAR 2 CAR Communication – Market Introduction and Success Factors*, 5th European Congress and Exhibition on Intelligent Transport Systems and Services (European ITS 2005), June 2005

[2] Institute of Electrical and Electronics Engineers, *IEEE Draft Amendment to Standard for Information Technology - Telecommunications and information exchange between systems - LAN/MAN Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 3: Wireless Access in Vehicular Environments (WAVE)*, 2007

[3] Committee SCC32 of the IEEE Intelligent Transportation Systems Council, *IEEE 1609.1 Draft Standard for Wireless Access in Vehicular Environments (WAVE), IEEE 1609.1 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - WAVE Resource Manager,* 2006

[4] Committee SCC32 of the IEEE Intelligent Transportation Systems Council*, IEEE 1609.2 Draft Standard for Wireless Access in Vehicular Environments (WAVE), IEEE 1609.2 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages,* 2006

[5] Committee SCC32 of the IEEE Intelligent Transportation Systems Council, *IEEE 1609.3 Draft Standard for Wireless Access in Vehicular Environments (WAVE), IEEE 1609.2 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services,* 2006

[6] Committee SCC32 of the IEEE Intelligent Transportation Systems Council, *IEEE 1609.4 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation,* 2006

[7] Institute of Electrical and Electronics Engineers, *IEEE 802.11-1999, IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*
[8] Institute of Electrical and Electronics Engineers, *IEEE Std 802.11, 1999 Edition (R2003) Information technology - Telecommunications and Information Exchange Between Systems - Local and metropolitan area networks - Specific Requirements - ; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications,* 2003

[9] Institute of Electrical and Electronics Engineers, *IEEE Std 802.11a-1999(R2003) Supplement to IEEE Standard for Information technology -Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks -Specific Requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications High-Speed Physical Layer in the 5 GHz Band,* 2003

[10] Institute of Electrical and Electronics Engineers, *IEEE Std IEEE Std 802.11b-1999(R2003) Supplement to IEEE Standard for Information technology -Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks -Specific Requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed*

Physical Layer Extension in the 2.4 GHz Band, 2003

[11] Institute of Electrical and Electronics Engineers, *IEEE Std IEEE Std 802.11g-2003; Supplement to IEEE Standard for Information Technology -Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks -Specific Requirements; Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band,* 2003

[12] European Telecommunications Standards Institute, *ETSI TR 102 492-1 V1.1.1 (2005-06) Electromagnetic compatibility and Radio spectrum Matters (ERM); Intelligent Transport Systems (ITS); Part 1: Technical Characteristics for Pan-European Harmonized Communications Equipment Operating in the 5 GHz Frequency Range and Intended for Critical Road-Safety Applications*; System Reference Document, 2005

[13] European Telecommunications Standards Institute, *Electromagnetic Compatibility and Radio spectrum Matters (ERM); Intelligent Transport Systems (ITS); Part 2: Technical Characteristics for Pan-European Harmonized Communications Equipment Operating in the 5 GHz Frequency Range Intended for Road Safety and Traffic management, and For Non-Safety Related ITS Applications;* ETSI TR 102 492 - 2 V1.1.1 (2006-03), Draft System Reference Document

[14] Institute of Electrical and Electronics Engineers, *IEEE 802.11E-2005 IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements,* 2005

[15] T. Narten, R. Draves, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*, IETF RFC 3041, January 2001

[16] R. Hinden, B. Haberman, *Unique Local IPv6 Unicast Addresses*, IETF RFC 4193, October 2005

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