Marc Torrent Moreno

Inter-Vehicle Communications: Achieving Safety in a Distributed Wireless Environment

Challenges, Systems and Protocols

universitätsverlag karlsruhe

Marc Torrent Moreno

Inter-Vehicle Communications: Achieving Safety in a Distributed Wireless Environment

Challenges, Systems and Protocols

Inter-Vehicle Communications: Achieving Safety in a Distributed Wireless Environment

Challenges, Systems and Protocols

Marc Torrent Moreno

universitätsverlag karlsruhe

Dissertation, Universität Karlsruhe (TH)
Fakultät für Informatik, 2007

Impressum

Universitätsverlag Karlsruhe
c/o Universitätsbibliothek
Straße am Forum 2
D-76131 Karlsruhe
www.uvka.de

Universitätsverlag Karlsruhe 2007
Print on Demand

ISBN: 978-3-86644-175-0

Inter-Vehicle Communications:
Achieving Safety in a Distributed Wireless Environment
–
Challenges, Systems and Protocols

zur Erlangung des akademischen Grades eines

Doktors der Ingenieurwissenschaften

der Fakultät für Informatik
der Universität Fridericiana zu Karlsruhe (TH)

genehmigte

Dissertation

von

Marc Torrent Moreno

aus Barcelona

Tag der mündlichen Prüfung:	19. Juli 2007
Erster Gutachter:	Prof. Dr. Hannes Hartenstein Universität Karlsruhe (TH)
Zweiter Gutachter:	Prof. Dr. Raja Sengupta University of California at Berkeley

Zusammenfassung

Aktive Sicherheit im Straßenverkehr kann durch den drahtlosen Informationsaustausch zwischen Fahrzeugen verbessert werden. Die aktive Sicherheit kann insbesondere in zweierlei Hinsicht durch Fahrzeug-zu-Fahrzeug-Kommunikation (Inter-Vehicle Communications, IVC) unterstützt werden. Einerseits können Unfälle vermieden werden, indem alle Fahrzeuge ihren aktuellen Status periodisch an ihre Nachbarn übermitteln, um somit eine frühzeitige Erkennung gefährlicher Verkehrssituationen zu ermöglichen. Andererseits kann der Fahrer durch die schnelle Verbreitung sicherheitskritischer Nachrichten über Gefahren informiert werden und dementsprechend reagieren. Ziel dieser Dissertation ist die Entwicklung notwendiger Kommunikationsprotokolle und -systeme, um einen robusten und effektiven Informationsfluss sicherheitskritischer Nachrichten zu ermöglichen.

Im ersten Schritt wird durch Simulationen die Leistungsfähigkeit der zugrundeliegenden drahtlosen Übertragungstechnologie analysiert, um die wichtigsten Herausforderungen für IVC zu identifizieren. Dem Simulationswerkzeug liegt eine ns-2.28 Version zu Grunde, die um präzisere und aktuellere Modelle erweitert wurde. Dies umfasst probabilistische Radiowellenausbreitungsmodelle, eine drahtlose Schnittstelle gemäß dem IEEE 802.11p-Entwurf, sowie realistische Fahrzeugbewegungen, die denen auf deutschen Autobahnen entsprechen. Die Ergebnisse unterstreichen, dass in IEEE 802.11p DCF-basierten Fahrzeugnetzwerken Interferenzen und Paketkollisionen nicht zum Verlust sicherheitskritischer Informationen führen dürfen. Hierbei liegt die Herausforderung darin, dass sich alle sicherheitsrelevanten Nachrichten einen gemeinsamen drahtlosen Kanal teilen müssen und die resultierende Last durch periodische Nachrichten zu einem ausgelasteten Netzwerk führt, wie es häufig in kritischen Verkehrslagen auftreten kann.

Es wurden zwei Methoden entwickelt, die auf Leistungskontrolle und Wettbewerbsmechanismen basieren, um den Datenverkehr so zu begrenzen, dass relevante Nachrichten mit hoher Wahrscheinlichkeit empfangen werden. Zunächst wird eine Methode basierend auf strikter Fairness vorgeschlagen, D-FPAV, die die Last der periodischen Nachrichten auf dem Kanal und stellt gleichzeitig eine hohe Empfangswahrscheinlichkeit im Sicherheitsabstand des sendenden Fahrzeugs sicherstellt. Im Anschluss wird die Methode EMDV präsentiert, die der schnellen und effektiven Verbreitung von Nachrichten in Notfallsituationen innerhalb

eines geographischen Region dient. Weiterhin werden mit Hilfe des erweiterten ns-2.28 Simulators das Leistungsvermögen beider Ansätze sowie ihre Synergie aufgezeigt. Die Simulationsergebnisse zeigen zum einen, dass D-FPAV dazu in der Lage ist, die Empfangswahrscheinlichkeit sowohl periodischer Nachrichten in unmittelbarer Nähe des Senders als auch von Nachrichten in Notfallsituationen über alle Distanzen hinweg signifikant zu erhöhen. Zum zweiten ermöglicht EMDV sicherheitskritische Informationen an alle Knoten einer Region mit kurzer Verzögerungszeit zu verbreiten. Drittens wird gezeigt, dass die Kombination von D-FPAV und EMDV zu einer deutlichen Effizienzsteigerung und Verkürzung der Verzögerungszeit der Nachrichtenverbreitung führt.

Zuletzt werden einige Entwurfsrichtlinien für Protokollarchitekturen vorgeschlagen, die an die Eigenschaften sicherheitsrelevanter Interfahrzeugkommunikation angepasst sind und als Implementierungsbasis genutzt werden können.

Die in dieser Arbeit entwickelten Kommunikationsprotokolle und der Systementwurf wurden im Projekt 'Network on Wheels' verwendet, um eine Plattform für Fahrzeug-zu-Fahrzeug-Kommunikation im Rahmen einer europaweiten Referenzimplementierung zu entwickeln.

Abstract

Vehicular 'active safety' can be enhanced by the wireless exchange of information among the vehicles driving along a road. In particular, inter-vehicle communications (IVC) can support safety systems designed to avoid road accidents by two means. First, periodic transmissions from all vehicles to inform their neighbors about their current status enables accident prevention by being capable of identifying dangerous road situations. Second, the fast dissemination of emergency information whenever a hazard has been detected can help drivers avoid the danger. The goal of this thesis is to design required communication protocols and systems in order to provide the means for a robust and effective transmission of safety-related information.

We first analyze the performance of the underlying wireless technology via simulation in order to identify the most relevant challenges for IVC. The simulation tool consists of a significantly extended network simulator (ns-2.28) with more accurate and up-to-date models, including probabilistic radio wave propagation, wireless interface adjusted according to the IEEE 802.11p draft (the envisioned technology) and realistic vehicular movement corresponding to fast-moving German highway scenarios. The obtained results show that in IEEE 802.11 DCF-based vehicular networks, one has to make sure that interference and packet collisions do not lead to a failure in the reception of safety-critical information. This effort represents a challenging task particularly when all safety-related messages share one wireless channel and the resulting load of periodic messages leads to a saturated network, as could easily happen in many critical vehicular traffic conditions.

Therefore, we propose two methods based on power control and contention mechanisms to shape data traffic such that messages are received with high probability where they are relevant. First, we propose a method based on a strict fairness criterion, D-FPAV, to control the load of periodic messages on the channel while ensuring a high probability of message reception within the safety distance of the sending vehicle. Second, we propose a method, EMDV, for fast and effective dissemination of emergency messages within a geographical area. Using the extended ns-2.28 simulator we show the merits of both approaches as well as of their synergies. Simulation results show that: *i)* D-FPAV is capable of improving the reception rates of periodic messages at close distances from the sender as well as increasing the probability of reception of emergency messages over a

wide range of distances between sender and receivers, *ii)* EMDV can deliver the emergency information to all nodes located in a geographical area with short delay and *iii)* when EMDV is used in combination with D-FPAV, the dissemination efficiency and delay are considerably improved.

Furthermore, we make use of the insight gained along the realization of this thesis to develop a set of design guidelines for an IVC protocol architecture. As a result, we obtain a system design tailored to the characteristics of safety-related IVC to be used as a basis for implementation.

The communication protocols and the system design proposed in this thesis have been adopted by the project Network on Wheels for the development of an inter-vehicle communications platform in an European prototype.

Acknowledgments

Working toward the realization of this thesis has been a fantastic experience in my life, a balanced combination of hard work, intensive learning and great fun. When looking back at the last three and a bit years of my life, I can certainly say that I am very happy that I made the decision to come to Karlsruhe for the development of my professional life and further my research. I am also certain that I would not have reached this point without the help of many people during the process. Their support and assistance are certainly reflected in this thesis, for which I am grateful.

First of all, I would like to thank Prof. Dr. Hannes Hartenstein who not only gave me the opportunity to join his research group in Universität Karlsruhe (TH), but has also been a great mentor. He encouraged me on my creative days and motivated me on the hard ones, guiding me towards the essence of research through honesty, respect and modesty. Thanks for all Hannes, you have been a constant inspiration on how to become a successful researcher and a better person.

During my time in Karlsruhe, I had the luck to be part of the excellent team of talented researchers of the Decentralized Systems and Network Services research group, also a group of friends. The hard work looks much easier when interacting daily with a group of motivated people who share the same vision and the same principles. I am glad to have shared this time with my colleagues Jochen Dinger, Moritz Killat and Felix Schmidt-Eisenlohr, as well as with my graduate students Jens Mittag, Tessa Tielert, Jon Letamendia-Murua and Steven Corroy, I have learned a lot with you and from you. I am also glad for the interaction with the 'newcomers', Thorsten Höllrigl, Mario Pink, Frank Schell and Horst Wenske, who added new perspectives to our group. I am thankful to Jochen for assuming the 'senior' role and keeping the group running smoothly. I am thankful to Moritz to keep the mood cheerful in our office. I am thankful to Felix and Jens for their commitment and great help on our joint efforts. Together we invested days, nights and weekends to achieve our ambitious goals and to meet our deadlines.

I would like to express my gratitude to Prof. Dr. Martina Zitterbart and her Telematics team at Universität Karlsruhe (TH) for their support. Such a large group provided me with the advantage of always having an expert on the field I needed in the 'next office'. I have special thanks for Frank Winter, our systems administrator, for his professionalism and support beyond his responsibilities. I also have special thanks for Astrid Natzberg, who kindly and efficiently assisted me with the administrative work. Then, I would like to thank Peter Baumung, Curt Cramer, Erik Blaß, Bernhard Hurler, Michael Conrad and Christian Vogt for the fun times during sports, coffee breaks, nights at the institute and diverse experiences in Washington D.C.

I would like to acknowledge the support of the German Ministry of Education and Research (BMBF) for the Network on Wheels (NoW) project under contract number 01AK064F, and the financial aid of NEC Deutschland. The NoW project has been a source of fruitful and inspiring discussions and collaborations. I would like to thank all my NoW colleagues and especially Holger Füßler and Matthias Transier from Universität Mannheim, as well as Dr. Andreas Festag, Ralf Schmitz and Roberto Baldessari from NEC Deutschland for making the work on the project a fun and successful experience.

Furthermore, the support from NEC Deutschland allowed me to travel to conferences around the world as well as to maintain fruitful international collaborations. I would like to thank Dan Jiang, who influenced me with his clarity and vision in inter-vehicle communications research during my time at DaimlerChrysler RTNA, Inc., previous to joining Universität Karlsruhe (TH). I would like to thank Prof. Dr. Raja Sengupta for inviting me to spend few months at U.C. Berkeley during my doctoral program. Prof. Sengupta and his skillful team at the California PATH Lab, with Paul Xu, Jeff Ko, Tony Mak and Anthony Patire, provided me with a great research experience in a fabulous environment. Paul, now my buddy, enlightened me with his kindness and life perspective, and also did me the favor of reviewing this thesis. I would like to thank Dr. Ken Laberteaux from Toyota Technical Center and Dr. Wieland Holfelder from DaimlerChrysler RTNA, Inc., who apart from sharing their knowledge and perspective with me, provided me the chance to participate in the organization of the ACM VANET workshops. I would like to thank very much Dr. Paolo Santi, from the Istituto di Informatica e Telematica del CNR in Italy, for accepting my invitation of collaboration. His expertise in wireless networks and exquisite research skills resulted in fruitful joint work which contribute on the most relevant parts of this thesis.

Finally, I would like to acknowledge the positive influence that all my friends and family have on my work. In particular, I would like to express my gratitude to my parents, Joan and Montse, who taught me the values and principles to grow up as a hard working person who could follow his dreams with self-confidence and determination but always with respect to others. They, together with my brother Eduard, my sister Montse, and their partners, Vero and David, make my live pleasantly easy, full of kindness and happiness with their unconditional support and encouragement.

Last –and definitely not least–, I thank my girlfriend Steffi who suffered my lack of free time the most but never lost her smile and kindness towards me. Steffi has been a great support and my constant link to the world outside of research. She kept my social live up and running and made me a very happy person during this period of time: Thank you very much Steffi.

Contents

List of Tables

List of Figures

1

Introduction to Safety-Related Inter-Vehicle Communications

The rapid evolution and cost reduction experienced during the last decade by wireless communication technologies have made them suitable for a wide spectrum of applications. In the field of Intelligent Transportation Systems (ITS), mobile communications can provide fundamental support to enable many active safety applications, which aim at avoiding or decreasing the severity of road accidents. The key benefit provided by wireless communications is the capability of making information available beyond the driver's (or other on-board sensors, e.g., radar) horizon of awareness.

The premise that wireless communications, referred to as inter-vehicle communications (IVC) in the vehicular field, can enhance road safety and efficiency have led governments and private entities to support several national and international projects around the globe. These projects investigate the performance of mobile communication technologies in vehicular environments and, in particular, of IEEE 802.11-based technologies referred to as 5.9 GHz DSRC (Direct Short Range Communications).

The major efforts dedicated to the development of IVC systems in the world are: the Vehicle Safety Communication Consortium (VSC) [VSC] and the Vehicle Infrastructure Integration initiative (VII) [VII] in the USA; the Car2Car Communication Consortium (C2CCC) [C2C] and the COMeSafety program [COM] in Europe; and the Advanced Safety Vehicle project (ASV), now in its fourth phase [ASV], and the InternetITS Consortium [Int] in Japan. The results of these initiatives, at the same time, are used by standardization bodies to define the basic system architecture and protocols to support road safety services. Currently, the IEEE 802.11p working group [WAV] is specifying a standard tailored to vehicular environments.

This thesis has been developed within the 'Network on Wheels (NoW)' [NoW] project which strongly collaborates with the C2CCC in an European framework. The NoW project started in June 2004, is partially supported by the German Ministry of Education and Research (BMBF), and joins the efforts of German industry and academia. The goal of the NoW project is to solve the key challenges regarding communication protocols and data security in the design of a communication platform for future inter-vehicle communications. Among the different fields of research covered by the NoW project, this thesis focuses on the design of appropriate communication systems and robust communication protocols to support active safety applications in vehicular environments.

Overview on safety-related inter-vehicle communications

Wireless communication technologies combined with vehicular on-board sensors (e.g., positioning systems, speedometers) can support road safety by two means: the periodic transmission of broadcast 'status' messages and the dissemination of event-driven messages. The first type of messages, also called *beacons* in this thesis, contain vehicles' status information such as position and speed vector. Upon reception of periodic messages issued by neighboring vehicles, a safety system is aware of its surrounding and is able to detect potential dangerous situations for the driver (e.g., traffic jam ahead). On the other hand, when an abnormal condition or an imminent peril is detected by a vehicle (e.g., airbag explosion), an event-driven message, also referred to as *emergency message*, is generated and disseminated through the vehicular network with high priority.

From a safety perspective, the main challenge for inter-vehicle communication technologies in the market introduction phase is to achieve a significant penetration rate of equipped vehicles [MML04]. However, IVC will be challenged more deeply in fully deployed, high density vehicular scenarios, where the load on the wireless channel must be carefully controlled in order to prevent the deterioration of the quality of reception of safety-related information.

In order to develop optimal solutions for inter-vehicle communications, the operating environment and the safety nature of this type of communications have to be taken into account. A vehicular network is characterized by specific node distributions and movement patterns, i.e., road-bounded and potential high mobility. Furthermore, vehicular environments present challenging characteristics to develop wireless communications. Multiple mobile and reflecting objects can lead to random attenuation of the received signal strength.

Safety applications are characterized by strong reliability and delay requirements as well as by the use of broadcast or geocast schemes, information is often addressed to all nodes located in a geographical area. Note that all vehicles in a node's surrounding can benefit from the safety-related information carried on the transmitted messages.

Main contributions of this thesis

This thesis makes contributions in the wireless communications field in general and in inter-vehicle communications in particular:

Enhancement of wireless communications modules of the network simulator ns-2.28 [NS2]: In order to provide the simulator with the desired level of realism, we examine and extend several of its models. Specifically, the channel access mechanism and the physical layer models are revised according to the IEEE 802.11 [11] and IEEE 802.11a [11a] standards as well as the IEEE 802.11p [11p] draft. Furthermore, the reception and interference modules are enhanced to better model the current wireless interfaces characteristics. Finally, vehicular movement patterns validated with German highway traffic are included.

Characterization of 802.11-based one-hop broadcast wireless communications: We perform a detailed simulation study of one-hop broadcast communications. The setup is typical for monitoring and safety-related applications where nodes exchange data with only its direct neighbors by means of broadcast messages, such as in vehicular networks. In this scenario, we analyze the effect of different values for the contention window, the system data-rate and the transmission power, as well as the impact of the channel model, the hidden terminal problem and channel access prioritization.

The performed analysis provides valuable insights on general principles on 802.11-based broadcast communications, especially when utilizing probabilistic radio propagation models.

Identification of relevant challenges and criteria for active safety communications: We define the application scenario for IVC and take into account the results of the simulation study in order to analyze vehicular networks with respect to the different types of communications supporting active safety.

We identify channel congestion as the main challenge for beaconing messages and stress the need of a strategy to carefully control it. A high load on the channel is likely to result in an increased amount of packet collisions and, consequently, a decreased 'safety level' as seen by the active safety application. Beacon messages are most relevant at close distances from the transmitter, and show a lower relevance at further distances according to the 'safety distance' of vehicles.

Additionally, we identify **fairness** as a required criterion for communication protocols in order to achieve safety. If a vehicle is not assigned a fair portion of the resources, it can not announce itself to its closer neighbors, and can become a danger itself.

Finally, predefined links are identified as the major cause of failure on the emergency dissemination in geographical areas due to their unreliability. An information dissemination strategy for event-driven messages is required which provides short delay and robustness against packet losses due to *i)* received power fluctuations, *ii)* packet collisions and *iii)* node movement.

Congestion avoidance by means of fair power control: We design a fully distributed strategy capable of controlling the transmission power of each node such that the channel load in a wireless network is kept under a given threshold. Due to the safety nature of the communications, the optimization criterion is to satisfy max-min fairness constraints: a higher transmit power of a sender should not be selected at the expense of preventing other vehicles from sending/receiving their required amount of safety information.

The proposed protocol, called D-FPAV (Distributed Fair Power Adjustment for Vehicular environments), is inspired by the Water Filling algorithm of Bertsekas and Gallagher [BG87] and is formally proven to achieve fairness. Simulation results show that D-FPAV can successfully control the beaconing load on the channel while: *i)* ensuring that the probability of beacon reception is high within the 'safety distance' of the sending vehicle, and *ii)* enhancing the probability of successful reception of event-driven messages over a wide range of distances to the sender.

Efficient dissemination of time-critical information: We propose a communication protocol to deliver time-critical information to nodes located in a geographical area which is robust against received power fluctuations, packet collisions and node movement.

Our protocol, called EMDV (Emergency Message Dissemination for Vehicular environments), requires that nodes are aware of their own position and the position of neighboring nodes by, e.g., the pro-active transmission of status messages. EMDV combines *i)* a contention-based scheme (inspired by the routing protocol proposed by Füßler *et al.* [FWK+03]) in order to reliably designate forwarding nodes, *ii)* a unicast-like addressing scheme in order to reduce the delay, and *iii)* a repetition strategy to improve reliability. Simulation results in highway scenarios show that the proposed strategy is suitable for emergency information dissemination in the presence of probabilistic radio propagation phenomena and with frequent beaconing messages sharing the channel.

To the best of our knowledge, our suite of protocols is the first 'comprehensive' solution for improving active safety communications in vehicular environments.

IVC system design: We develop a set of design guidelines for a modular architecture tailored to IVC requirements with low complexity to be used as a basis for implementation of vehicular communication systems. The main characteristics of the proposed design are: *i)* the fundamental protocol organization is layered and the processing of a packet is vertical through the layers, and *ii)* an information connector provides a clean interface to allow the sharing of information between protocol entities on each layer and vehicle sensors. Additionally, we specify the assignment of responsibilities to different layers, providing a scheme able to make an efficient use of the limited wireless resources and guarantee the compatibility between different types of IVC nodes, e.g., the ones with different computational capabilities.

Overview of this thesis

This thesis is structured as follows: Chapter 2 presents the underlying wireless technology to be used by IVC and outlines the focus of this thesis. We first describe the 5.9 GHz DSRC specifications, under development under the IEEE with the name of WAVE (Wireless Access in Vehicular Environments) [WAV], and sketch the current bandwidth allocation status in different parts of the world. In more detail, we describe the channel access mechanism necessary for the proper understanding of the performed analysis and the proposed protocols in the later chapters. Then, we define the different types of safety-related inter-vehicle communications and outline the general goal of this thesis, which consists in enhancing IVC performance to support active safety applications. Last, we specify the application scenario with the corresponding configuration parameters that can be found in IVC environments, which is used to develop this thesis.

For an accurate identification of relevant IVC challenges and prior to the design of IVC enhancing strategies, the performance of the corresponding wireless technology (IEEE 802.11p[11p]) has to be understood in detail. Chapter 3 presents a thorough simulation analysis of the performance of one-hop broadcast communications in vehicular environments. The main goal of this chapter is to obtain valuable insight in different setups of IVC and examine extreme working conditions. Previous to the analysis, we present our simulation framework for IVC, which consists in a set of modifications and enhancements to the network simulator ns-2 [NS2] to improve the degree of fidelity of its models as well as to adjust them with respect to the WAVE draft standards. At the same time, we introduce the required concepts and terminology common to wireless ad hoc networks research.

Chapter 4 utilizes the results obtained in the previous chapter as well as existing literature in order to identify the main challenges of safety-related IVC. We address the effects of the hidden terminal problem, the stringent mobility of the nodes, the received power fluctuations, the self organization and the high requirements of safety applications. This analysis, allows us to derive the required pieces to build a robust IVC system, which is the goal of this thesis. In particular, we point out the need of *i)* a versatile communication system design, *ii)* a strategy able to control the beaconing load on the wireless channel that guarantees a strict fairness, and *iii)* a strategy to disseminate time-critical emergency information, i.e., event-driven messages, in a robust and efficient manner. Furthermore, we outline the design criteria to be followed by both communication strategies.

In Chapter 5, we describe our two protocol proposals, D-FPAV and EMDV, outlined previously in this chapter. Afterwards, a simulation study is performed in Chapter 6 that evaluates the performance of both protocols in highway scenarios. The results obtained show how both protocols achieve their design goals. D-FPAV controls the beaconing load on the channel while maintaining fairness and high reception rates of periodic messages at close distances from the transmitter. EMDV disseminates in an effective and fast manner emergency information within a geographical area. Furthermore, we show the benefit of EMDV's operation when combined with D-FPAV, i.e., when the beaconing channel load is kept under control.

Chapter 7 presents the design guidelines for an IVC system architecture, as outlined previously. The goal of this chapter is to propose an IVC system architecture as a basis for implementation and to assign packet forwarding responsibilities into protocol layers.

Finally, Chapter 8 reports the conclusions that can be drawn from this thesis' results and provides directions for further research. Appendix A defines the link and physical layer parameters of 802.11p that are relevant for the simulator extensions. Appendix B provides a detailed description of the effect that hidden nodes have on broadcast reception rates with a deterministic propagation model.

The contributions of this thesis have been previously published in [TMJH04], [STMHE04], [FTMT+05], [TMSH05], [TMKH05], [SELMTMH06], [TMFH06], [TMSEFH06], [TMSH06], [TMM06], [FTMK+06], [SETMT+06], [TMCSEH06], [SETMMH07] and [TM07].

2
Enabling Vehicular Active Safety with IVC-Based Systems

Several projects, technologies and applications involving inter-vehicle communications (IVC) have been proposed in the last couple of decades. Moreover, commercial services enabled by wireless communication between vehicles and road side equipment (or road side units) have become quite popular in the late 90s. The CEN (European Committee for Standardization) DSRC [CEN04], operating at 5.8 GHz, is currently used for interoperable electronic toll collection systems in Europe, China, Australia and major South American countries.

However, IVC-based safety systems have not become a mass product due to several reasons. Among them was the lack of a dedicated frequency band and commercially available high-performance, low-cost radio hardware. These dissuaded the automotive industry from investing much resource in developing DSRC (Direct Short Range Communications) services to improve road safety.

In October 1999 though, the FCC (Federal Communications Commission) allocated, in the USA, 75 MHz spectrum in the 5.9 GHz range to be used by intelligent transportation systems [FCC99]. This dedicated frequency band and the corresponding maturity of WLAN (Wireless Local Area Networks) systems have encouraged governments, industry and academia, to join efforts with the premise that DSRC is an appropriate technology to enhance safety and efficiency on the road.

The results achieved by these efforts, in turn, are used by standardization bodies to define the basic system architecture and protocols to develop road safety services, e.g., the co-operation between ETSI ERM TG37 [ETS], ISO TC204 WG16 (CALM M5) [ISO], C2CCC [C2C] and IEEE P1609/802.11p (WAVE) [WAV].

In this chapter we present the enabling technology of IVC, 5.9 GHz DSRC, whose standardization effort is led by the IEEE WAVE [WAV] working groups. In more detail, we describe the IEEE 802.11-based channel access mechanisms, necessary for the understanding of the analysis and results presented in later chapters. In the second part of this chapter, we set the basis for the development of this thesis and define our focus as well as our general goal. To do this, we characterize safety-related communications with respect to their motivation and classify them in two categories, periodic and event-driven. Last, we outline the envisioned application scenario with the corresponding 5.9 GHz DSRC configuration parameters.

2.1 Underlying wireless communications technology

In this section, we provide an overview of the overall 5.9 GHz DSRC architecture, which is an OFDM-based (Orthogonal Frequency Division Multiplexing) technology under development at the IEEE under the name of WAVE (Wireless Access in Vehicular Environments). WAVE includes IEEE P1609.1 [9.1], IEEE P1609.2 [9.2], IEEE P1609.3 [9.3], IEEE P1609.4 [9.4] and IEEE 802.11p [11p]. Afterwards, we describe the basic mechanisms of the standards IEEE 802.11 [11] and 802.11e [11e] required to understand the strategies and results obtained in following chapters. First though, we present the current situation of the dedicated bandwidth allocation in different parts of the world.

2.1.1 Bandwidth allocation

As commented above, the USA already has a dedicated 75 MHz band, between 5.850-5.925 GHz. The FCC decided the use of microwave systems in the 5 GHz range due to their spectral environment and propagation characteristics which are suited to vehicular environments. Indeed, waves propagating in the 5.9 GHz band can offer high data rate communications for distances up to 1000 m with low weather dependence.

The whole band must be operated under licenses in order to avoid the delay and interference that undesired data traffic could cause to high priority safety-

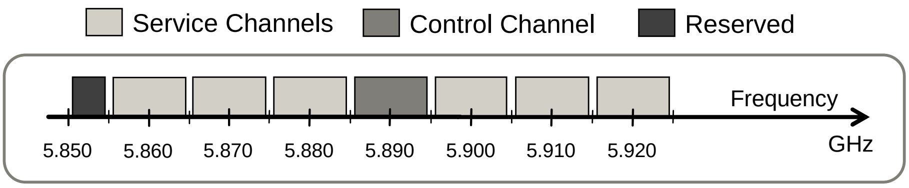


Figure 2.1: Spectrum allocation for intelligent transportation systems in the USA.

related applications. In order to accommodate different types of applications, the band is divided in eight different channels – one 10 MHz control channel (5.885-5.895 GHz, Channel 178), six 10 MHz service channels, and one 5 MHz channel that is held in reserve (see Figure 2.1). The control channel must accommodate the exchange of safety-related information as well as service announcements. The information transaction correspondent to non-safety related applications must take place on service channels. The decision to use 10 MHz channels for inter-vehicle communications, instead of the 20 MHz channels used in WLAN systems, was made to reduce the OFDM inter-symbol interference caused by multi-path propagation and achieve larger communication distances.

Contrary to the USA, Europe can not benefit from a dedicated band allocation yet. Currently, the ETSI (European Telecommunications Standards Institute) is leading the allocation effort and requires: *i)* 2x10 MHz bandwidth for high-priority safety-related applications based mainly on inter-vehicle communications, *ii)* 30 MHz for road safety and road management applications based mainly in communications between vehicles and roadside units, and *iii)* 20 MHz bandwidth for non-safety related applications.

For compatibility reasons with the USA assignment, the ETSI proposes the frequency range between 5.855-5.925 GHz to be allocated where a control channel should be centered at 5.880 GHz (see [ETS05] and [ETS06]). This harmonization would allow a global compatibility and interoperability of the systems.

In the far east, Japan and Korea intend to deploy inter-vehicle communication systems in the 5.8 GHz range. In China, although an interest in the WAVE standards exist, there is no known initiative in terms of spectrum allocation. Australia and major South American countries have not presented their intentions with respect to WAVE systems.

2.1.2 IEEE 1609 family

The IEEE is developing the 1609 family in order to provide compatibility between communication interfaces of different automotive manufacturers, and thus, encourage externally-driven services to vehicles. The IEEE 1609 family is composed of four draft standards which define the architecture, interfaces and messages to support secure wireless communications in vehicular environments, including vehicle safety. These draft standards combined with the specification of the Medium Access Control (MAC) and the physical layer (PHY) defined in IEEE 802.11p provide the complete set of future WAVE standards.

IEEE P1609.1 – WAVE resource manager

This draft standard [9.1] defines the services, interfaces and data flows corresponding to the WAVE Resource Manager. The WAVE Resource Manager is an application designed to enable the communication of remote applications, which are potentially located outside of the vehicular environment, with WAVE equipped vehicles.

IEEE P1609.2 – WAVE security services for applications and management messages

The motivation for this draft standard [9.2] is to protect WAVE communications from attacks such as eavesdropping, spoofing, alteration and replay, as well as to provide privacy to its users. It specifies secure message formats and their processing methods.

IEEE P1609.3 – WAVE networking services

This draft standard [9.3] sets the basis for a protocol architecture and defines services, operating at the OSI [Zim80] network and transport layers to support WAVE communications.

The WAVE architecture draft is composed by two planes (see Figure 2.2), a *Management Plane* (WME - WAVE Management Entity) used to configure and maintain the system, and a *Data Plane* which consists of the communication protocols and hardware used to deliver data. Additionally, the Data Plane provides two protocol stacks, Internet Protocol (IPv6) and WAVE Short Message Protocol (WSMP).

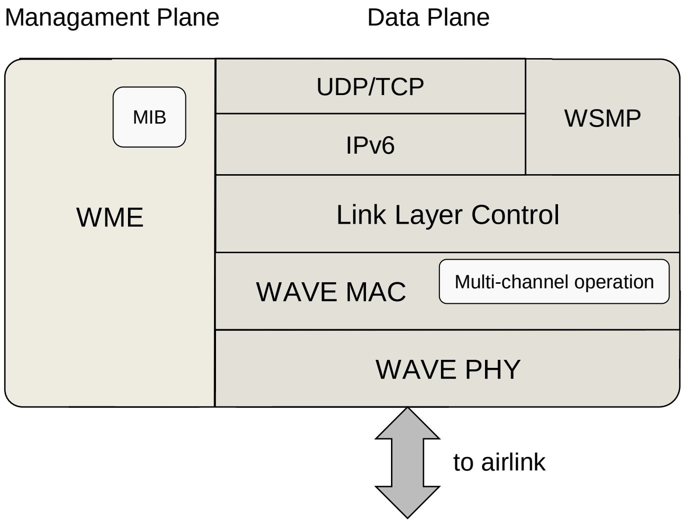


Figure 2.2: The WAVE architecture draft as depicted in IEEE 1609.3.

WSMP is a low overhead protocol designed to optimize WAVE operation, which permits applications to control physical parameters such as the transmission power, the data rate and the channel number.

On top of IPv6, although both TCP (Transport Control Protocol) and UDP (User Datagram Protocol) are supported, the latter one is expected to be used by most applications due to its low overhead and latency.

IEEE P1609.4 – WAVE multi-channel operation

This draft standard [9.4] specifies the operators and primitives designed to manage the different channels to be used by WAVE systems. The following services are described: channel routing, user priority, channel coordination and MSDU (MAC Service Data Unit) data transfer.

WAVE systems must support two types of channels, a *control channel* where WSM and WAVE service announcements are transmitted, and multiple *service channels* where the transactions corresponding to the different services take place. IP datagrams are not allowed on the control channel.

The channel coordination among WAVE devices is based on a coordinated universal time (UTC). Coordination among WAVE devices ensures that all of them will be monitoring the control channel during a common interval where safety information can be exchanged. The UTC could be provided by road side units or by GPS receivers, which typically provide a precise 1 PPS (pulse per second) with an error below 200 nanoseconds. In case no UTC is present, WAVE devices should not monitor other than the control channel.

Additionally, 1609.4 designates up to eight levels of priority to be used by the different applications using the mechanisms defined in 802.11e [11e].

2.1.3 IEEE 802.11p draft standard

IEEE 802.11p [11p] is a variant of 802.11a [11a] that modifies its MAC and PHY to support low latency vehicular communications. As the previously described WAVE draft standards, 802.11p is under development at the time this thesis is written. However, the basic characteristics and functionalities are provided, which are described in the following.

With respect to the MAC specifications, it adapts the IEEE 802.11 [11] standard to the requirements of WAVE environments. Due to the safety nature of WAVE communications, active scanning, passive scanning, or authentication and association procedures are not used. Additionally, it specifies that a WAVE device must monitor and operate on the control channel upon startup. WAVE devices can switch to service channels after the reception (or transmission) of a WAVE announcement frame.

The channel access mechanisms are, so far, inherited from IEEE 802.11 which specifies the DCF (Distributed Coordination Function) as the fundamental strategy in case of ad hoc communications, i.e., in the absence of a central coordinating entity. DCF is the dominant channel access strategy used to exchange safety information among cars and is explained in more detail later in this section.

EDCA (Enhanced Distributed Channel Access) is supported in order to differentiate different priorities among applications. The set of EDCA parameters specific to WAVE, which differs from the ones suggested in the 802.11e standard, are listed in Section 2.1.4.

The WAVE physical layer, which consists of a 10 MHz OFDM system, provides data payload communication capabilities from 3 to 27 Mbps. Also, the option to operate in 20 MHz channels is supported, what would double the mentioned data rates.

The WAVE PHY description indicates the transmitter and receiver specifications, such as the maximum power levels depending on the channel or the minimum sensitivity with respect to the data rate. The power value utilized for public safety in North America is specified with a maximum EIRP (Equivalent Isotropically Radiated Power) of 44.8 dBm. The intention is to provide communication distances up to 1000 m, when using the most robust modulations, i.e., the lowest data rates. Also, the WAVE OFDM PHY characteristics are specified, which are summarized in Appendix A. The main differences with respect to the values of 802.11a are the extension of the air propagation time (AirPropagationTime) and the slot time (SlotTime), as well as the introduction of the WAVE channel switching time (CHSwitchTime).

Distributed coordination function

The medium access mechanism of IEEE 802.11 in its ad hoc mode is the distributed coordination function, which is a form of CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), see Figure 2.3. This medium access protocol specifies that when a frame arrives at the MAC layer to be transmitted the status of the channel must be checked. If the channel is sensed idle at this point and during a DIFS (DCF Interframe Space) time interval, the station can proceed with the transmission. On the other hand, if the channel is busy, or becomes busy during that interval, the transmission is deferred using the backoff mechanism. The backoff mechanism is designed to avoid a collision with the station which is currently transmitting and with any other station which may be also waiting for the medium to become idle.

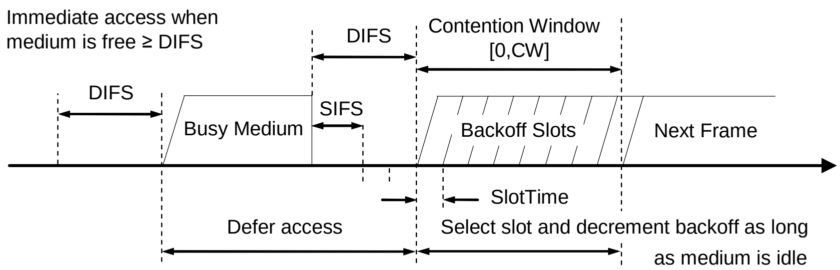


Figure 2.3: Distributed coordination function for channel access.

The backoff mechanism first sets the backoff timer with an integer random number of slots within [0,CW], where CW is the contention window size. The backoff timer is decremented by one unit for each slot time interval (SlotTime) that no medium activity is indicated until reaching 0. At this instant the station can transmit. If, on the other hand, the medium becomes busy before the backoff timer reaches 0, the process is suspended until the medium becomes idle again. However, before the backoff mechanism is allowed to start or resume decrementing the backoff timer, the medium has to stay idle for the duration of a DIFS.

After a transmitted frame a new backoff is performed even if there is no other frame waiting to be sent. This 'post' backoff ensures that the transmitting station will not have priority over any other waiting station, if any.

In unicast communications, the destination station must send an acknowledgment (ACK) frame following the successful reception of the message. The ACK is sent a fixed period of time after the reception of the DATA frame, which is referred to as short interframe space (SIFS). The SIFS, which is sensibly shorter than DIFS (see Table A.1) prioritizes the transmission of the ACK frame over any transmission from other stations.

Additionally, in order to reserve the medium a two way hand-shake is proposed prior to the DATA frame transmission. Figure 2.4 depicts the two additional frames RTS (Ready To Send) and CTS (Clear To Send) followed by DATA and ACK. Thus, the station intending to transmit a DATA frame, can send first an RTS frame to reserve the medium for the complete exchange, i.e., the four frames. Upon reception of the RTS frame, the destination station must wait for a SIFS period of time and then answer with a CTS. The DATA frame, can then be sent after another SIFS period from the moment the CTS frame is received. Any other station receiving the RTS or CTS frame will set their NAV (network allocation vector) to the time left until the exchange is completed, not being allowed to transmit during this period.

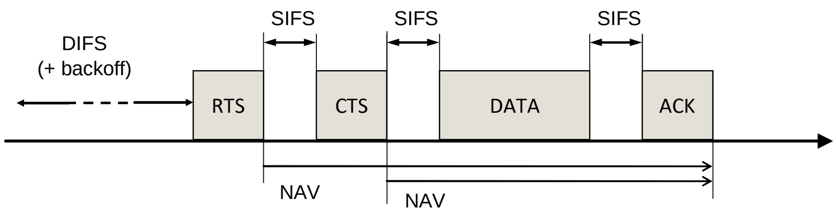


Figure 2.4: Unicast channel reservation and acknowledgment exchange scheme.

The RTS/CTS exchange intends to avoid packet collisions caused by the hidden node problem. A potential hidden node is any station which is located out of range[1] of the transmitting node but close enough to the destination one so it can disturb an information exchange with a simultaneous transmission. The impact of the hidden nodes on a broadcast environment is analyzed in Chapter 3 and addressed again in Chapter 4.1.

In case the CTS or the ACK frames are not successfully received, the exchange is determined to be failed. The transmitting station can use its MAC-level recovery mechanism which will repeat the procedure in order to retransmit the DATA frame up to a certain number of times[2], after performing a new backoff and read-

[1]Out of range in this context refers to a location where a transmission from another node can not be sensed on the medium and, therefore, it does not prevent a station from transmitting.

[2]The default maximum number of retransmissions defined in IEEE 802.11 is 4 for frames larger than 3000 Bytes and 7 for shorter ones.

justing the CW value. The CW is initially assigned to CW_{min}, and is increased by the following expression:

$$2x(CW + 1) - 1,$$

in each transmission failure with an upper limit of CW_{max}.

Broadcast messages do not reserve the medium before the DATA frame transmission and are not followed by a corresponding ACK. Note that there is no specific node addressed by the transmitted message. Therefore, two special considerations must be taken into account when focusing on broadcast messages. The first one is that there is no MAC-level recovery mechanism for broadcast frames and, thus, the value of the contention window CW will not be increased. Secondly, since the RTS/CTS exchange is not used, the hidden node problem is not alleviated.

In vehicular environments both types of addressing, uni- and broadcast, are expected to be utilized. However, broadcast communications, or the variant addressing all nodes within a geographical area (commonly known as geocast), are expected to be the fundamental addressing scheme utilized by safety-related applications.

2.1.4 Prioritized channel access

The wireless LAN standard IEEE 802.11 proposes with its enhanced distributed channel access (EDCA) [11e] a strategy to provide differentiated channel access to data traffic with eight different priorities.

These priorities are classified in four different access categories (AC) which have an independent queue, each with their corresponding configuration parameters. AIFS[AC] (Arbitration InterFrame Space), CW_{min}[AC] and CW_{max}[AC] are utilized for each access category instead of the basic channel access mechanism values DIFS, CW_{min} and CW_{max} respectively.

The AIFS[AC] is determined as follows:

$$AIFS[AC] = aSIFSTime + AIFSN[AC] \times aSlotTime,$$

where AIFSN (AIFS Number) is fixed by the access categories. The corresponding configuration values proposed by IEEE 1609.4 to be used in the control channel can be found in Table 2.1.

All outgoing traffic must be mapped into one AC and, therefore, introduced in their corresponding queue, see Figure 2.5. Each queue is a single EDCA entity and computes a backoff timer independent from the other queues with its corresponding configuration parameters. The AC with shorter backoff timer accesses the medium first, after all queues contend for the medium with the other stations. In case two or more queues finalize their contending period simultaneously, the frame with higher priority is transmitted.

Note that with this mechanism, a frame with lower priority may access the medium with a shorter delay due to the 'virtual internal contention'. As mentioned

AC	CW$_{min}$	CW$_{max}$	AIFSN
0	aCW$_{min}$	aCW$_{max}$	9
1	(aCW$_{min}$+1)/2 - 1	aCW$_{min}$	6
2	(aCW$_{min}$+1)/4 - 1	(aCW$_{min}$+1)/2 - 1	3
3	(aCW$_{min}$+1)/4 - 1	(aCW$_{min}$+1)/2 - 1	2

Table 2.1: Configuration values for the WAVE enhanced distributed channel access (EDCA) mechanism when utilized in the control channel.

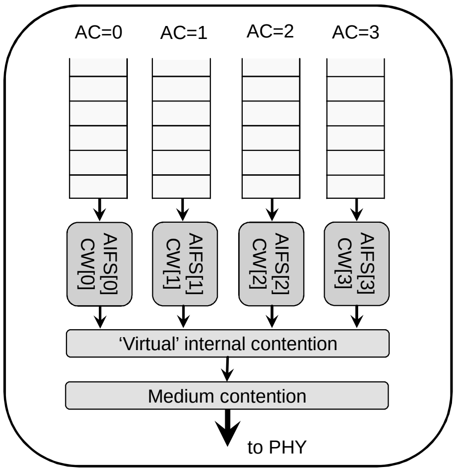


Figure 2.5: EDCA access category queues for one WAVE channel.

above, this draft standard is not finalized yet. Therefore, a deterministic priority mechanism strictly prioritizing an AC over the others could still be adopted in case safety applications would require it.

2.2 General goal of this thesis

There exist a wide range of candidate applications which are being considered for future inter-vehicle communications. These applications can be divided in two main categories according to their final goal: *safety* and *non-safety*.

In this thesis, we focus on wireless communication protocols and systems designed to support active safety applications which, in turn, assist drivers to reduce accidents and fatalities on roads. These communication protocols must be designed in order to satisfy strong requirements in terms of awareness. Each vehicle must be aware of, or in other words, obtain the status information, about its surrounding with the required promptness in order to avoid a potential danger.

Non-safety applications can be of many diverse types such as vehicular traffic efficiency, entertainment, information download, remote vehicle diagnosis, etc. All these applications can add a significant value to the end user, especially in the introductory phase of the 5.9 GHz DSRC technology when a small number of vehicles are equipped. However, their requirements differ from the ones of safety applications and are not addressed in this thesis.

Wireless technologies can support road safety applications by two means: by the periodic transmission of 'status' messages of each node and by the dissemination of 'hazard' messages once a potential danger has been detected.

The first type of messages, called *periodic messages* or *beacons* in this thesis, are transmitted in a broadcast fashion and contain vehicle's status information such as position, speed and direction. Periodic messages are exchanged by neighboring vehicles and can be considered as a preventive safety strategy: upon reception of beacons issued by neighboring vehicles, a safety system is aware of its surrounding and is able to detect potential dangerous situations, e.g., at intersections or highway entrances with low visibility, see Figure 2.6. Note that the beaconing mechanism can also be fundamental to enable non-safety applications (e.g., road traffic monitoring), or to support protocols (e.g., geocasting). However, the main goal of periodic messages is to provide up-to-date status information, or awareness, about all surrounding vehicles.

In this thesis, we are interested in mechanisms capable of ensuring the successful reception of 'status' information from surrounding nodes under all network conditions. Special attention is devoted to the challenges present in scenarios where high vehicular speed is found with a high level of channel saturation, since they might be critical situations from a safety point of view.

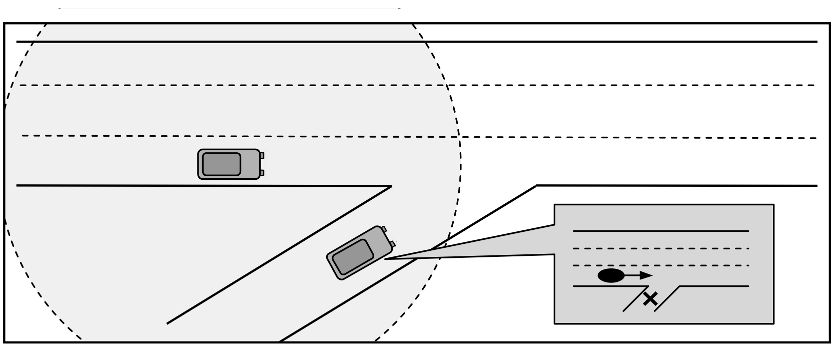


Figure 2.6: Exemplary road situation where the existence of periodic messages can assist the driver in low visibility conditions. The vehicle entering the highway is aware of the near vehicle when it receives a beacon. The shaded circle represents the direct communication range of the vehicle driving on the highway.

The second type of messages, called *event-driven messages* in this document, shall rapidly and reliably disseminate information of a hazard to alert other drivers of an imminent peril. The dissemination of the information will be originated by a node detecting a potential dangerous situation, e.g., a high deceleration or a car crash, and should be forwarded by other nodes in order to disseminate the information into larger geographical areas than the direct communication range, see Figure 2.7. The key aspect of the dissemination techniques is how to select appropriate forwarders to efficiently provide the required reliability and satisfy the delay constraints within a geographical area.

There exist different types of hazards depending on the safety risk involved. Clearly, information regarding a slippery road five kilometers ahead and information regarding a car crash just occurred fifty meters ahead should be treated with different priority and communicated following different requirements, or even with different strategies. Our interest in this work focuses on the latter case, which is related to imminent collisions and are referred to as *safety-of-life* situations in the DSRC Industry Consortium [DSR05]. In these situations, the rapid dissemination of emergency information is required to take immediate driving measures. Therefore, from this point on we will refer to as event-driven messages the ones used to deliver emergency information within a specific area in a reliable and rapid manner due to a safety-of-life hazard.

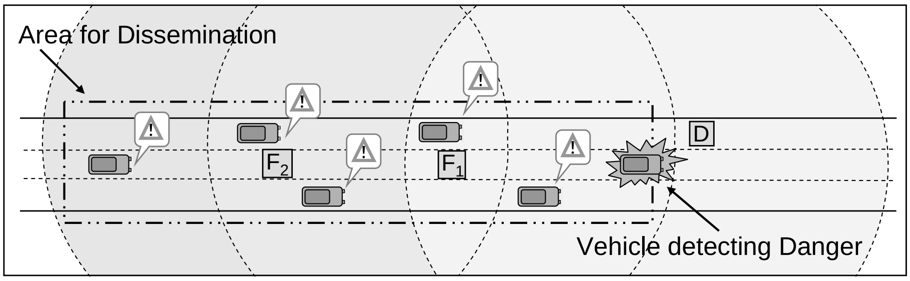


Figure 2.7: Exemplary road situation where vehicle D detects a hazard and issues an event-driven message. Vehicles F_1 and F_2 forward the message to cover the area of dissemination where the information is relevant. The shaded circles represent the direct communication ranges of the nodes originating and forwarding the event-driven message, D, F_1 and F_2.

Note that road side units could also take part and improve inter-vehicle communications' performance. This type of stations could serve as a relay or information originator, however their benefit is not addressed in this thesis.

In summary, the goal of this thesis is to provide the required inter-vehicle communication protocols and systems capable of supporting active safety applications achieving the following objectives: *i)* detecting dangerous driving situations and *ii)* informing other vehicles about detected emergencies. The detailed design criteria of our protocol proposals are derived in Chapter 4, which take into consideration the insight gained by the simulation analysis performed in Chapter 3.

2.3 Specification of the IVC system setup

Designers of safety applications have not yet agreed on a standardized set of safety requirements nor does a standardized set of IVC applications exist to improve safety on roads. Therefore, it is not possible to design or evaluate safety-related communication strategies according to a common set of specifications. However, reliability, robustness, delay and fairness present the basic set of parameters to measure the quality of a safety communication protocol and are taken, therefore, as design criteria for our protocol proposals (see the definition of our evaluation metrics in Chapter 4).

In the following, we present the different DSRC configuration values that can be found in the literature and can be used as guidelines, which we utilize to define our nominal setup later. Table 2.2 presents a summary of the described parameters and their values.

Parameter	**Value**
Transmission data rate	from 3 to 27 Mbit/s
One hop communication distance	up to 1000 m
Beaconing generation rate	up to 20 packets/s
Packet size	from 250 to 800 Bytes
Dissemination distance	up to few km (time-critical information)

Table 2.2: Configuration values for inter-vehicle communications.

As described in the IEEE 802.11p [11p] draft, we assume the utilization of 10 MHz channels, which provide data rates from 3 to 27 Mbps. Lower data-rates are preferred for safety applications due to their robustness against noise and interference [MFW05]. Indeed, it is assumed a default data rate of 6 Mbps for the exchange of safety information, e.g., [DSR05] and [CJTD06].

The IEEE 802.11p [11p] draft also specifies that IVC will occur over distances up to 1000 m between high-speed vehicles. According to previous studies, such as [XMKS04] or [RRR05], it is envisioned that several messages per second from each vehicle will be needed in order to provide the required accuracy for safety applications. The authors of [XMKS04] derive a minimum of 2 and a maximum of 20 packets/s (a period of 50 ms) from vehicle driving speeds and driver reaction times [OS86]. Also, system latencies below 50 ms are specified by the DSRC Industry Consortium prototype team [DSR05]. The size of a safety message is relatively large, between 250 and 800 Bytes depending on the utilized PKCS (Public Key CryptoSystem), due to security-related overhead (i.e., digital signature plus a certificate), see [RH05].

In case of an existing hazard, the emergency (time-critical) information should be disseminated with minimum delay at distances up to a few kilometers in order to allow a proper coordination and prompt reaction of the drivers, e.g., 1 mile according to [STC+06] or 5 km according to [BSH00]. Clearly, this information can be relevant for further distances also, and could be disseminated with lower requirements to larger areas.

Finally, we recall that although WAVE is a multi-channel approach, a multi-transceiver solution is not yet being considered, due to cost reasons. Additionally, the FCC recently reserved one channel, 5.855 to 5865 GHz, for high availability, low latency vehicle safety communications [FCC06], where non-safety data traffic can not be exchanged. Therefore, according to the one-transceiver approach and due to our focus on safety critical situations, we consider the case in which nodes operate continuously in one single channel where only safety-related communications take place.

3

Simulation Analysis of IVC: Periodic One-Hop Broadcast

As specified in the previous chapter, the goal of this thesis is to design robust communication protocols and systems to support vehicular active safety applications. In order to identify the relevant challenges of inter-vehicle communications (IVC) and propose appropriate solutions, the performance of the underlying wireless technology has to be understood in detail. In particular, we are interested in identifying and analyzing critical working conditions from a safety perspective.

In this chapter, we study the performance of IEEE 802.11p [11p] by the analysis of the basic strategy to exchange status information in vehicular networks, which makes use of periodic one-hop broadcast messages. These messages, also called beacons, contain updated status information acquired by the on-board sensors of the transmitter. Beacons are periodically generated and each of them is sent only once to the channel due to their broadcast fashion, i.e., there is no default reliability mechanism that would re-transmit the message in case of packet or frame collision.

We set up a vehicular scenario with different configurations outlined in Chapter 3.4 in order to observe the working conditions of the wireless network. Additionally, we evaluate the performance of the EDCA mechanism to see the benefit of utilizing an access category with a higher priority. The goal of this analysis is twofold: *i)* obtain valuable insight on the performance of IVC (which is used in Chapter 4 to define the main challenges faced by safety-related IVC), and *ii)* identify the IEEE 802.11p configuration values appropriate for our scenarios, especially for the ones where a high vehicular speed can be encountered with a high load offered to the channel.

In order to perform our analysis, an extended implementation of the network simulator ns-2.28 [NS2] is utilized. Simulators are a valuable tool to evaluate the performance of wireless communication protocols. On the one hand, analytical models are sometimes not sufficient to perform detailed studies without the need of idealistic assumptions. On the other hand, real world testbeds with the desired dimension are not a feasible option due to their elevated cost and required effort in the case of vehicular networks.

However, the development of a proper simulation framework for inter-vehicle communications is not straightforward. One must take into consideration all technological and environmental aspects in order to perform simulations with the desired 'closeness to reality'. Appropriate and up-to-date models are critical in the simulations of IVC due to the expected extreme working conditions, i.e., amount of nodes, amount of wireless load and the robustness required by the challenging goal of improving safety.

We devote special attention to the random characteristics of the radio channel which is often omitted in wireless networks research. While the hidden node problem is usually treated as well understood, it changes its shape when we look at it in the presence of realistic radio propagation phenomena. Indeed, there exist as many wireless channel conditions as different environments. These situations are modeled with different radio propagation models, deterministic or probabilistic, with adjustable parameters that can affect the communication performance in diverse manners. With probabilistic radio propagation, hidden nodes can appear much closer to a sender than typically expected with a deterministic model.

Before presenting the results obtained from our analysis, we present the main extensions and enhancements that were implemented to the network simulator ns-2.28 [NS2] in order to improve its accuracy to model inter-vehicle communication systems. Additionally, we define the main metrics utilized to evaluate IVC performance, including the performance of the protocols proposed later in this thesis, see Chapter 6.

In the following section, we outline the most relevant studies related to our work addressing one-hop broadcast communications, prioritized channel access and the improvement of simulation tools for wireless and inter-vehicle communications.

3.1 Related work

Wireless ad hoc networks and their hidden node problem have been an intense field of research for many years. Performance measures have been analyzed using both event-based simulators and analytical approaches that modeled these types of networks under different conditions.

As early as 1975, [TK75] treated analytically the hidden node problem in an ALOHA system using a deterministic radio model. Later, [Bia00] presented an analytical model of the 802.11 DCF able to estimate the throughput of unicast flows assuming a deterministic channel model. This work was extended in [GK04] which took into account channel errors modeled as a 2-state Markov chain, retransmissions and multi-hop communication.

Addressing the performance of broadcast communications we can find studies such as [CSK05], which analytically modeled a broadcast scheme and addressed the achievable throughput in the sense of the fraction of time that the channel is successfully transmitting user data. In [LNM04a], an analytic model is proposed that predicts the optimal range for maximizing 1-hop broadcast coverage.

However, all the studies mentioned above assumed an optimal coordination among neighboring nodes when accessing the medium. Indeed, the variety of possible communication states needed to be modeled when taking into account probabilistic radio propagation make a deep analysis highly complex.

Similar to the analytical approaches, simulation studies often assumed unicast flows and idealistic radio conditions. A broadcast study introducing a random behavior of the propagation model is [LNT02], which introduces 'communication gray zones' as regions where severe packet loss is experienced. This study focuses on AODV (Ad hoc On-Demand Distance Vector) routing flows in an in-door scenario and does not, therefore, present the characteristics of a vehicular network.

Broadcast communications in the vehicular field are addressed in [XMKS04], where the performance of several layer-2 repetition strategies is evaluated in terms of number of updates per period of time and probability of reception failure for different fractions of channel capacity assigned to this type of messages. Furthermore, they identify 'infeasible regions' (situations) where potential safety applications' requirements cannot be satisfied due to technological limitations. However, their assessment is based also on a wireless channel with deterministic properties, which does not provide the insight we intend to obtain with our study.

We analyzed different broadcast scenarios in several studies where different protocol configurations and propagation models were utilized [TMJH04], [TMM06], [TMCSEH06] and [SETMMH07].

In terms of prioritized channel access, most of existing work aims to characterize or improve unicast flows. The simplistic or idealized scenarios addressed in these papers, however, make it difficult to apply their results into vehicular networks. In this category we can find interesting analytical studies that model the most important EDCA parameters, e.g., [AC01] and [ZC03], which either do not consider or consider briefly the relevant issue of the hidden node problem. Other studies addressing unicast flows propose service differentiation strategies which are not valid for dynamic topologies since they require a period of time in order to tune the protocols, e.g., [KLS$^+$02] and [RNT03]. Prioritized channel access has been treated in vehicular environments within the Fleetnet project [Fle] with [Lot02] and [MLJ03]. However, the selected radio interfaces for these studies were based on UMTS (Universal Mobile Telecommunications System) terrestrial radio access, time division duplex technology. They make use of synchronized slotted superframes and, thus, are not comparable to CSMA/CA. We addressed the performance of the EDCA mechanism in vehicular one-hop broadcast scenarios in [TMJH04].

Due to the increasing interest generated by vehicular networks, we can find recent efforts, in parallel to our work, proposing improved models to evaluate IVC appropriately. Indeed, inter-vehicle communications are different from other wireless communications in terms of mobility, radio propagation phenomena and application (safety) requirements.

With respect to node mobility, Choffnes et al. [CB05] proposed street-bounded node movement and showed the unsuitability of random two-dimensional movements for studying communication protocols in vehicular environments. Since then, other simulation tools where published that provided movement patterns for vehicular environments, e.g., [HFFB06] and [VO07]. In our simulation platform we make use of the highway movement patterns proposed in [FTMK$^+$06] which are described in Section 3.2.4.

Other modeling work addresses the inaccuracy of the ns-2.28 wireless channel as well as its reception and interference model. Xiuchao [Xiu04] describes how to add an error model based on BER (Bit Error Rates). Yin *et al.* [YEY$^+$04] derive BER curves tailored to IVC by implementing a realistic channel simulator and adjusting it with values found in the literature. Also addressing vehicular communications, Chen et al. [CJTD06] developed an improved reception model of the ns-2.28 simulator with a better software design. Their implementation includes a physical layer state machine which allows managing the signal and interference of OFDM systems as well as cumulative noise capabilities. Their implementation includes the Nakagami fading model that they previously suggested in [TJM$^+$04] after verifying and adjusting it with empirical data collected on USA highways. Their channel fading model is adopted for the studies of this thesis. The result of their work is a simulator adjusted to 5.9 GHz DSRC including the modeling of all IEEE 802.11p supported data rates. However, their implementation does not include the improved capture effect (see Section 3.2.1) which we believe is required for a proper evaluation of wireless broadcast communications. The extensions that we realized to the network simulator ns-2.28 are reported in [SELMTMH06], [SETMT$^+$06] and [SETMMH07], and are summarized in the next section.

Note that ray tracing techniques, although more accurate to model the radio channel e.g., [MFW05], make the simulation of networks of hundreds of nodes infeasible due to their high computational cost.

3.2 Simulation framework for IVC: extended ns-2.28

In this section, we present the developed simulation platform for the design of inter-vehicle communication protocols. The core building block is the network simulator ns-2.28 [NS2] which is a widely used tool in the field of computer networks research. Moreover, we have modified and extended many modules of the standard distribution of ns-2.28 in order to provide our simulations with a higher level of fidelity with respect to current development status of inter-vehicle communication systems. The main blocks modeling inter-vehicle communication technology and environments are: *a)* a reception model with improved capture capabilities according to current chipsets; *b)* a fading radio propagation model selected according to empirical data; *c)* adjusted medium access control and physical models according to the IEEE 802.11p draft [11p]; and *d)* realistic highway movement patterns validated with German highways' traffic.

In the following, we describe separately each building block in more detail in order to provide the required background to understand the simulation results presented in later chapters. Additionally, the modifications and extensions implemented in the ns-2.28 simulator are justified and outlined. A detailed description of our ns-2.28 modifications can be found in two technical reports, [SETMT$^+$06] and [SELMTMH06].

3.2.1 Reception and interference model

When analyzing the performance of wireless networks via simulation, the implementation of the reception and interference models has to be well understood. The network simulator ns-2.28 manages the reception of messages using three power level thresholds. These are implemented in the standard distribution of ns-2.28 and can be described as follows (we assume all power values to be expressed in dB):

– *Carrier Sense Threshold (CSTh)*: Any node is able to sense a transmission of another station if the signal arrives with a power higher than CSTh. In this case, the wireless interface sets the state of the channel as busy. Any transmission arriving at a node's location with power below CSTh is not sensed and is discarded immediately by the simulator.

– *Reception Threshold (RxTh)*: Any node is able to successfully receive another station's transmission, in the absence of other nodes' signals, if the signal arrives with power higher than RxTh.

– *Capture Threshold (CpTh)*: A packet (with power above RxTh) can be successfully received in the presence of interferences if: *i)* the packet arrived at the interface while the channel is idle, and *ii)* the power of the packet is CpTh above the power of the strongest interfering signal. A packet arriving while the channel is sensed busy can not be successfully received.

As pointed out in existing studies, e.g., [TMB01], ns-2.28 has lower accuracy in its lower layers' modules in comparison to other network simulators. In our implementation, we modified the way the reception of a signal is handled with respect to interference in order to better model reality. First we implemented cumulative noise capabilities. The original ns-2.28 code does not keep track of all ongoing messages at a node's interface, i.e., it does not accumulate the power level of all ongoing interferences. As depicted above, a message is determined to be successfully received if its power is CPTh higher than the strongest interfering signal. As other network simulators already do, e.g., GloMoSim [Glo], we accumulate the power of all interferences signals together with the existing background noise ($\mathtt{Noise}$), in order to determine if the reception of a message is successful. Assuming that the co-channel interference in a OFDM system, such as IEEE 802.11p, behaves similar to AWGN noise, we set the CpTh value to the required SINR (Signal to Interference plus Noise Ratio) specified for each modulation. Now, a message is determined to be successfully received if during the complete reception time the following inequality is satisfied:

$$P_r \geqslant I + CpTh, \tag{3.1}$$

where P_r is the power of the received message, I corresponds to the cumulative power level of all existing interferences plus $\mathtt{Noise}$, and all powers are expressed in dB. In order to have a higher level of accuracy, we take into consideration all signals arriving at the interface with a power higher than $\mathtt{Noise}$, instead of discarding signals below CSTh as in the original ns-2.28. The finite state machine implemented to model cumulative noise has been validated by setting up a table of all possible combinations of triggers and conditions for each state, eliminating non-feasible combinations and determining the finite state machine's transactions to the remaining ones.

We also modified the capture feature since the standard distribution of ns-2.28 only allows a message to be captured if it arrives when the channel is idle. According to current wireless chipsets' capabilities [KVSA04], our implementation also allows to successfully receive a message that arrives during a busy period of the channel as long as the inequality (3.1) is satisfied. In this case, however, the second packet can not be received correctly if it arrives between 4 and 10 μs after the previous one due to resynchronization issues[1].

The configuration values of the thresholds described above, corresponding to IEEE 802.11p's default data rate of 6 Mbps [ETS05] are reported in Table 3.1. Apart from the data rate of 6 Mbps, also 3 Mbps is addressed later in the chapter due to its robustness and, therefore, its corresponding thresholds are also included in Table 3.1. A data rate of 3 Mbps requires the lowest SINR (signal to interference plus noise ratio) to successfully receive a message, namely 4 dB.

[1] The physical layer model of our ns-2.28 implementation is configured according to the values obtained from private conversations with the electronics company Siemens within the 'Networks on Wheels' project [NoW].

Parameter	Value
6 Mbps data rate: Reception Th. (RxTh) Capture Th. (CpTh)	 -92 dBm 7 dB
3 Mbps data rate: Reception Th. (RxTh) Capture Th. (CpTh)	 -95 dBm 4 dB
Carrier Sense Th. (CSTh)	-96 dBm
Noise	-99 dBm

Table 3.1: Configuration values of the reception and interference models configured in our extended version of ns-2.28 for data rates of 6 Mbps and 3 Mbps.

3.2.2 Radio propagation model

In order to obtain valuable results, not only the transceiver technology model has to be correctly implemented but also the radio propagation characteristics have to be carefully modeled.

In a real scenario, the attenuation of a transmitted signal is characterized by the effect of path loss and fading. Path loss can be defined as the attenuation caused by the free-space loss together with the interaction caused by reflections, diffractions or scattering between the radio waves and the environment. Fading phenomena consists of the distortion of the transmitted signal that is caused by the movement of the environment relative to the sender along the time.

In the literature [Rap02], models that estimate the attenuation of a transmitted signal in the wireless channel are classified as deterministic and probabilistic. The latter ones are characterized by an attenuation that follows a probabilistic distribution, which estimates the variation over time of the signal power at specific transmitter-receiver distances. Deterministic models estimate the average attenuation and predict a fixed value for a given transmitter-receiver distance at any time.

Previous studies, such as [TMSEFH06], [BM05], [TMJH04], [STMHE04] and [TMB01], have shown the significant difference of using a deterministic propagation model, which assumes a fixed received signal strength at a fixed distance, in comparison to probabilistic ones which include fading phenomena.

The standard distribution of ns-2.28 offers three radio propagation models, two deterministic (the free-space model and the two ray ground model) and one probabilistic (the log-normal shadowing model).

The free space propagation model estimates the received signal power at a receiver assuming that the signal propagates only on one clear line-of-sight path. The two ray ground model[2] derives the signal attenuation modeling the direct

[2]The two ray ground model implemented in ns-2.28 is a simplification of the commonly known model in the electromagnetic radio waves propagation field.

path of radio waves between sender and receiver as well as one reflection on the ground. Both of them predict a signal attenuation as a deterministic function of the distance to the transmitter assuming no change in the interface configuration, e.g., carrier frequency or antennas' gains.

The log-normal shadowing (LNS) models the path-loss of radio waves relative to a reference distance and the shadowing effect of the possible variations of the environment, i.e., obstacles or relief. LNS uses a log-normal random variable to reflect the variations of the received power and is characterized by two parameters, the path loss exponent β and the shadowing deviation σ.

Besides the ones used in ns-2.28, there exist many other radio propagation models in the literature. Among them, the Nakagami distribution [Nak60] is utilized and suggested by many authors as a suitable model to estimate the physical propagation phenomena of mobile communication channels due to the good match with empirical data collected from mobile communications experiments, such as in [SMSA00], [BD91], [Zha99] and [LZG04] . Recently, Taliwal et al. performed real world tests on highways and suggest the use of the Nakagami fading model for these type of vehicular scenarios [TJM+04]. Furthermore, they implemented the model into ns-2.28, which we use in this thesis.

Therefore, we select the Nakagami fading model to perform our simulation studies and, additionally, the two ray ground implementation from the standard distribution of ns-2.28 for comparison.

Two ray ground implementation in ns-2.28

The two ray ground model, as implemented in ns-2.28, is often used in the evaluation and characterization of wireless communication protocols due to its simplicity. As commented above, it is deterministic and estimates the average signal reception power considering the direct path and one reflection on the ground. The two ray ground model predicts two different values of the path loss exponent depending on the distance between sender and receiver, which changes from 2 to 4 at a specific distance commonly referred to as cross-over distance (d_c):

$$d_c = \frac{4\pi h_t h_r}{\lambda} \tag{3.2}$$

where h_t and h_r are the antenna heights of the transmitter and the receiver respectively and λ is the carrier wavelength. The cross-over distance identifies where the signal changes from following a free-space propagation to being influenced by the ground reflection. The expressions to compute the average received power, at a distance d from the transmitter, according to the two ray ground model are the following:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \qquad \text{if} \qquad d \leqslant d_c \tag{3.3}$$

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L} \qquad \text{if} \qquad d > d_c \tag{3.4}$$

where P_t is the power that the signal was transmitted with; G_t and G_r are the antenna gains of the transmitter and the receiver respectively; and L is the system loss. Table 3.2 reports the configuration values required by the two ray ground model used in all our simulations, except the transmission power which varies for different experiments.

Parameter	**Value**
Antenna gain (G_t and G_r)	2.512 dB
Antenna height (h_t and h_r)	1.5 m
Carrier wavelength (λ)	50.85 mm
System loss (L)	1

Table 3.2: Configuration values to compute the reception power with the two ray ground model in inter-vehicle communication scenarios.

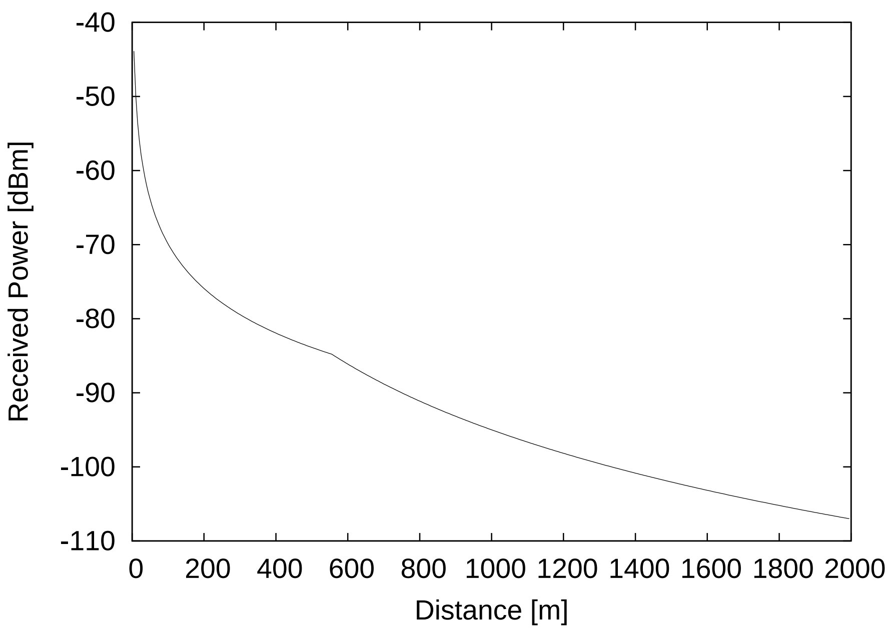


Figure 3.1: Received signal power with respect to the distance to the transmitter computed by the ns-2.28 implementation of the two ray ground propagation model.

Figure 3.1 presents the deterministic values of the received signal power expressed in dBm with respect to the distance assuming a transmission power of 9.95 dBm. It is worth noting the strong decrease suffered by the transmitted signal, following the inverse square law, at short distances from the sender, i.e., up to 200m. This behavior results in the known 'near-far effect' that refers to the situation where a node R is close to one specific transmitter T_1 and further away from another one T_2 when both are simultaneously sending a message to the wireless channel. In the case that both messages are transmitted with the same power, T_1's message can be successfully received (captured) by R since its signal received power is much higher than the one from T_2.

Due to its deterministic nature, the two ray ground model, together with the threshold based reception model of ns-2.28 (see Section 3.2.1) results in a model commonly referred to as *Disc Range* model. Consequently, given a transmission power one can derive two widely utilized concepts in wireless communications research:

- *Carrier Sense Range (CS):* Given a transmission power, the CS is the distance up to which a node's sent message can be sensed by another station, i.e., $RxPower \geqslant CSTh$. In other words, a transmission prevents nodes in its CS range from sending.

- *Communication Range (CR):* Given a transmission power, the CR is the distance up to which a node's message can be successfully received by another station in the absence of other nodes' interferences, i.e., $RxPower \geqslant RxTh$.

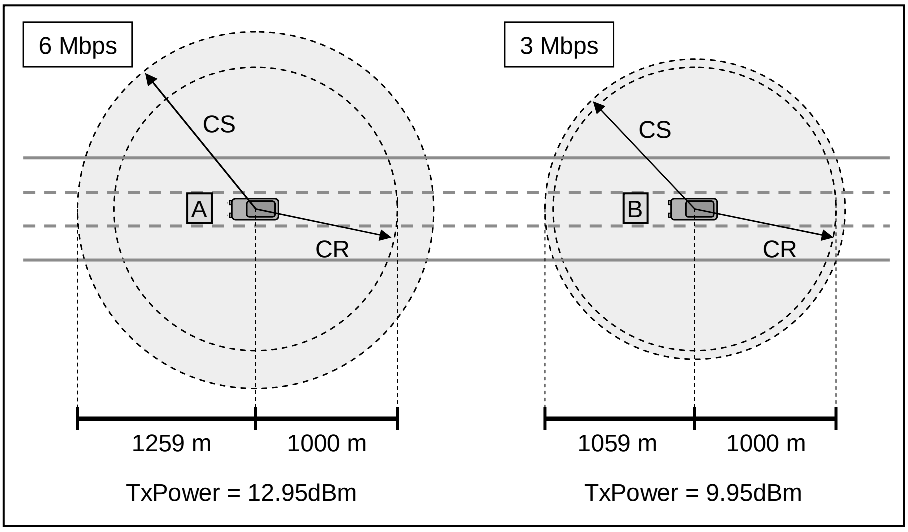


Figure 3.2: Communication and carrier sense ranges obtained for a signal transmitted power of 12.95 dBm with a data rate of 6 Mbps, and 9.95 dBm with a data rate of 3 Mbps.

Figure 3.2 illustrates the CR and CS values corresponding to the thresholds specified in Table 3.1 according to a transmission power of 12.95 dBm with a data rate of 6 Mbps and of 9.95 dBm with a data rate of 3 Mbps. Note that for higher data rates, the required SNR (Signal to Noise Ratio) is higher and, therefore, the transmission power must be also higher in order to achieve the same CR.

However, communication and carrier sense ranges are not accurate when using probabilistic propagation models since the received power is not a fixed value, i.e., it follows a random distribution over time, at each distance. Therefore, there exist no fixed CR and CS ranges when using a probabilistic radio model.

In the rest of the thesis, we use the term *intended communication range*, or simply *communication range (CR)*, to refer to the CR value that would be experienced with the deterministic propagation two ray ground model. Additionally, for clarity, intended CR, or solely CR, is also used equivalently to express the transmission power that provides this CR value with the two ray ground model.

The Nakagami-m fading model

The Nakagami-m model derives the received signal strength from a multi-path environment where the different signal components arrive randomly because of the different propagation phenomena. It is used to estimate the signal amplitude at a given distance from the transmitter as a function of two parameters, Ω and m. The following expression describes the Nakagami probability density function (*pdf*) of the received signal amplitude x:

$$f_{amp}(x; m, \Omega) = \frac{2m^m}{\Gamma(m)\Omega^m} x^{2m-1} \exp(-\frac{m}{\Omega} x^2), \qquad m \geqslant \frac{1}{2} \tag{3.5}$$

where Ω defines the average received power at a specific distance; the value m identifies the fading intensity and depends on the environment and the distance to the sender; and Γ is the *Gamma function*.

The Nakagami-m model can be also used to approximate other multi-path distributions. Indeed, it offers via the m parameter a wide range of fading severities or *amount of fading*[3] [SMSA00]. For $m = 1$ it represents the Rayleigh distribution, which considers non-line of sight communications. For scenarios with a lower level of fluctuations ($m > 1$), Nakagami-m can be used to approximate a Rice distribution. When m is set to a positive multiple of 0.5 the Nakagami can be described by an Erlang distribution, which is how it is implemented in the simulator.

In next chapters, we set Ω to match the two ray ground model for a proper comparison, and we take different values of m to model different levels of fading intensity, resulting from a different weight of the line of sight component.

Figure 3.3(a) illustrates the *pdf* of the Nakagami distribution of the received power for different values of m at a distance of 100 m when assuming a transmission power of 9.95 dBm, i.e., with a resulting Ω of -69.9 dBm (see Figure 3.1) or the corresponding 0.102 nW. We present in Figure 3.3(b) the corresponding received power values in a dBm scale. Note the higher probability of obtaining lower reception power values with $m \leqslant 1$, also called 'heavy tail' case. Also, it is worth noting the lower variance experienced by smaller intensities of fading,

[3] The fading figure, or *amount of fading*, was proposed by Charash [Cha74] as a unified measure for the fading severity.

i.e., higher values of m, which result in a higher probability to obtain a received power around the mean value Ω.

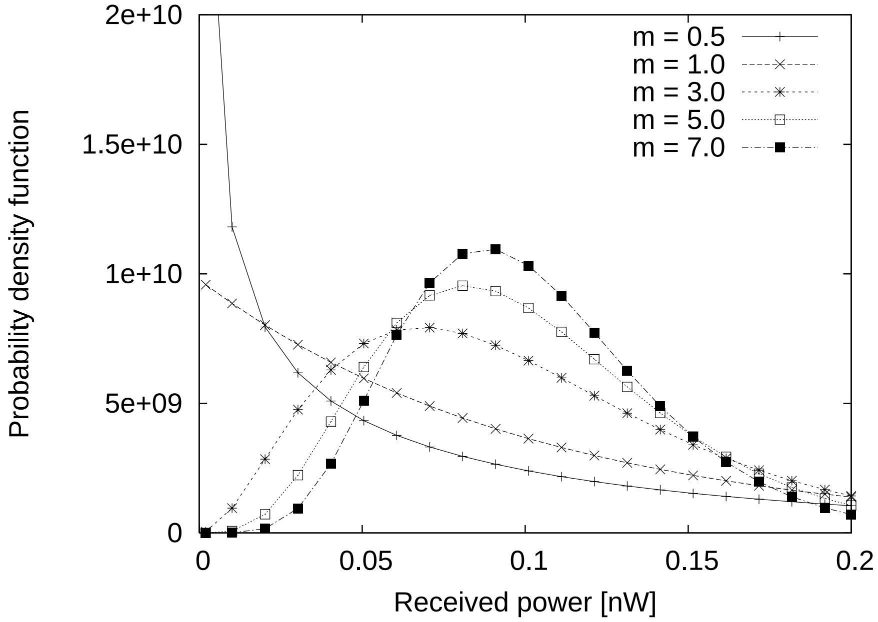
As mentioned above, a random behavior of the channel model does not provide deterministic values for the carrier sense range. This characteristic challenges the coordination of CSMA approaches as we can observe in the simulation results presented in Section 3.4.

3.2.3 IEEE 802.11p model

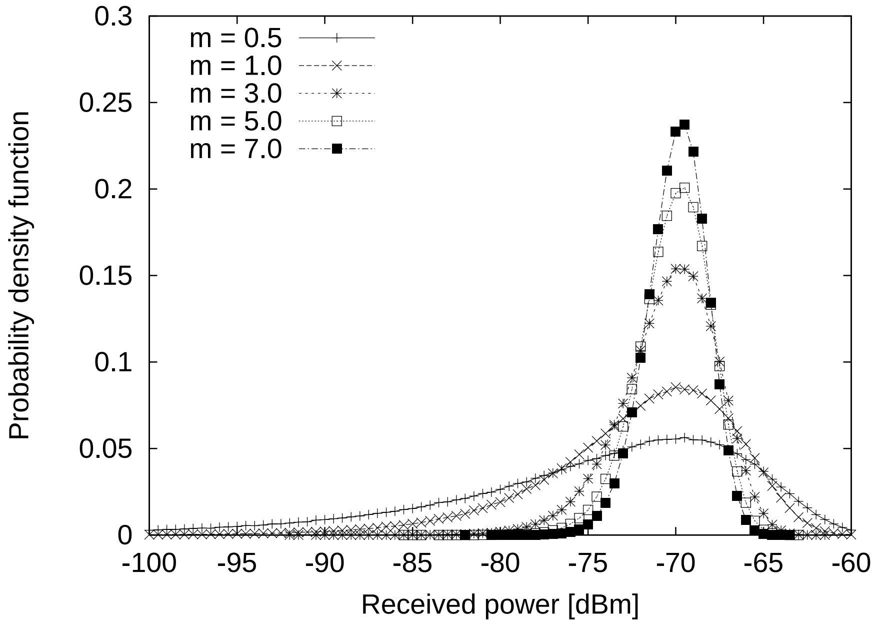
As described in Chapter 2, the IEEE 802.11p draft of the future standard introduces modifications mainly in the physical and management domain. Features like channel scanning or authentication and association procedures will not be used due to the safety nature of WAVE communications. On the other hand, elaborated channel management capabilites are envisioned due to its multi-channel approach. On the physical layer, the carriers use the 5.9 GHz band and channels are set to 10 MHz in order to reduce inter-symbol interference. With respect to the basic channel access mechanisms of 802.11, i.e., the distributed coordination function (DCF) based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), no changes are expected.

Since ns-2.28 does not implement management functions and our study focuses on safety-related information exchange performed in one single channel, no modifications have been implemented in the management entities. Likewise, no extensions have been introduced on the channel access mechanisms apart from the bug fixes described in [SELMTMH06] and the different channel access categories from EDCA (Enhanced Distributed Channel Access [11e]) to provide traffic prioritization.

With respect to the physical layer, ns-2.28 models a Lucent WaveLAN 802.11 DSSS (Direct Sequence Spread Spectrum) radio interface. In order to model a WAVE OFDM system, which operates at 5.9 GHz with 10 MHz channels, several modifications were required according to the IEEE 802.11a [11a] standard and the IEEE 802.11p [11p] draft. Independently from the data rate used to transmit a message payload, the preamble and the PLCP header are always transmitted using the lowest data rate, 3 Mbps. The modulation scheme that provides 3 Mbps is the most robust one, Binary Phase Shift Keying (BPSK) with the lowest coding rate (1/2). However, note that 16 service bits of the PLCP header are transmitted with the payload data rate, instead of the basic rate, and that padding and tail bits are added in order to fill up the last symbol of a message. Additionally, the slot time parameter is adapted to support larger communication distances. Again, we refer the reader to [SETMT$^+$06] for a detailed report on the implementation issues. Table 3.3 presents the main parameters configured in our version of the simulator for two modulations, corresponding to data rates of 6 Mbps and 3 Mbps. Further details and a brief description of IEEE 802.11p MAC and PHY parameters can be found in Appendix A.



(a) nW scale, Ω = 0.102 nW.



(b) dB scale, Ω = -69.9 dBm.

Figure 3.3: Probability density function of the Nakagami-m fading model for different fading intensity values.

Parameter	Value
Frequency	5.9 GHz
Data rate	6 Mbps / 3 Mbps
RxTh	-92 dBm / -95 dBm
CpTh	7 dB / 4 dB
CSTh	-96 dBm
Noise	-99 dBm
Antenna gain	2.512 dB
Antenna height	1.5 m
Slot time	16 μs
SIFS time	32 μs
Preamble length	32 μs
PLCP header length	8 μs

Table 3.3: Ns-2.28 MAC and PHY configuration values for simulations of inter-vehicle communications.

3.2.4 Vehicular movement patterns

The choice of an appropriate scenario is an important factor for a correct design and/or analysis of wireless communication systems and protocols. The potential high speeds and the street-bounded mobility presented by the nodes in vehicular environments must be taken into consideration in order to develop tailored solutions. During the realization of this thesis, we contributed on the development of the HWGui tool [FTMK+06], which is publicly available under [HWG]. The HWGui project was developed during the FleetNet [Fle] and NoW [NoW] projects and transforms highway movement data, provided by DaimlerChrysler, into ns-2.28 `tcl` movement traces. The original data from DaimlerChrysler was generated by means of microscopic traffic simulation and validated against real-world data collected on German highways. Additionally, the HWGui provides the statistical analysis of the scenarios from a communication perspective as well as a graphical visualization. Figure 3.4 presents a snapshot of the visualization and analysis tool *HWGui*.

The ns-2.28 movement traces correspond to vehicles driving during 60 seconds in a straight bidirectional highway with different settings of number of lanes, 2 or 3 per direction, and node density, from 2 to 15 vehicles per kilometer in each lane. Several scenarios of each configuration are provided. The average speed of the nodes driving on the highway segment depends on the vehicle density, varying from 140.8 km/h to 111.2 km/h. The lane width is configured to be 2.5m and the median strip to 2m, according to realistic values for German highways.

Note that all possible configurations correspond to free-flow traffic conditions, the highest node density per lane (15 vehicles per kilometer per lane) presents an average distance between vehicles of 66.6m and an average speed of 111.2km/h.

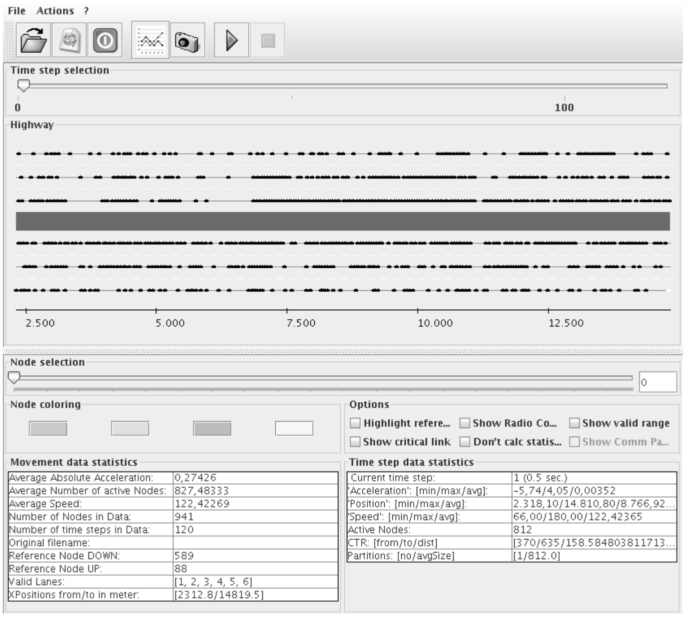


Figure 3.4: Screen-shot of the HWGui tool [FTMK+06] with a scenario composed of 3 lanes per direction and 6 nodes per kilometer in each lane.

We have selected the configuration of 3 lanes per direction and 11 vehicles per kilometer and lane as our nominal case. From our point of view, this is one of the most critical situations from a safety point of view, i.e., fast moving 'heavy' traffic. However, during the analysis we also offer the performance results of a scenario with lower vehicular density, namely 3 lanes per direction and 6 vehicles per kilometer and lane.

Although the original highway scenarios offered with the HWGui tool are 15 km long, we chop them into 6 km long segments to gain computational efficiency.

3.3 Evaluation metrics

Another important task in simulation studies is the proper evaluation and interpretation of the obtained data. In the following, we introduce the main metrics utilized to evaluate the performance of inter-vehicle communications. Note that, due to the safety nature of the information contained in IVC messages, we compute some of the metrics with respect to the distance from the originator.

- *Probability of successful message reception:* The probability that a transmitted message can be successfully decoded by the receiving node at a specific distance from the transmitter. This metric represents the reception ratio of one-hop messages without retransmission schemes, i.e., when messages are not retransmitted to improve reliability.

– *Probability of information reception:* The probability that the information generated by a specific node is received by another node located at a specific distance from the information originator. Contrary to the previous metric, this one accounts for multi-hop forwarding and retransmission techniques.

– *Channel Access Time (CAT):* The span between the time an application generates a packet and the time this packet is eventually transmitted to the channel. This metric includes the time a packet has to wait in the interface queue as well as the delay introduced by the MAC protocol with the DCF access strategy.

– *Information reception delay:* The span between the time a safety application generates a message and the time this message is received by the corresponding application at another vehicle located at a specific distance from the originator.

– *Channel Busy Time (CBT):* The time ratio that a specific node determines the channel as busy, i.e., the time ratio that the accumulated power of packets and interferences is higher than $CSTh$ at the node's location.

Note that in this chapter, only the probability of successful message reception and the channel access time are used to study the performance of the IEEE 802.11p-based one-hop communications. The other three metrics are used in Chapter 6 to evaluate the communication protocols proposed in Chapter 5.

3.4 Analysis of periodic one-hop broadcast reception rates

In this section, we analyze via simulation the performance of periodic one-hop broadcast communications in a vehicular scenario. We configure each vehicle to send beacons in a shared wireless channel according to the different parameters specified in Chapter 2.3 and compare the results obtained. The selected packet generation rates are 10 pckts/s and 20 pckts/s. The communication ranges utilized are 250 m, 500 m, 750 m and 1000 m and the contention window (CWmin) values are 15, 31 and 63, corresponding to the three lower values specified in [11]. We also consider two different data rates, 3 Mbps and 6 Mbps, and fix the packet size of all packets to 500 Bytes as a middle value among the ones presented in [RH05]. The density and movement patterns are configured utilizing the highway scenarios described in Section 3.2.4. The chosen environments consist of a fast-moving 'heavy' traffic bidirectional highway with 3 lanes per direction and 11 cars per kilometer and lane, and a smoother traffic situation with 3 lanes per direction and 6 cars per kilometer and lane. Note that both scenarios correspond to free flow vehicular traffic, the vehicular density can be much higher in many real highways during several hours per day. However, we are interested in high speed scenarios with high dynamism where the utilization of high transmission power and packet generation rates is envisioned. Finally, the propagation models used are the deterministic two ray ground, and the probabilistic Nakagami with different fading intensities, namely m = 1, 3, 5 and 7. The configuration values are summarized in Table 3.4.

Each studied configuration is simulated with 10 different highway scenarios (with the same vehicular density) and 10 different random seeds. The results obtained are averaged over 10 s of simulated time and presented with a 95% confidence interval. Also, in order to avoid border effects, the presented reception probabilities correspond to the messages sent by a reference node, located two kilometers away from the edge of the scenario.

Parameter	**Value**
Data Rate	3 Mbps, 6 Mbps
Packet generation rate	10 pckts/s, 20 pckts/s
Packet size	500 Bytes
Intended communication range	250 m to 1000 m
Vehicle density	36 cars/km, 66 cars/km
Radio propagation models	Nakagami, two ray ground
Fading intensity m	1, 3, 5, 7
Contention Window	15, 31, 63

Table 3.4: Configuration values of the simulated one-hop broadcast communications in highway scenarios.

3.4.1 Radio propagation models

For a better comprehensibility of the broadcast reception rates in scenarios where all nodes send periodic messages, we present first in Figure 3.5 the probability of successful reception in the absence of interferences from other nodes, i.e., collision-free. The transmission power is set to 1.83 dBm, which provides a communication range of 500 m (CS = 664 m) with two ray ground when utilizing a data rate of 6 Mbps. In the same figure we present the values obtained with Nakagami m = 1, 3, 5 and 7. The difference between deterministic and probabilistic models can be clearly observed: the deterministic two ray ground model experiences a probability of reception equal to 1 within its communication range and drops to zero exactly at its edge. On the other hand, the probabilistic models show a smoother decrease over the distance, with different decrease slopes depending on the chosen fading intensity.

Note how a reliable communication range significantly differs from the intended CR when taking into consideration fading phenomena. For example, with a fading intensity m = 7 reception failures can be experienced at 300 m from the

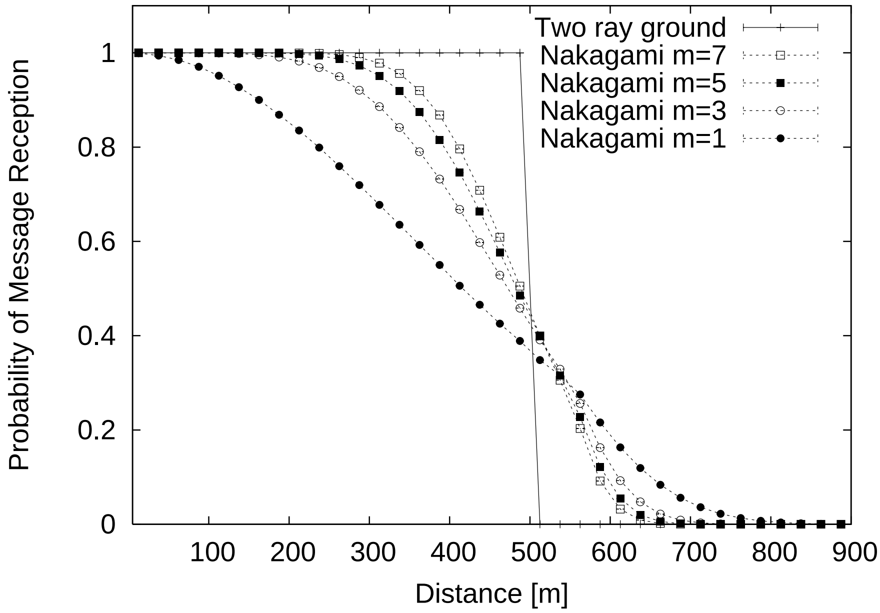


Figure 3.5: Probability of successful packet reception without interferences from other nodes with respect to the distance with a transmission power corresponding to a CR of 500m with a data rate of 6 Mbps and different radio propagation models.

transmitter. This situation is more critical with higher fading intensities, e.g., with m = 1 only within the first 30 m we can consider a transmission as reliable. All curves present reception rates at the edge of the intended communication range around 40%.

Consequently from a transmitter perspective, a higher transmission power than the one corresponding to the intended CR should be used in the presence of a probabilistic radio channel. However, note that increasing the transmission power also increases the level of interference and the amount of nodes sharing the channel. As we show later in this chapter, a high transmission power used by all nodes in the network can be harmful from a system perspective due to an increased amount of collisions.

Another key observation with respect to probabilistic channel models is that there are chances of successful reception outside of the CR. The probabilistic behavior of the channel challenges the nodes coordination provided by the DCF mechanism: transmissions from neighboring nodes may suffer a high attenuation while further nodes' messages may suffer low attenuation. Furthermore, the resulting variance is accentuated with higher fading intensities, which may cause lower reception probabilities within the intended communication range but higher reception probability for larger distances.

In the following, we study a highway scenario where all vehicles are equipped with 5.9 GHz DSRC technology and send periodic messages to the channel.

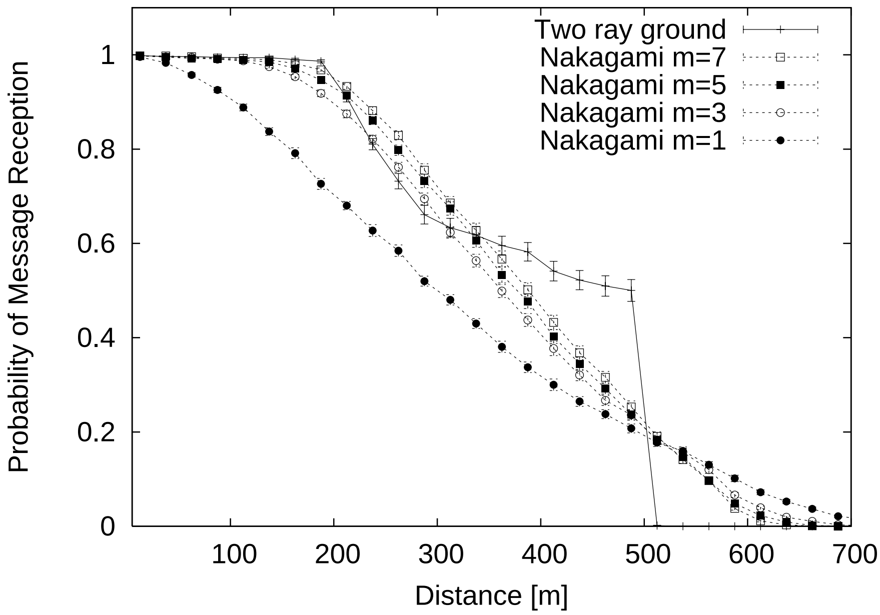


Figure 3.6: Probability of successful beacon reception with respect to the distance in a 3-lane per direction highway scenario with 36 vehicles/km. Comparison of the results obtained by using different propagation models with a data rate of 6 Mbps, an intended communication range of 500 m and a packet generation rate of 10 pckts/s.

Figure 3.6 presents the successful reception rates from the lower vehicular density scenario where all cars are configured to send 10 packets per second with an intended communication range of 500 m. The contention window in this setup has been configured to 31, which allows all generated messages to be transmitted to the channel (see the next section for further details). The average amount of load offered to the channel within a node's CS, referred to as *beaconing load* (BL), can be computed as follows:

$$BL = VD(cars/km) * 2CS(km) * PGR(pckts/s) * PS(bits/pckt) = 1.9\,Mbps$$

where VD = 36 cars/km is the average vehicular density (taking into account the 6 lanes); CS = 0.664 km is the carrier sense range corresponding to a CR = 500 m; PGR = 10 pckts/s defines the packet (beacon) generation rate of each node; and PS = 4 kbits/pckt represents the size of beacons[4]. Therefore, we obtain a resulting beaconing load of 1.9 Mbps in a 6 Mbps medium.

Contrary to the scenario illustrated in Figure 3.5, nodes must contend with their neighbors before transmitting a message and packet collisions are experienced. There are two reasons that can cause a collision at a receiver: *i)* two or

[4]For the sake of simplicity, we account the packet size of a packet to include the amount of bits corresponding to the MAC header, the preamble length, the PLCP header, the tail bits and the padding bits [11a].

more nodes select the same slot to transmit after a channel busy period, and *ii)* one or more nodes could not sense an ongoing transmission and access the channel at that time. The second case is commonly known as the hidden node (or hidden terminal) problem and is illustrated in Figure 3.7. See how, in comparison to a collision-free scenario (Figure 3.5), the reception rates shown in Figure 3.6 present lower values at the edge of the CR, at 500 m. There is a 50% drop in case of two ray ground and around 22% drop in case of Nakagami, due to the collisions corresponding to hidden nodes.

It is also worth noting in Figure 3.6 how the probability of successful reception of all curves, except for Nakagami m = 1, is close to 100% up to a distance of 200 m approximately. These high reception rates are achieved due to two reasons. First, since the wireless channel does not experience a high saturation in this scenario, there is a low probability that two nodes within the CS range of each other select the same slot to transmit creating a collision. Second, radio interfaces can successfully receive a message if the signal level is CpTh above the interference level due to the capture feature. Therefore, we call this distance 'robust distance against hidden nodes', which represents the range where the power of the transmitted signal is (in average) CpTh higher than the interference caused by hidden nodes located outside of the CS range of the sender. See Appendix B for a detailed description of how the robust range against hidden nodes is computed.

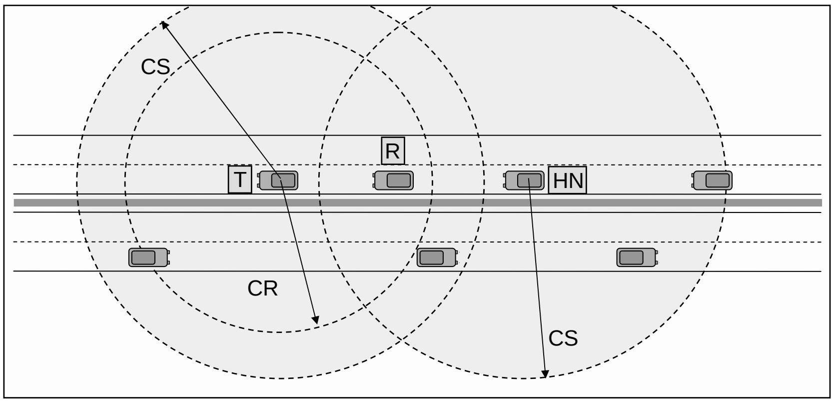


Figure 3.7: The hidden node (or terminal) problem: In a CSMA/CA scenario assuming a deterministic propagation model, node R is inside the Communication Range of T and node HN is placed outside of the Carrier Sense range (CS) of T, i.e., HN can not sense ongoing transmissions from T. In that case, the hidden node problem occurs when T's message is interfered by an HN's transmission at R's position.

With a data rate of 6 Mbps and an intended communication range of 500 m, we obtain a robust range against hidden nodes of 192.4 m. At this distance the curves in Figure 3.6 present a 'knee' where they start decreasing with a high slope, which corresponds to the amount of hidden nodes that can collide with these transmissions at each distance. The amount of such nodes is increasing due to the fact that, with higher distances, the reception power experienced at the potential receiver R is decreasing while potential hidden nodes are closer to this node R. The resulting curves of Nakagami present a 'smoother' shape (i.e., without sharp knees[5]) than the two ray ground one due to the probabilistic nature of the radio propagation phenomena. Indeed, hidden nodes can also be located within the intended CS range with Nakagami, which causes uncoordinated transmissions even among nodes located within the CS range of each other. The curve presenting lower reception rates within the communication range is Nakagami with m = 1, due to its heavy tail as seen in Figures 3.3(a) and 3.3(b). Fading intensities corresponding to m = 3, 5 and 7 present similar results according to the similar probability density functions, see Figure 3.3(a). We refer the reader to Appendix B for a description of the impact of hidden nodes and, in particular, the case of utilizing the two ray ground propagation model.

We now present the results obtained in a highway scenario with a higher vehicular density, i.e., 66 cars/km, see Figure 3.8. In this case, the beaconing load increases up to an average of 3.5 Mbps. First, note how all curves present lower reception rates within the robust range against hidden nodes. The higher amount of neighboring nodes increases the probability that two or more nodes select the same slot to access the channel and, therefore, they generate a packet collision also at close distances from the transmitter. Second, the probability of successfully receiving a message is also decreased at all distances compared with Figure 3.6 due to the higher incoordination among nodes accessing the channel experienced for all propagation models. In this scenario, the reception rates at the edge of the intended communication range is below the 10% for all propagation models.

The results obtained show the challenge of achieving high reception rates in vehicular scenarios. The solely existence of probabilistic phenomena causes increasing reception failures with respect to the distance from the transmitter. Furthermore, the reception rates significantly decrease when the wireless medium is shared with other nodes, and is dependent on the amount of nodes and the resulting load on the channel. In the following sections, we study different configuration options.

In the rest of the thesis, we illustrate the results obtained with the Nakagami model and a (medium) fading intensity m = 3. Moreover, we utilize the scenario with 3 lanes per direction and 11 vehicles per kilometer and lane as our nominal case. The results obtained with the lower vehicular density scenario are discussed in Section 3.4.5, and comments with respect to the results obtained with the other radio propagation options are provided when appropriate.

[5] The shape of the two ray ground curve is addressed in more detail in Appendix B.

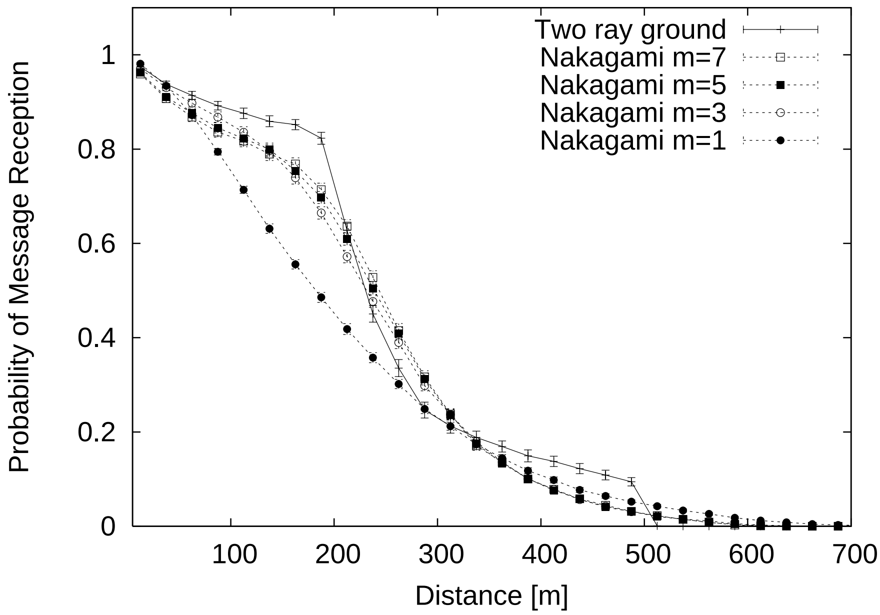


Figure 3.8: Probability of successful beacon reception with respect to the distance in a 3-lane per direction highway scenario with 66 vehicles/km. Comparison of the results obtained by using different propagation models with a data rate of 6 Mbps, an intended communication range of 500 m and a packet generation rate of 10 pckts/s.

3.4.2 Configuration options

In this section, we study the effects that different contention window values, data rates, transmission powers and packet generation rates have on the performance of one-hop broadcast periodic transmissions. As mentioned above, the results presented correspond to the highway scenario with 66 cars/km and assuming the Nakagami propagation model with m = 3.

First, we intend to select the appropriate contention window (CWmin) value to be utilized on the rest of the thesis. The existing trade-off when selecting the contention window value is the following: on the one hand, a higher value decreases the probability that two nodes select the same slot to access the medium; on the other hand, it also increases the delay experienced by a packet until it is transmitted to the channel.

Table 3.5 presents the results obtained when configuring all vehicles in the highway with the maximum intended communication range utilized (1000 m), for three contention window values (15, 31 and 63), two data rates (6 Mbps and 3 Mbps), and two packet generation rates (10 pckts/s and 20 pckts/s). The values presented in Table 3.5 correspond to the average channel access time experienced by nodes whose middle position lays within the four center kilometers of our highway, i.e., the nodes that are within 1 km to one of the borders of our

CW size	63	31	15
6 Mbps, 10 pckts/s	298.3 ms	78.3 ms	19.3 ms
3 Mbps, 10 pckts/s	231.6 ms	39.8 ms	16.1 ms
6 Mbps, 20 pckts/s	293.6 ms	270.0 ms	213.0 ms
3 Mbps, 20 pckts/s	301.4 ms	266.6 ms	208.7 ms

Table 3.5: Average channel access time in a 3-lane per direction highway scenario with 66 vehicles/km. Comparison of the results obtained by using different data rates, packet generation rates and contention window values with a communication range of 1000 m.

highway segment are not taken into account. The middle position of a vehicle represents the middle point between its position at the beginning of the simulation and its position at the end.

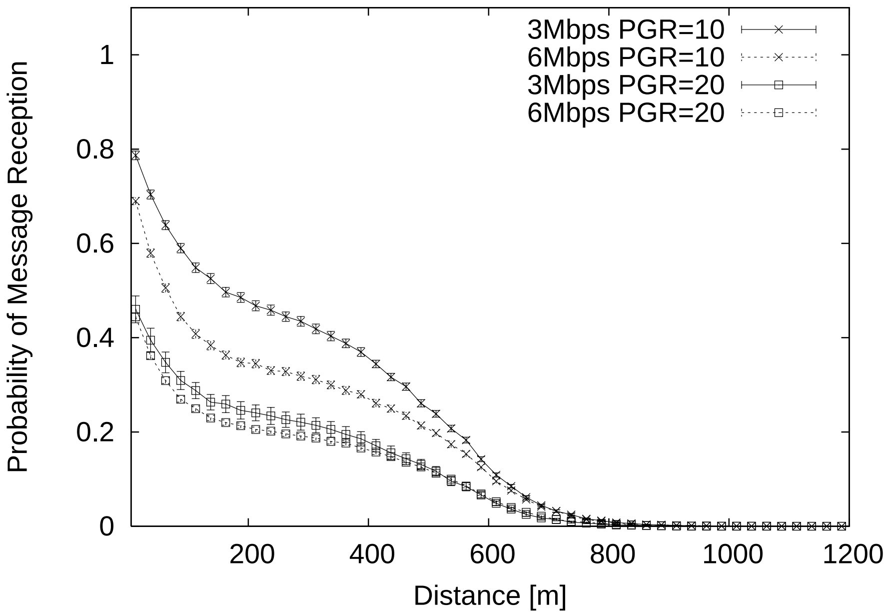
With a packet generation rate of 10 pckts/s and a data rate of 6 Mbps, the contention window value of 63 should not be utilized. Setting CWmin = 63 causes that the resulting average CAT[6] is larger than the beaconing period, i.e., 100 ms. Therefore, not all generated packets are transmitted to the wireless medium. In case of 3 Mbps, a contention window equals to 15 and 31 presents all CAT values below 100 ms.

Note that when configuring PGR = 10 pckts/s, the CAT values experienced in case of using a data rate of 3 Mbps are shorter than in case of 6 Mbps. This result might appear counterintuitive at first due to the shorter time that messages reside on the channel with higher data rate. However, it must be taken into account that the transmission power corresponding to a CR = 1000 m with a data rate of 3 Mbps is lower than in the case of 6 Mbps for the same intended communication range due to the required CpTh. Accordingly, the resulting CS for 3 Mbps is 1059 m, instead of the 1259 m obtained with 6 Mbps, which results in an average of 26 nodes less sharing the wireless medium.

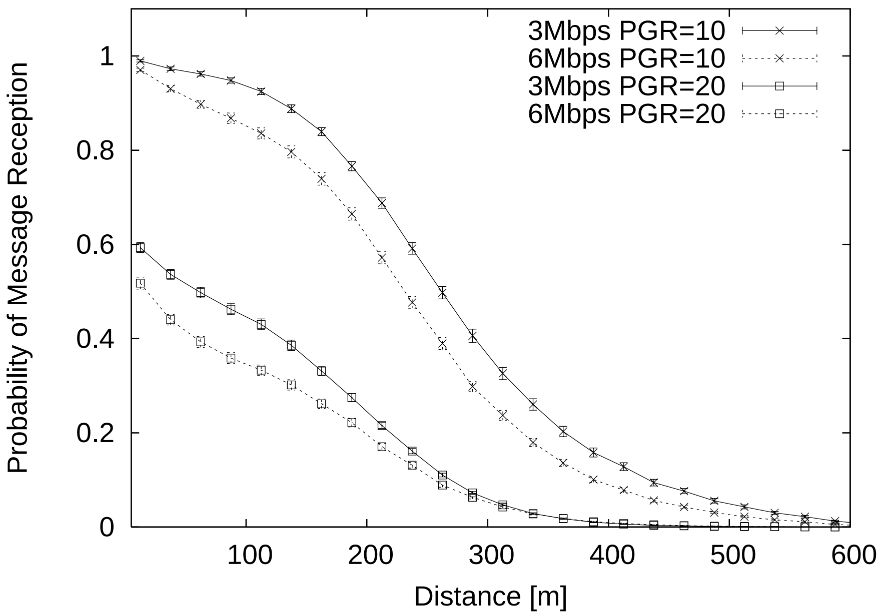
In the case of 20 pckts/s both data rates present significantly larger CAT values than the 50 ms beaconing period for all contention window values. Therefore, we can state that 20 pckts/s can not be supported for the vehicular density configured (66 cars/km) and the selected communication range (1000 m).

Let us now look at the achieved reception rates with respect to the distance from the transmitter for the two selected data rates: IEEE 802.11p's default one, 6 Mbps, and the most robust against interference, 3 Mbps. Figures 3.9(a) and 3.9(b) present the results for two different PGR values (10 pckts/s and 20 pckts/s) and two different CRs (1000 m and 500 m) with the contention window set to 31. The curves presented correspond to the ratio of generated packets

[6] The computed average channel access time (CAT) only takes into consideration messages that are transmitted to the medium, and not the ones remaining in the interface queue or the ones dropped due to queue overflow. Therefore, resulting values above the beaconing interval are just used to identify situations where not all generated messages can be transmitted to the medium.



(a) CR = 1000 m.



(b) CR = 500 m.

Figure 3.9: Probability of successful beacon reception with respect to the distance in a 3-lane per direction highway scenario with 66 vehicles/km. Comparison of the results obtained by using different data rates, communication ranges, and packet generation rates with a contention window of 31.

that are successfully received. Beacons not transmitted to the medium due to the high saturation experienced are considered not successful.

We observe in Figure 3.9(a) how for both PGR values the data rate of 3 Mbps achieves higher successful reception rates than 6 Mbps, e.g., a 37% higher in case of 10 pckts/s at half of the communication range (250 m) and a 16% in case of 20 pckts/s. The same conclusion can be drawn when configuring the communication range to 500 m (Figure 3.9(b)), a data rate of 3 Mbps appears to be a better option for our scenarios.

With respect to the different packet generation rates, as expected, a higher amount of generated packets turns into a higher saturation on the medium and, therefore, a higher rate of reception failures is experienced. More interesting is the effect of different CR values, which is further studied in the next section. For a detailed analysis of the reception success and failure in vehicular, one-hop, broadcast communications we refer the reader to our work [SETMMH07].

In this section, we have shown the importance of selecting an appropriate contention window value and data rate. In the rest of the thesis we make use only of the 3 Mbps data rate and configure the contention window to 31, due to the results outlined in high channel load vehicular scenarios. Moreover, we consider 10 pckts/s as our nominal case, which is a common value used in inter-vehicle communication research, e.g., [RRR05], [EGH$^+$06] and [CJTD06].

3.4.3 Transmission power values

To clearly observe the impact of adjusting the transmission power (TxPower) we set up a scenario with our nominal values designated in the previous sections and compare the resulting reception rates for different intended communication ranges. Figure 3.10 presents the results obtained with a fixed PGR = 10 pckts/s, a data rate of 3 Mbps and a contention window of 31, while increasing the intended communication range from 250 m to 1000 m.

In general, increasing the transmission power of one message increases its robustness against power fluctuations as well as interference and, thus, it is capable of reaching further distances. However, increasing the transmission power of all nodes in a network increases their CS ranges and, therefore, the amount of nodes sharing the channel at all locations. We can observe that, while the channel is not over-saturated, increasing the transmission power does not significantly decrease the reception rates at close distances, and provides improved reception rates at further ones, i.e., curves corresponding to 250 m and 500 m. We consider the channel to be over-saturated when collisions caused by neighboring nodes are not negligible. On the other hand, a CR = 750 m already experiences a significantly higher amount of collisions due to not only hidden nodes but also neighboring nodes. With a highly saturated channel, there exist a large number of messages transmitted from nodes at close distances which can not be captured due to the high power of the interferences. The reception rates at close distances from the sender are further reduced in case of CR = 1000 m. We remark that due to the kinetic energy of moving vehicles reception rates at close distances are more relevant from a safety perspective. Therefore, with a PGR of 10 packets per second a CR of, e.g., 500 m would be a better choice than 1000 m, even though a higher CR provides increased probability of reception at far distances.

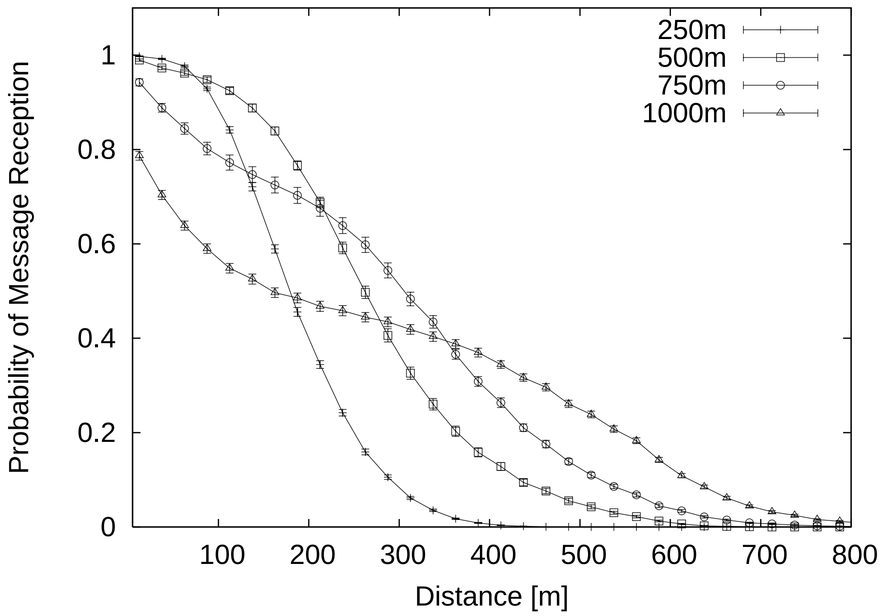


Figure 3.10: Probability of successful beacon reception with respect to the distance in a 3-lane per direction highway scenario with 66 vehicles/km. Comparison of the results obtained by using different communication ranges with a data rate of 3 Mbps, a contention window value of 31 and a packet generation rate of 10 pckts/s.

It is worth noting the resulting shape of the reception rates curve in a high saturation case. For example, even though the offered load to the channel achieves 5.6 Mbps in case of CR = 1000 m, beacons achieve a probability of successful reception above 50% up to 200 m thanks to the capture feature. This effect and the sharp slope present at close distances (up to 150 m) are due to the abrupt decrease of the signal power experienced in this range, i.e., the near-far effect introduced in Section 3.2.2.

From the results obtained, we identify (transmission) power control as a critical issue of inter-vehicle communications. On the one hand, a higher transmission power can be used in order to achieve higher reliability of one specific message. On the other hand, not controlling the system (meaning all nodes in the network) transmission power can result in a lower safety level due to the decreased reception rates experienced at close distances from the transmitters.

3.4.4 Priority channel access

When a node detects an emergency situation, it is expected to transmit a message with high priority. In this section, we evaluate the benefits of the EDCA mechanism [11e] in a vehicular environment. For this purpose, we configure the set up utilized in the previous section with one node in the highway, the reference node, with a higher priority than all the other nodes. Specifically, while 'non-priority' nodes are configured with a CWmin = 31 and a standard distributed interframe space (DIFS) of 64 μs, the high priority node has a CWmin = 7 and an interframe space one slot time shorter, i.e., 48 μs.

Com. Range	Non-priority	Priority
500 m	3.5 ms	1.3 ms
1000 m	39.8 ms	5.3 ms

Table 3.6: Average channel access time experienced in a 3-lane per direction highway scenario with 66 vehicles/km. Comparison of the results obtained by a priority node and a non-priority one with different communication ranges, a data rate of 3 Mbps, and a packet generation rate of 10 pckts/s.

Table 3.6 presents the average channel access time experienced by the reference node for CR values of 500 m and 1000 m, which result in a beaconing load of 2.9 Mbps and 5.6 Mbps respectively. We can observe how, in case of CR = 500 m, the access time with the priority scheme decreases from 3.5 ms to 1.3 ms, a 63% reduction. In case of CR = 1000 m, the time reduction reaches a 87%, from 39.8 ms to 5.3 ms. Therefore, the EDCA mechanism achieves its goal of reducing the CAT of high priority messages and its benefit depends on the data load experienced on the channel. Note that this benefit can be more relevant when disseminating information to distances larger than the direct communication range, as evaluated in Chapter 6, since the time reduction is additive with each forwarding node in each traveled hop.

Figure 3.11 presents the probability of reception with respect to the distance achieved by the reference node in the cases described above. The resulting curves show that when the beaconing load is high, EDCA can provide not only a shorter CAT but also an increased probability of reception for priority messages. For example, for a CR = 1000 m the probability of reception increases from a 43% to a 71% at 300 m from the transmitter.

In order to explain this effect we have to refer to the 802.11 DCF (Distributed Coordination Function) [11]. Under certain conditions, the high priority node is able to access the channel earlier than all others, therefore sending without any chance to collide with any other node that can sense its signal on the channel. Assuming a deterministic propagation model to simplify the explanation, there are two situations from which the high priority node can benefit:

– During a busy period a priority node generates a packet and selects a backoff timer equal to 0. In this case no other node inside its carrier sense range is able to collide with it, since they have to wait, at least, one slot more to start decrementing their backoff timer.

– A backoff timer different than 0 is picked during a busy period and later the decrementing process is paused when only one slot is left to decrement. In this case, the high priority node will only be able to collide with nodes inside its CS range that generate a packet during this last busy period and, additionally, select 0 for their backoff timer.

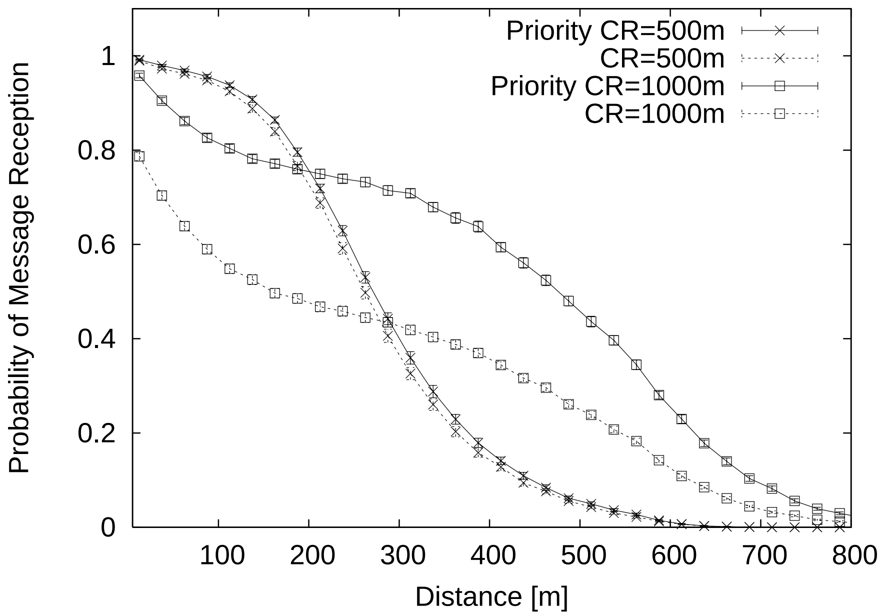


Figure 3.11: Probability of successful beacon reception with respect to the distance in a 3-lane per direction highway scenario with 66 vehicles/km. Comparison of the results obtained by a priority and non-priority node with different communication ranges, a data rate of 3 Mbps, a contention window of 31, and a packet generation rate of 10 pckts/s.

In case of assuming wave propagation according to the two ray ground model, all nodes within the CS range of a transmitter are able to sense its transmission due to the deterministic characteristics of the radio channel. This behavior favors, therefore, the node with high priority. The results obtained with the two ray ground model with the larger CR value, which are not shown here, present a higher reception probability for the priority node. At 300 m from the sender, for example, the probability of successful reception reaches a 74% for prioritized messages, instead of the 71% obtained with the Nakagami model (m = 3).

3.4.5 Lower vehicular density

In order to evaluate the performance of the channel access protocol under a lower vehicular density environment we re-run the setup discussed in Section 3.4.3 with another highway scenario. In this case, the vehicular density is 36 cars/km, corresponding to 3 lanes per direction with 6 cars per kilometer and lane.

Figure 3.12 presents the probability of successful reception with respect to the distance to the transmitter for different CR values, from 250 m to 1000 m. In this scenario, increasing the transmission power of all nodes does not significantly decrease the reception rates at close distances of the transmitter, contrary to what is observed in Figure 3.10. The probability that two nodes select the same slot to transmit after a busy period is not significant for this vehicular density due to the lower load resulting on the channel.

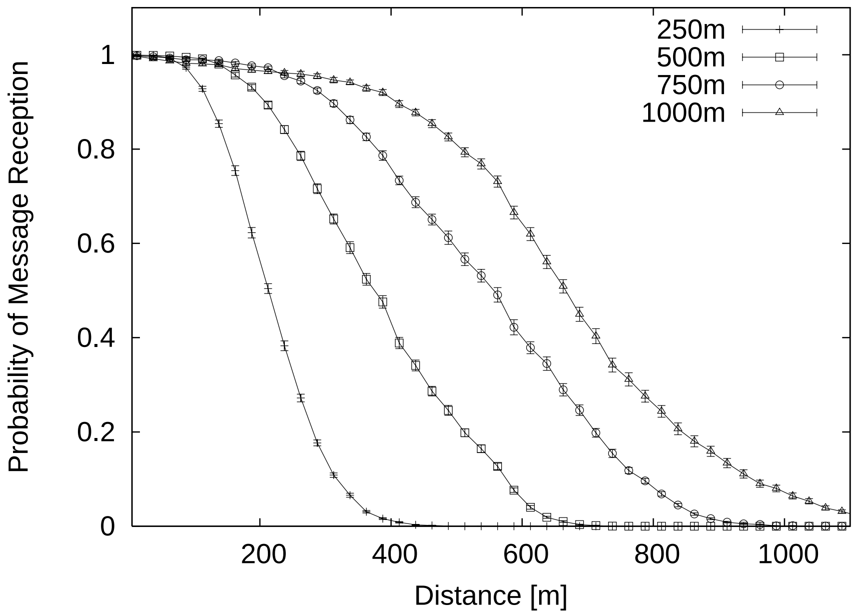


Figure 3.12: Probability of successful beacon reception with respect to the distance in a 3-lane per direction highway scenario with 36 vehicles/km. Comparison of the results obtained by using different communication ranges with a data rate of 3 Mbps, a contention window value of 31, and a packet generation rate of 10 pckts/s.

Therefore, for low vehicular density scenarios power control does not appear to be as relevant for controlling channel congestion. Although beaconing load values can be also high, i.e., 3 Mbps in case of CR = 1000 m in our scenario, increasing the transmission power of all nodes does not present the before mentioned drawback and, at the same time, can be beneficial in case of sparse networks.

In terms of priority access, the benefit of being capable of accessing the channel earlier does not present a high impact on the resulting probability of reception either. For example, in case of CR = 1000 m the reception rates increase from a 95% to a 96% at 300 m distance from the transmitter. Note though, that the average CAT is still significantly reduced for the priority node, e.g., from 2.51 ms to 1 ms in the case of CR = 1000 m.

4 Identification of Challenges and Criteria for Safety-Related IVC

In Chapter 2, we defined two types of communications, or messages, to support vehicular active safety. These communications differ with respect to their motivation and consist *i)* of 'status information' exchange via beacon messages and *ii)* of emergency information dissemination via event-driven ones. In Chapter 3, we analyzed the performance of IEEE 802.11p-based one-hop broadcast communications under different vehicular networking conditions.

In this chapter, our goal is to identify and analyze the challenges faced by both of the safety-related communications to achieve their goals. We first identify the challenges based on the insight gained from the performance analysis presented in Chapter 3 as well as from the literature and from empirical data. Then, we classify these challenges according to the two types of safety-related messages. Finally, we derive the design criteria for the required strategies to support both beaconing and event-driven messages overcoming the challenges presented.

The results of this chapter are utilized to design, in Chapter 5, two communication protocols capable of overcoming the identified challenges for enabling IVC-based active safety applications. Furthermore, key aspects identified here are used in Chapter 7 to derive design guidelines for a communication system architecture tailored to vehicular environments and to propose a model to be used as a basis for implementation.

4.1 Challenges of inter-vehicle communications

Inter-vehicle communications have to be able to cope with adverse conditions such as received radio signal strength fluctuations, channel load saturation, and high mobility to provide robust communication services as a basis for safety-related applications. In the following, and as we did in [TMKH05], we identify and outline the main challenges of robust inter-vehicle communications with respect to their specific characteristics and motivation.

4.1.1 Lack of connectivity and channel congestion

Vehicular networks will suffer from poor connectivity during the early deployment phase. When only a small number of vehicles are equipped with 5.9 GHz DSRC technology, resulting from a low market penetration, communication among nodes will be clearly a challenge. Indeed, according to recent projects [Fle], a penetration rate of at least 10% is required to enable a typical active safety application by inter-vehicle communications. A 10% of penetration could take around one and a half years from the time when the technology is ready to be installed, if all new vehicles would be sold with an incorporated 5.9 GHz DSRC system; three years if only trucks and vehicles of middle and upper classes are to be equipped; or up to six years if only vehicles with a navigation system would be equipped, see [MML04]. In this market introduction phase, not all safety applications can be deployed and they will benefit from strategies such as 'store and forward' [LA05] which uses the node movement to transport the information until a new neighbor (an equipped vehicle or a road side unit) appears.

On the other hand, when the penetration rate is high and many vehicles are equipped with 5.9 GHz DSRC systems, vehicular networks will present several scenarios where a high number of nodes are concentrated in a small area. In these cases the number of packet collisions might be too high to support safety systems when using the CSMA/CA link-layer broadcast scheme of 802.11 without any additional control mechanism (see Chapter 3).

Additionally, in the draft of the 802.11p technology [11p] it is considered that transceivers could switch between different radio channels. In that case, the safety information exchange could be restricted to only a portion of the total usable time for systems with one transceiver. Xu *et al.* address this situation in [XMKS04], where they define feasibility regions that depend on the required probability of successful packet reception. These regions outline which requirements are feasible to be met depending on the time ratio that safety messages can make use of the control channel and the number of nodes located in a specific area.

4.1.2 Radio channel characteristics

As described in Chapter 3.2.2, the attenuation of a transmitted signal in a real scenario is not only caused by free-space loss. Phenomena such as path loss or fading can lead to unpredictable losses in the power of the received signal. Indeed, vehicular environments present unfavorable characteristics to develop wireless communications: multiple reflecting objects could degrade the strength and quality of the receiving signal and, therefore, have a negative impact on messages reception rates. Additionally, fading effects have to be taken into account due to the mobility of the surrounding objects and/or the sender and receiver themselves. Because of fast fading phenomena a transmitter can experience a different multipath environment each time it sends a packet and, therefore, each message can experience a different degree of attenuation.

We present in Table 4.1 the results obtained from empirical data from tests performed within the Network on Wheels (NoW) project [NoW]. We utilized two cars equipped with 5.9 GHz DSRC prototypes provided by DENSO Corporation operating at 5.9 GHz and 10 MHz channels. Each car sent ten broadcast packets per second with a transmission power of 20 dBm while driving at different distances from each other on a German Highway with medium traffic conditions. We recorded the RSSI (Received Signal Strength Indicator) of all received packets and the position of the cars at transmission/reception times for post processing. Each run took a minimum of seven minutes and was repeated five times. In Table 4.1, we can see how the ratio of received packets decreases with the distance between the vehicles, as outlined by the models presented in Chapter 3, due to the radio propagation characteristics. Note that the amount of obtained data does not present enough statistical significance in order to characterize the channel[1], but enough to observe the non-deterministic behavior.

Distance	Avg. Reception Rate	Avg. RSSI values	Standard Deviation
50 m	97.5%	-73.8	4.3
100 m	97.5%	-80.3	5.0
200 m	93.4%	-83.6	4.6
300 m	84.3%	-89.0	3.1
400 m	67.2%	-89.6	2.1
500 m	61.5%	-91.9	1.9

Table 4.1: Reception rates and RSSI values obtained from empirical data on a German Highway. The RSSI values only reflect those of the received messages.

4.1.3 Hidden terminal problem and lack of coordination

Due to the safety nature of inter-vehicle communications, it is envisioned that broadcast will be the most common addressing strategy to transmit messages to the wireless medium. The broadcast channel access mechanism though is espe-

[1] The high cost of each test in a real environment prevented us from obtaining the critical amount of required data to properly derive a channel model.

cially sensitive to hidden terminals since no strategy like RTS/CTS is used to reserve the channel before a data frame transmission.

Additionally, assuming a non-deterministic behavior of the radio channel as described in the previous section, the hidden terminal appears in a new flavor. Due to the variable attenuation suffered by transmitted messages in different directions, hidden terminals may be located closer to the original transmitter than expected. We illustrate in Figure 4.1 the nodes that do not sense a transmission from the node located in the middle of the highway scenario configured with our nominal case. All these nodes could potentially transmit an overlapping message resulting in message reception failures from nodes located between both transmitters. We remark that the closest distance between the sender and nodes that are not able to sense the message is only 735.9 m when using a transmission power of 9.95 dBm (corresponding to an intended carrier sense range of 1059 m).

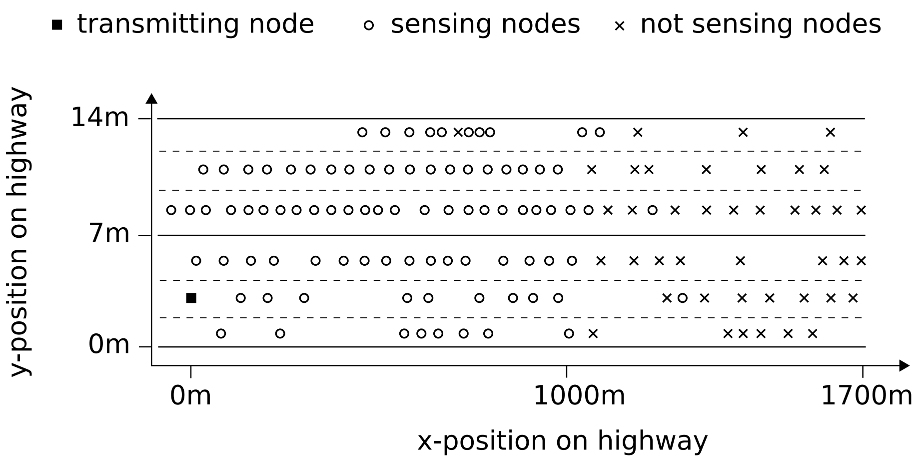


Figure 4.1: The node represented with a black square, transmits one message to the channel with an intended CR range of 1000 m, what corresponds to a CS of 1059 m. Using the non-deterministic Nakagami radio propagation model, with an m parameter set to 3, white circles represent nodes that sense the message on the medium and 'x's represent those which do not.

As presented in Chapter 3, hidden nodes challenge the CSMA/CA mechanism used by IEEE 802.11p with respect to the coordination among transmitting nodes in the network. Under such conditions, the amount of packet collisions are likely to quickly increase with the number of nodes and load to the channel. As can be seen in Figure 3.8, the amount of successfully received packets could decrease below a 20% at the edge of the intended communication range (500 m) when a high amount of neighbors and a high load on the channel is experienced.

4.1.4 High mobility and lack of centralized management entity

One of the characteristics that differentiates vehicular networks from many other mobile networks is the high node speed. The relative speed between two nodes is even higher in case they drive in opposite directions. For example, two vehicles driving in opposite directions in a highway at 120 km/h and experiencing a reliable communication range of 500 m could have a 7.5 s communication window. Therefore, the high mobility of driving vehicles might compromise existing iterative optimization algorithms aiming to make a more efficient use of the channel bandwidth (e.g., [XYLW05]) or the use of predefined routes to forward information (e.g., [FWK+03]).

Figure 4.2 shows the performance of the AODV (Ad hoc On-Demand Distance Vector) [PR99] topology-based routing protocol for a connected network in a highway scenario. It presents the probability that a ping packet successfully travels (two ways) a distance of up to 4500 m when configuring the communication ranges to 500 m. Observe the impact of mobility (the two ray ground curve) on broken routes in a totally connected network. In this case, the delivery ratio falls to a 84% for few hops. The protocol is further challenged when the channel follows the Nakagami model (configured with $m = 3$). The success rates fall down to 27% when the destination node is at 1500 m or to a 6% when the destination node is at 3000 m. See our previous work [TMSEFH06] for a complete description.

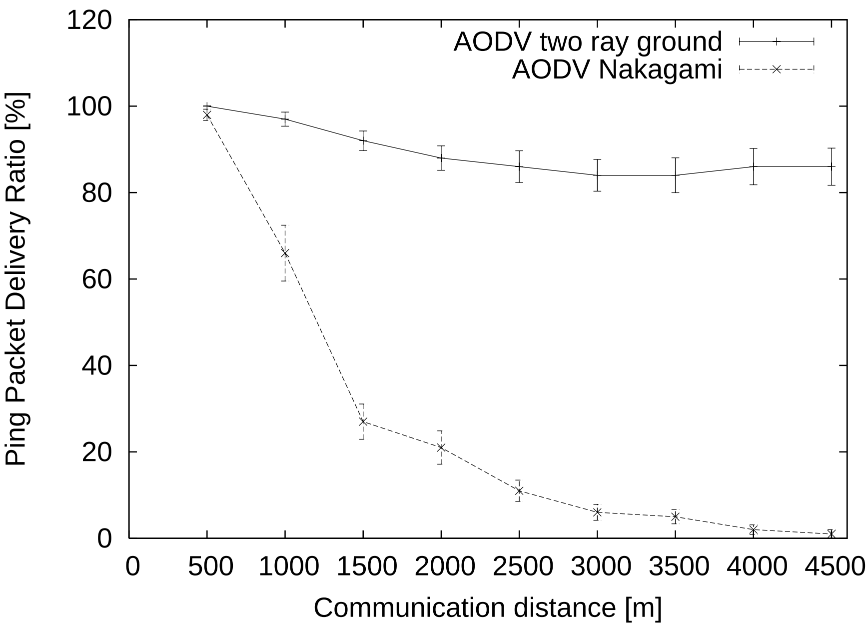


Figure 4.2: Ping message delivery ratio in a multi-hop highway scenario with a connected network and utilizing AODV, a communication range of 500 m, and the propagation models of two ray ground and Nakagami. Values presented with a 95% confidence interval.

Additionally, the high mobility of the nodes together with the large areas covered by vehicular networks make it infeasible to have a centralized management entity. Fair and efficient use of the resources is a hard task in a totally decentralized and self-organizing network. The Distributed Coordination Function (DCF) is a totally asynchronous approach and it is known for its inability to efficiently manage the media resources, especially in case of broadcast messages. Therefore, the inexistence of an entity able to synchronize and manage the transmission events of the different nodes in a network results in a less efficient usage of the channel (e.g., the use of random backoff timers is needed) and in an increased number of packet collisions (see Chapter 3).

The authors of [MLS04] propose an approach to coordinate the information exchange in the surrounding of a road side unit. However, the resulting strategy requires to silence all vehicles in a circle of radius 536 m during the coordinated message exchange of nodes within a much smaller circle of radius of 80 m.

4.1.5 System architecture design

In comparison to other communication networks, vehicular networks present unique characteristics with respect to applications, types of communication and self-organization. Contrary to traditional systems, safety-related communications do not consist of point-to-point unicast streams, but rather of broadcast or geocast dissemination of data. Also, it is expected that some information is of high value for many protocol entities, e.g., position of surrounding vehicles which can be used by both driver assistance and packet forwarding decisions. Additionally, control parameters should have a fine granularity, e.g., to send two consecutive packets through different channels or using different transmission power.

Furthermore, systems compatibility and cost related decisions can influence the architecture design of an IVC system and its features. For example, on the one hand, the compatibility of nodes with limited computational capabilities, e.g., cheap road side units, with others with strong computational resources may be required. On the other hand, the integration of one or multiple transceivers should be specified. The latter option must be carefully considered when assigning different types of data traffic to the available channels. Note that a prioritization among safety-related messages would be necessary in the (reasonable) case that they share one single channel or transceiver.

Last, communication control mechanisms must take into consideration the safety nature of the information carried on the different types of messages, i.e., it must be avoided that in order to ensure a stable system, the overall safety level is decreased in a specific environment.

All properties mentioned above make the system design of an IVC system itself a challenge. In Chapter 7, we discuss the main characteristics of IVC and reason the structuring of functionalities into modules in order to propose a system architecture tailored to vehicular networks' needs.

4.2 Design options of safety-related IVC

In the following, we address the two types of messages defined in Chapter 2 (beacons and event-driven messages) in more detail, including the requirements and challenges involved with both of them. Based on this analysis we will define in Section 4.3 the design criteria of the required communication strategies.

4.2.1 Periodic messages

In order to develop systems capable of detecting unsafe driving situations, communication protocols must provide to every node accurate and updated information about the state of all surrounding vehicles. We remark that even though the reception of a beacon is somehow 'expected', the information contained can be of critical importance in close distances to the sender since it can make possible to detect an unsafe road situation (e.g., proximity of crossing vehicles at an intersection). Therefore, it is important that *all* vehicles are able to transmit their state to the channel and, therefore, a fair assignment of the resources is fundamental. On top of that, we expect that for the system to be trustworthy, safety information should be delivered within a specific maximum time and with some minimum reliability. In the following, we outline the main requirements and discuss different design options in order to achieve a robust information exchange.

Requirements

Minimum update rate and minimum range: The baseline approach to inform the surrounding vehicles about one's state is to send an updated broadcast message in every specific period covering a specific area. These two parameters should be specified by application designers, who should take into consideration the requirements to improve safety as well as relevant matters such as reaction time of the human drivers, time needed to brake until stopping the car completely, accuracy of the positioning systems, etc. However, as mentioned in Chapter 2.3, a set of standardized requirements does not exist yet. Therefore, it is up to the communication protocol designers to find the technology limitations and propose the best alternatives to efficiently use the existing resources.

High reliability and controlled channel load: When intending to find technology limitations or to satisfy safety requirements, the challenges presented in Section 4.1 must be considered. More specifically, the hidden terminal problem and the radio channel characteristics result in a relevant amount of packets not being successfully received by their targeted destinations.Therefore, repetition of these messages (by the node generating the message itself or by some other one) or a higher packet generation rate will be required to guarantee a minimum reliability. Note though, that the physical channel presents a load limitation and a broadcast environment is likely to raise rapidly the number of collisions when the channel load is increased. Therefore, the amount of load added to the channel by all nodes sharing a medium has to be controlled to guarantee the system performance.

Fairness: In a communication network where safety is the main goal fairness becomes a critical issue. Trying to optimize, e.g., packet delivery ratio, achieved bandwidth, etc., without taking fairness into consideration can turn to be a harmful approach. In other words, improving, e.g., the overall packet delivery ratio of the system while not satisfying the safety requirements of a single node (transmission power, channel access opportunities, etc.) can become a danger for the surrounding nodes.

Additionally, it is very important to address fairness considering the different requirements, or 'level of danger', specific of each individual node in a network. Indeed, there exist a wide variety of nodes and situations in vehicular environments where different nodes could require a higher share of the resources due to their current status, e.g., their speed.

Design options

Packet generation rate: The straightforward approach to increase information accuracy is to raise the number of transmitted information updates. However, if all nodes on a network follow the same strategy it can be counterproductive due to an increased amount of packet collisions, as seen in Chapter 3. Assuming that all nodes act according to the same principles, increasing the packet generation rate has to be controlled. Indeed, the load offered to the channel has to be limited due to the challenges described above, i.e., the high amount of equipped vehicles expected in the future and the increasing amount of packet collisions experienced in broadcast environments with higher channel loads.

Transmission power control: How to select the intended transmission range of all nodes in a vehicular network is a key point for safety communication protocols. As with the packet generation rate, increasing the transmission power of a message can result in an increased safety, a larger range of awareness in this case. However, the listed characteristics of vehicular environments have to be taken into account to thoroughly balance the existing trade-offs.

On the one hand, we encounter two reasons to use a high power, a safety-related and a communication related. For safety purpose, the higher the area addressed by all state messages from a node the higher the level of safety can be achieved. For communication purpose, a higher power would help us fight against the radio channel propagation phenomena described in Chapter 4.1.2, as can be observed in existing analyses, e.g., [YEY+04]. On the other hand, having a higher communication range can result in a poorer system performance as shown in many topology or capacity studies, e.g., [GK00],[PS02] or [LNM04b].

Basically, as we have shown in Chapter 3.4.3, increasing the transmission power of all nodes on the road implies having to share the medium with a higher number of neighbors and, therefore, increasing the probability of packet collision at all distances from the transmitter. Especially, situations where the successful reception probability of messages significantly decreases at close distances from the transmitter should be avoided, see Figure 3.10.

Power control is also a versatile scheme in particular vehicular environments. A higher transmission power could improve road safety for special cases of the car state (e.g., speed, time to break completely), special situation on the road (e.g., last car in a traffic jam) and low vehicular density scenarios.

Single- or multi-hop: The range of awareness experienced by a vehicle could be extended without the need to increase the transmission power. Vehicle status information could be delivered to vehicles outside of direct communication range with the use of a multi-hop forwarding scheme based on aggregation, i.e., transmitting within the same message the sender's own status information together with the information gathered via the wireless channel about its neighbors. Of course, the impact in terms of additional load and reliability has to be studied. Moreover, this approach could benefit from the decreasing safety value of information for higher distances to adjust the re-transmission interval of some information and, thus, save some bandwidth.

4.2.2 Event-driven messages

In situations of danger the rapid dissemination of alert-messages may allow an intervention to avoid an accident. In *safety-of-life* situations, it is very important that the information is delivered reliably to all drivers in a certain geographical area with enough time to react. As with the periodic messages, in this section we outline the requirements of event-driven messages from a communication perspective and depict their design options.

Requirements

Geographical area of dissemination: Unlike periodic messages, event-driven messages are not used to detect a potential dangerous situation in the vehicle surrounding. Event-driven messages are the result of the detection of an existing hazard and, therefore, they are expected to travel larger distances than beacons by the use of multi-hop strategies. Depending on the type of safety application and the type of road, different geographical areas can be required for dissemination of the information.

Delay: In order to provide enough reaction time to a driver approaching a hazard, event-driven messages have to be disseminated with the maximum promptness. However, as in the case of periodic messages' requirements, there is no strict reference value to evaluate information dissemination protocols yet.

High reliability: The information carried by event-driven messages must be delivered to *all* vehicles located in the relevant area for dissemination, which is selected by the corresponding application. Note that at the moment a road accident occurs, all drivers with no exception must be warned of the peril. Any driver not realizing the anomaly of the situation can result in a danger itself.

Design options

Forwarding scheme: The most straightforward approach to disseminate information among nodes would simply flood the entire area, broadcasting an emergency message to all nodes in transmission range that, in turn, would retransmit the message again. Due to the multitude of retransmissions such a mechanism comes along with packet collisions and increased contention on the transmission channel, decreasing the reliability and speed of information dissemination. This problem is commonly known as the *Broadcast-Storm-Problem* (see [NTCS99]). However, many strategies have been proposed that improve the flooding mechanism and smartly choose specific nodes to forward the information. Among them, optimistic results are obtained by schemes that make use of position information, see Chapter 5.1. Note that it is a reasonable assumption that vehicles equipped with 5.9 GHz DSRC technology will also be equipped with a positioning system such as GPS.

Hop distance: When designing and adjusting a forwarding scheme the probabilistic radio channel characteristics and the possible channel load have to be taken into consideration. Selecting a forwarding node at further distances to the sender increases the probability of reception failure due to the radio channel phenomena and collisions from hidden nodes. On the other hand, choosing a closer node increases the reliability of the information delivery at the cost of an increased delay and overhead caused by a higher amount of wireless hops needed to reach all nodes in the selected area.

4.3 Design criteria for safety-related IVC protocols

In this chapter, we have identified the challenges of robust inter-vehicle communications that arise from the high mobility of the nodes, the hidden terminal problem, likely high channel load and unfavorable radio propagation conditions. In more detail, considering safety as the main and most beneficial goal of IVC, we discussed how the different challenges affect the safety-related communications in their effort of providing awareness of the vehicle's surroundings.

This thesis focuses on fully deployed vehicular networks, where all vehicles are equipped with IVC systems, and where situations are encountered where the technology limitations described above become a challenge. Unfortunately, these situations are often critical in terms of safety. For instance, consider scenarios with medium to high vehicle densities and relatively high speeds, such as highways near the entrance of big cities or a temporary working area. Due to a large number of vehicles sharing the medium, it is not clear whether the channel capacity is sufficient to support the data load generated by beaconing while at the same time leaving enough available bandwidth for event-driven safety messages.

In the following we outline the rationale behind the strategies proposed in Chapter 5. In more detail, we *i)* present the link between safety and fairness as a sequence of reasonings that eventually define the requirements for fair power adjustment for vehicular networks, and *ii)* outline the need of a multi-hop strategy able to cope with an unreliable wireless channel.

1. Relevance of safety messages. Event-driven messages should be able to access the channel with short delay, and they should have low probability of collision even when targeting large areas, i.e., when being transmitted with high power and using multi-hop strategies. Beacons, on the other hand, show a high relevance in the close neighborhood of the sender, but they are less relevant at higher distances (in analogy to the standard 'safety distance' of vehicles[2]). Additionally, under the reasonable assumption that safety-related messages will share one single channel (or one transceiver): a resource allocation strategy is needed that achieves a clear *prioritization*, or *balance*, among the messages according to their relevance for safety.

2. Controlling the beaconing load. In Chapter 3, we have evaluated the reception rates of periodic broadcast messages for different configurations of transmission power and packet generation rate. On the one hand, the results of our evaluation have shown that, as expected, lower beacon generation rates achieve higher probability of message reception due to a lower channel load. However, a maximum time span between updated beacon messages is strictly required by safety applications in order to be capable of detecting a dangerous situation. On the other hand, we observed that while increasing the transmission power extends the communication range, it could also lead to a congested channel where reception rates for vehicles close to the sending vehicle decrease due to packet collisions. Accounting for these observations, we propose to adjust the transmission power of beacons in case of congestion. The proposed mechanism should keep the load on the wireless medium below a certain level, called Maximum Beaconing Load (MBL) in the following.

We are aware of the fact that before decreasing the transmission power of beacons other strategies should be implemented, such as an admission control mechanism to drop all non-safety related packets before they are sent to the channel, or dynamically adjusting the packet generation rate to the minimum required by the safety applications. Nevertheless, there will be many situations where decreasing the transmission range of certain nodes on top of that is necessary (e.g., fast moving medium density traffic conditions).

Although transmit power control has been a deeply studied subject in the mobile networks field already (see related work in Section 5.1), vehicular environments present new challenges. Most of previous studies addressing power control try to ensure connectivity and/or optimize capacity of ad hoc networks. However, the primary goal of transmit power control when applied to IVC is not to opti-

[2]The safety distance of a vehicle commonly refers to the distance that a driver needs in order to stop the vehicle completely, and it is approximately calculated (in meters) as half of the value of the speed (in km/h). For example, a car driving at 120 km/h has a safety distance of approximately 60 m.

mize data transport capacity for several ongoing point-to-point communications, or to build a connected network topology (see the toy examples depicted in Figure 4.4), but instead to improve as much as possible the driver's awareness of a vehicle's surroundings.

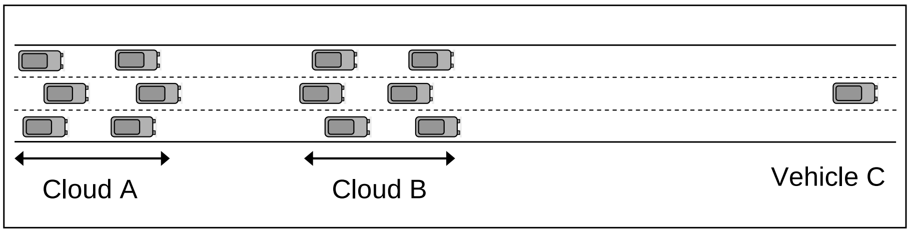


Figure 4.3: If nodes from Cloud B would try to be connected with far away Vehicle C, they can create a high level of interference disturbing information exchange among vehicles inside Cloud A.

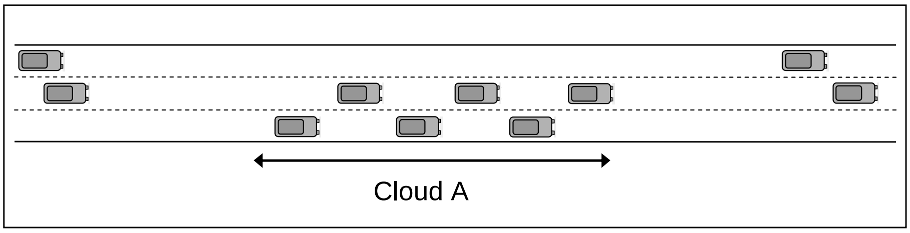


Figure 4.4: If nodes forming Cloud A would try to optimize capacity they would adjust their transmit power to reach only the closest car [GK00]. In this case, they would not have direct awareness of the next vehicle in the same lane even though it is very close.

3. The elements of fairness. To limit the beaconing load offered to the medium below the specific common MBL, vehicles should restrict their beacons' transmission power. From an individual safety point of view (e.g., looking at the kinetic energy of vehicles) a higher range of awareness is preferable. From a system perspective the vehicle with the minimum transmission power can be considered a hazard to other cars. Note that, it is very important that *every* vehicle has a good estimation of the state of *all* other vehicles (with *no* exception) in its proximity. Thus, essentially, a max-min fairness concept is required. One might argue that due to different velocities of vehicles – or more generally due to different 'states' of the vehicles – the vehicles should send beacons with a transmission power value related to their velocity or states. In this case, the transmission power should be restricted by a weighted scheme to satisfy MBL.

4. Fairness with low complexity. Vehicular networks are composed of highly mobile nodes. Therefore, the power adjustment mechanism cannot be based on a strategy which converges to stable power settings over a relatively long period of time. Instead, it must be able to quickly react to changes of nodes' requirements and locations, and operate in a distributed fashion.

5. Balancing event-driven messages and beacons. As mentioned in the first point, in case that both event-driven messages and beacons share one channel, a 'congestion control mechanism' considering their relevance to safety is required. This way, by restricting the transmission power of beacons but not the one of the event-driven messages, the MBL threshold can be seen as a handle to fine-tune the level of prioritization between both types of messages: by increasing the MBL, the beaconing activity is assigned a larger portion of the available bandwidth and a relatively 'lower' priority (although still higher than that of beacons) is implicitly assigned to event-driven messages.

6. Dissemination of Emergency information. The strategy responsible to disseminate event-driven messages has to be robust against the uncertainties caused by node mobility, packet collisions and radio propagation phenomena. To overcome these challenges, contention-based approaches are a promising candidate to select the nodes to forward the message, as we showed in [TMSEFH06]. These schemes make use of contention periods to designate the node that forwards the message next (next hop). This way, after a message transmission, all receivers wait a certain time before forwarding the message, using the newly forwarded message as an 'implicit ack' to cancel the running contention process. Indeed, not selecting the next hop prior to transmission alleviates the dependence on one single node, allowing all neighbors to be potential forwarders at once. Additionally, in safety-of-life situations message retransmission strategies could be added in order to achieve a higher reliability, if needed.

5

Design of Communication Protocols to Support Active Safety

In this chapter, we propose two protocols to overcome the challenges and achieve the goals specified in Chapter 4. First, we develop D-FPAV (Distributed Fair Power Adjustment for Vehicular environments) in order to adjust the transmission power of beaconing messages. While beaconing messages are necessary to enable IVC-based active safety applications, we observed in Chapter 3 that an uncontrolled load on the channel results in a high amount of packet collisions and therefore in a decreased safety level. The goal of D-FPAV is to control the resulting load of beacons on the channel such that it is below an MBL (Maximum Beaconing Load) limit. The D-FPAV protocol is formally proven to achieve fairness, which we believe is fundamental in order to accomplish IVC's ultimate goal of increasing road safety.

Then, we propose the EMDV (Emergency Message Dissemination for Vehicular environments) protocol to disseminate emergency information within a geographical area. The EMDV protocol is to be utilized in safety-of-life situations when a hazard is detected, and its goal is to deliver to the approaching vehicles the information required to avoid the hazard. The key objectives of EMDV are robustness against packet reception failures (due to packet collisions and received power fluctuations) as well as to provide a short delay.

Before the protocols description, we present the studies and approaches related to our work.

5.1 Related work

As outlined above, in this chapter we propose two protocols for safety-related IVCs with different goals: channel congestion avoidance and dissemination of emergency information. Therefore, we address the relevant work related to both subjects separately.

We first discuss the related work of our congestion control strategy which is based on power control and fairness. To the best of our knowledge, the only proposal that exists in the IVC field to alleviate the load on the wireless channel is to prevent lower priority messages of being transmitted. The IEEE 802.11p draft [11p] proposes to transmit only messages with the highest priority if the channel occupancy rate is higher than 50%. However, as observed in Chapter 3 further strategies are needed to control solely the load on the channel generated by beaconing messages. Apart from congestion control, our work is related to research in two other fields: topology control and fairness.

Power control in ad hoc networks has been an intensively studied subject for many years in the field of topology control. However, vehicular networks' specific paradigms and the particularity of having safety as the main goal make all these analyses or proposed algorithms not valid to satisfy IVC's requirements. Most of these power control studies address unicast environments and intend to improve the spatial reuse by minimizing the interference or energy consumption. These studies find the path to the destination that minimizes energy consumption and/or maximizes the overall throughput, see [KK05]. References [CSW03], [KKW$^+$03] and [CFK03] propose 'energy aware' adaptive algorithms that make use of only local information to adjust their power. Further, the study [XYLW05] also considers non-uniform transmission ranges. A slightly different approach is taken in [PS02], [PS03] and [LL02] where the authors agree that the minimum transmission power does not always maximize throughput and then propose an adaptive algorithm as a function of the traffic load. Although we can find related issues and interesting methodologies in all these studies we have to remember that energy efficiency is not an issue in vehicular networks where nodes have almost unlimited power supply for communication. Another common goal of these approaches is to keep the network connected for unicast flows, which is totally different from the goal of our system design. As specified in Chapter 4.3, our goal is to make sure that nodes close to the sender receive the messages with high probability while ensuring fairness in the overall system.

Maybe the most related study to our work is performed by Li *et al.* in two steps [LNM04a] and [LNM04b]. The authors propose, first, an analytical model able to find a transmission power that maximizes 1-hop broadcast coverage and, second, an adaptive algorithm that converges to a given fixed transmission power. Although they focus on a pure broadcast environment, their assumptions make their approach infeasible for vehicular networks: *a)* all nodes are static and *b)* all nodes have the same priority (i.e., the same required transmission power levels).

The second area of research related to our power control work is the one addressing fairness in order to share the wireless media. In the literature, there exist two main principles to assign network resources based on fairness criteria: proportional fairness, introduced by Kelly *et al.* [KMT98], and max-min fairness, utilized as a design objective for communication networks first by Bertsekas and Gallager [BG87]. Both principles present a different balance with respect to the existing trade-off between 'efficiency' and 'fairness'. As stated in Chapter 4.3, in order to maximize safety, the awareness of the close surrounding should be maximized, i.e., a vehicle without a fair assignment of resources becomes a danger itself. Therefore, max-min fairness is the selected criterion to be followed by our proposed protocol.

Strategies to achieve fairness in conventional networks often consider only unicast communications and either *i)* assign a portion of the estimated bandwidth to each flow, such as [FB04], or *ii)* provide a scheduling mechanism to achieve its fairness criteria, e.g., [GNB01]. Recently, due to the increasing attention gained by inter-vehicle communications, some studies have tried to apply these methodologies to vehicular environments. The work [ARP05] addresses power control in IVC with the goal of producing a connected network topology. [WR05] describes a scheme based on a utility fair function to share the broadcast media. In the latter, a scheduling approach is proposed that is applicable to non-safety IVC applications, however, it does not satisfy all the safety requirements presented in Chapter 4.

With respect to our second proposed protocol, for information dissemination, several studies exist in the mobile ad hoc networks literature for improving efficiency of data dissemination. These include probabilistic [NTCS99], area-based [DPIK05], and neighbor-knowledge schemes [DPIK05, SM00]. However, they do not consider the key aspects of vehicular communication, especially the high requirements of safety-of-life applications.

Furthermore, we can find several strategies in the field of IVC that take advantage of the existence of positioning systems, e.g., GPS, to improve simple flooding. These approaches are designed according to different criteria corresponding to different types of applications and environments.

On the one hand, there is a group of studies which address non-safety applications and, therefore, are not designed according to strong reliability constraints and pay little or no attention to the reduction of the delay experienced during the dissemination process. These schemes, e.g., [SFL+00], [WFGH04], [LA05], [WER05], [NSI06] and [CGM06], intend to deliver information over large distances, from several kilometers to complete cities. Also, there exist non-safety information dissemination schemes addressing smaller areas, e.g., in order to enable cooperative driving, such as [TAF00].

On the other hand, several proposals exist which consider time-critical safety applications such as [DDB05], [STC+06], [BTD06] and [BSH00], which intend to deliver the information to all vehicles within local areas (up to a couple of kilometers) with low delay. Durresi *et al.* propose in [DDB05] to construct a hierarchical structure among cars driving in the same direction in order to manage efficiently the dissemination process. However, highly dynamic topologies cannot be supported, e.g., with cars entering or leaving the road.

Sormani *et al.* [STC$^+$06] suggest selecting message forwarders by the use of a probabilistic scheme, which is not proven to be a valid approach to reliably deliver time-critical information.

The authors of [BTD06] and [BSH00] propose interesting schemes to disseminate the emergency information in a certain direction making use of contention periods, i.e., after a message transmission all receivers wait a certain time before forwarding the message. Briesmeister *et al.* [BSH00] favor the re-transmission of receivers located at further distances from the sender by the selection of shorter waiting times. Biswas *et al.* [BTD06] propose selecting random waiting times and utilize an implicit acknowledgment scheme to cancel re-transmissions from nodes closer to the danger (where the message was originated).

Our proposed approach for information dissemination described in Section 5.3 makes use of the two latter principles (from [BTD06] and [BSH00]) and further complements them with mechanisms aimed at reducing dissemination delay and improving reliability. Furthermore, contrary to all above cited studies, we consider probabilistic radio propagation and high medium load conditions resulting from beaconing, as described in Chapter 4.3.

5.2 Congestion control with fair power adjustment

Based on the rationale described in Chapter 4.3 we propose a power adjustment strategy in order to limit the beaconing load on the wireless channel. This strategy is built upon the concept of fairness since, as previously discussed, it is the design concept that best fits the safety nature of inter-vehicle communications. Before presenting the protocol, we specify the scenario we focus on and provide the formal description of the problem.

5.2.1 Reference application scenario

We consider a scenario in which a set of vehicles is moving along a road and periodically send beacon messages to inform the nodes in their vicinity about their current position, direction, velocity, etc. For clarity reasons in the problem formulation, we assume that the beaconing frequency is the same for all the nodes in the network and that all beacons have a fixed size (or average size). However, the power used to transmit the beacons can be adjusted, so that the overall network bandwidth used for beaconing can be controlled.

In principle, a node will send its beacon at maximum power, as this in general guarantees that more nodes will receive the beacon, resulting in increased safety conditions. However, the higher the power used to send beacons, the higher is the network load generated by the beacon exchange activity.

In the envisioned application scenario, the beaconing activity is assigned with a limited portion of the available network bandwidth *MBL*, in order to avoid saturating the wireless channel, as shown in Chapter 3. Thus, the 'node optimal strategy' of sending the beacon at maximum power in general conflicts with the network-wide task of keeping the network load offered by beaconing below a certain threshold. As a consequence of this, we need a distributed strategy for setting the node transmit power levels such that the beaconing network load does not exceed the threshold, and the beaconing transmit power levels are maximized.

5.2.2 Formal problem definition

Assume a set of nodes $N = \{u_1, \ldots, u_n\}$ is moving along a road. To simplify the problem statement, we assume that the road is modeled as a line[1] of unit length, i.e., $R = [0, 1]$, and that nodes can be modeled as points in $[0, 1]$. Given a node $u_i \in N$, $x(i, t)$ denotes the position of u_i in R at time t. To simplify the notation, in the following we drop the argument t, focusing our attention on a snapshot of the system at a certain time instant.

Each of the network nodes sends a beacon with a pre-defined beaconing frequency F, using a certain transmit power $p \in [0, P_{max}]$, where P_{max} is the maximum transmit power. In order to simplify the presentation, we assume that all the nodes have the same maximum transmit power level. We remark that this assumption is made only to simplify the notation, and the framework described in this section can be applied to the case when the nodes have different maximum transmit power levels.

Definition 1 (Power assignment)**.** *Given a set of nodes* $N = \{u_1, \ldots, u_n\}$*, a power assignment* PA *is a function that assigns to every network node* u_i*, with* $i = 1, \ldots, n$*, a ratio* $PA(i) \in [0, 1]$*. The power used by node* u_i *to send the beacon is* $PA(i) \cdot P_{max}$*.*

Definition 2 (Carrier Sensing Range)**.** *Given a power assignment* PA *and any node* $u_i \in N$*, the carrier sensing range of* u_i *under* PA*, denoted* $CS(PA, i)$*, is defined as the intersection between the commonly known CS range of node* u_i *at power* $PA(i) \cdot P_{max}$ *and the deployment region* R*. The CS range of node* u_i *at maximum power is denoted* $CS_{MAX}(i)$*.*

The above definition of carrier sensing deserves some further explanation. As discussed in Chapter 3.2.2, modeling the CS range as a deterministic situation is a simplification of what occurs in practice, where the wireless channel conditions fluctuate over time. It is not difficult to extend our definition of carrier sensing to account for variable channel conditions: essentially, it is sufficient to associate a certain probability density function over [0,1] to each pair $(u_i, PA(i))$. However, in order to simplify the presentation of our framework, we assume that the

[1]Modeling the road as a line is a reasonable simplification in our case since we assume the communication ranges of the nodes to be much larger than the width of the road.

notion of carrier sensing range is deterministic and it is defined by the received signal power mean value.

Besides the deterministic carrier sensing assumption described above our notion of carrier sensing range is very general, as we do not assume that the CS range is regular – e.g., a segment centered at $x(i)$ – nor that it is contiguous – due to the presence of obstacles, there might exist 'holes' in the carrier sensing region. The only other assumption necessary for the correctness of the proposed framework is a monotonic property, namely that the carrier sensing range of node u_i at power $(PA(i) + \epsilon) \cdot P_{max}$ contains the carrier sensing range of node i at power $PA(i) \cdot P_{max}$, for every $\epsilon > 0$.

Given a power assignment PA, the network load generated by the beaconing activity under PA is defined as follows:

Definition 3 (Beaconing load under PA)**.** *Given a set of nodes* N *and a power assignment* PA *for the nodes in* N*, the beaconing network load at node* u_i *under* PA *is defined as:*

$$BL(PA, i) = |\{u_j \in N, j \neq i : u_i \in CS(PA, j)\}| ,$$

where $CS(PA, j)$ *is the carrier sensing range of node* u_j *under power assignment* PA.

We remark that the above definition of beaconing load can be extended to account for beacon messages of different size, and for different beaconing frequencies in the network. The framework for distributed power control discussed below can be applied also with a more general definition of beaconing load.

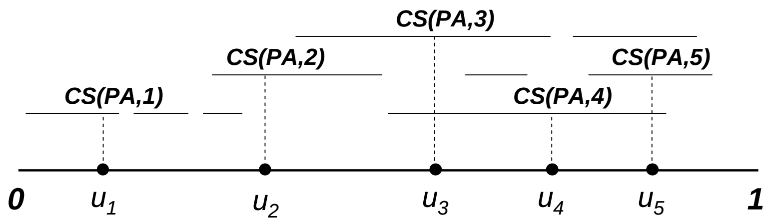


Figure 5.1: Network load based on carrier sensing: the maximum load is experienced in $R = [0, 1]$ where the number of intersecting carrier sensing ranges is maximal. In the example, we have $BL(PA, 5) = 3$.

An example clarifying our notion of network load based on carrier sensing is depicted in Figure 5.1. The intuition is the following: since the beaconing frequency is pre-determined, the network load depends on the transmit power levels used for beaconing – the higher these levels, the higher the network load[2]. Assuming that nodes are not allowed to transmit while they sense some message in

[2]Here, we use the assumption of monotonic carrier sensing range.

the channel, the maximum load is experienced in those subregions of R where the number of intersecting carrier sensing ranges is maximal.

We are now ready to define the beaconing with max-min transmit power problem addressed in this thesis:

Definition 4. *(Beaconing Max-Min Tx power Problem (BMMTxP)): Given a set of nodes* $N = \{u_1, \ldots, u_n\}$ *in* $R = [0, 1]$*, determine a power assignment* $\overline{PA}$ *such that the minimum of the transmit powers used by nodes for beaconing is maximized, and the network load experienced at the nodes remains below the beaconing threshold* MBL*. Formally,*

$$\begin{cases} \max_{PA \in \mathbf{PA}} (\min_{u_i \in N} PA(i)) \\ \text{subject to} \\ \quad BL(PA, i) \leqslant MBL \ \forall i \in \{1, \ldots, n\} \end{cases},$$

where **PA** *is the set of all possible power assignments.*

Essentially, we are interested in finding the power assignment scheme such that the minimal 'quality of service' guaranteed to the network nodes is maximized, i.e., is fair to all nodes, while not exceeding the portion of network bandwidth assigned to the beaconing activity. Notice that in our problem formulation we assume that the portion of bandwidth assigned for beaconing can be expressed in terms of the maximal number of overlapping nodes' carrier sensing ranges in a single point. This assumption is reasonable under our working hypothesis of fixed beaconing frequency and message size.

Also, note that our problem definition differs from the standard formal definition of max-min fair allocation, as in [BG87]. As we further discuss in Section 5.2.3, we do not require all the 'resources' to be assigned.

Therefore, in general there exist several power assignments that can be regarded as optimal solutions to BMMTxP. For instance, assuming a certain power assignment $\overline{PA}$ is optimal for BMMTxP, and there exists a node $u_i \in N$ such that the power assignment $\overline{PA}(i, \epsilon)$ obtained from $\overline{PA}$ by increasing u_i's transmit power to $(PA(i) + \epsilon) \cdot P_{max}$, for some $\epsilon > 0$, does not violate the constraint on the network load. It is immediate to see that $\overline{PA}(i, \epsilon)$ is also an optimal solution to BMMTxP.

5.2.3 The FPAV algorithm

In this section we present a centralized algorithm for solving BMMTxP. The algorithm, called FPAV (Fair Power Adjustment for Vehicular environments) and based on a 'water filling' approach [BG87], is able to compute PA when global knowledge is assumed.

The FPAV algorithm, which is summarized in Figure 5.2, works as follows: every node starts with the minimum transmit power, and all the nodes increase their transmit power simultaneously with the same amount $\epsilon \cdot P_{max}$ as long as the constraint on the beaconing network load (*MBL*) is not violated. Note the strict fairness is achieved at the end of this stage where all nodes increase their power the same number of steps k and end up with a power of $p = (k\epsilon) \cdot P_{max}$.

Algorithm FPAV:
Input: a set of nodes $N = \{u_1, \dots, u_n\}$ in $[0, 1]$
Output: a power assignment PA which is an ($\epsilon \cdot P_{max}$-approximation of an) optimal solution to BMMTxP

```
∀uᵢ ∈ N, set PA(i) := 0
while (BL(PA) ⩽ MBL) do
   ∀uᵢ ∈ N, PA(i) := PA(i) + ϵ
end while
∀uᵢ ∈ N, PA(i) := PA(i) − ϵ
```

Figure 5.2: The FPAV algorithm.

Notice that in a previous work [TMSH05] we proposed a 'second stage' of the FPAV algorithm in order to achieve per-node maximality. At the second stage, specific nodes could further increase their transmission power until no node was able to increase without violating the condition on beaconing load, in accordance to the formal definition of max-min fair allocation as in [BG87]. However, simulation experiments where global knowledge was assumed showed that the second stage could only achieve a marginal gain in scenarios with high network dynamics. Therefore, and due to the higher complexity that it would add to the distributed protocol presented in the next section, the second stage of the algorithm is not considered here.

The following theorem shows that the FPAV algorithm results in an optimal solution to BMMTxP. Technically, the power assignment computed by this strategy is an $\epsilon \cdot P_{max}$-approximation of the optimal solution to BMMTxP. Since the step size ϵ is an arbitrarily small constant, the solution computed by BMMTxP can be regarded as optimal for all practical purposes.

Theorem 1. *The FPAV algorithm computes an $\epsilon \cdot P_{max}$-approximation of the optimal solution to BMMTxP for any constant $\epsilon > 0$.*

Proof. First, we observe that the power assignment PA computed by FPAV, with a power level $p = (k\epsilon) \cdot P_{max}$, is the minimal assignment among all the power assignments with minimum power level p, since in PA *all* the nodes have the same power level p. Thus, if a power assignment PA' with minimum power level

p does not violate the constraint on the network load, then also does PA because the nodes' carrier sensing ranges under PA' are at least as large as those under PA. This is true because of the assumption of monotonic carrier sensing range.
Let $\overline{p}$ be the minimum of the node transmit powers in an optimal solution to BMMTxP, and assume $(k\epsilon) \cdot P_{max} < \overline{p} \leqslant ((k+1)\epsilon) \cdot P_{max}$ for some $k \geqslant 0$. The following cases can occur:

(i) $\overline{p} = ((k+1)\epsilon) \cdot P_{max}$. Given the observation above it follows immediately that the power assignment computed by FPAV is optimal, indeed our algorithm would compute $\overline{p}$ in this case;

(ii) $(k\epsilon) \cdot P_{max} < \overline{p} < ((k+1)\epsilon) \cdot P_{max}$. In this case, given the observation above and the assumption of monotonic carrier sensing range we can conclude that the power assignment PA computed by FPAV is a feasible solution to $BMMTxP$, which is at most $\epsilon \cdot P_{max}$ away from the optimal solution.

This concludes the proof of the theorem. □

Observe that we had to introduce the constant ϵ in our algorithm to discretize the process of increasing the nodes' transmit power. The smaller ϵ, the more accurate the solution computed by FPAV, the longer the running time of the algorithm. On the other hand, in a practical setting we expect that nodes can set the transmit power only to a limited number of different levels, and discretizing the transmit power increase process is not an issue. It is immediate to see that, under the assumption that all the nodes use the same power levels $\{p_1, \dots, p_h\}$, the FPAV algorithm computes an optimal solution to BMMTxP (subject to the constraint that the possible power levels for the nodes are $\{p_1, \dots, p_h\}$).

5.2.4 The D-FPAV protocol

Clearly, a centralized strategy is impractical for a real and dynamic vehicular scenario. In this section, we present a fully distributed, asynchronous, and localized protocol called Distributed Fair Power Adjustment for Vehicular environments (D-FPAV) for solving BMMTxP.

D-FPAV is based on locally executing the FPAV algorithm at each node, on exchanging the locally computed transmit power control values among neighbors, and on selecting the minimum power level amongst the one computed locally and those computed by the neighbors.

D-FPAV is summarized in Figure 5.3. A node u_i continuously collects the information about the status (current position, velocity, direction, and so on) of all the nodes within its CS_{MAX} range. These are the only nodes that node u_i can affect when sending its beacon. In order to obtain the information from nodes outside of the communication range, a strategy based on multi-hop communication has to be utilized. Various alternatives of the strategy are discussed later in this section. Based on this information, node u_i makes use of FPAV to compute

PROTOCOL D-FPAV: (operation at node u_i)
INPUT: status of all the nodes in $CS_{MAX}(i)$
OUTPUT: a power setting $PA(i)$ for node u_i, such that the resulting power assignment is an optimal solution to BMMTxP

1. Based on the status of the nodes in $CS_{MAX}(i)$, use FPAV to compute the maximum common tx power level P_i s.t. the MBL threshold is not violated at any node in $CS_{MAX}(i)$

2a. Deliver P_i to all nodes in $CS_{MAX}(i)$

2b. Collect the power level values computed by nodes u_j such that $u_i \in CS_{MAX}(j)$; store the received values in P_j

3. Assign the final power level: $PA(i) := \min\left\{P_i, \min_{j:u_i \in CS_{MAX}(j)}\{P_j\}\right\}$

Figure 5.3: The D-FPAV protocol. Note that in order to deliver/collect information to/from nodes outside the communication range multi-hop communication is involved (steps 1, 2a and 2b).

the maximum common value P_i of the transmit power for all nodes in $CS_{MAX}(i)$ such that the condition on the MBL is not violated (step 1). Note that this computation is based on local information only (the status of all the nodes in $CS_{MAX}(i)$), and it might be infeasible globally, it might violate the condition on MBL at some node. To account for this, node u_i must deliver the computed power level P_i to all nodes in $CS_{MAX}(i)$ (step $2a$). Also, node u_i collects the same information from the nodes u_j such that $u_i \in CS_{MAX}(j)$ (step $2b$). Node u_i can assign the transmit power level to the minimum among the value P_i computed by the node itself and the values computed by nodes in the vicinity (step 3). Setting the final power level to the minimum possible level is necessary in order to guarantee the feasibility of the computed power assignment (see Theorem 2 below).

Theorem 2. *Assume the CS ranges of the nodes are symmetric, i.e.,* $u_i \in CS_{MAX}(j) \Leftrightarrow u_j \in CS_{MAX}(i)$. *Then, D-FPAV computes an optimal solution to BMMTxP.*

Proof. First, we have to show that the power assignment computed by D-FPAV is a feasible solution to BMMTxP. Assume the contrary, i.e., there exists node u_i such that $BL(PA, i) > MBL$, where PA is the power assignment computed by D-FPAV. This means that node u_i has too many interferers, all of which are located in $CS_{MAX}(i)$ (assuming symmetric CS ranges). Let $u_j, \ldots, u_{j+h}$, for some

$h > 0$, be these interferers, and let PA_i be the power assignment computed by node u_i for all the nodes in $CS_{MAX}(i)$. In step 1 of D-FPAV, u_i computes an optimal solution PA_i to BMMTxP restricted to $CS_{MAX}(i)$. Assuming symmetric CS ranges, this solution includes a power setting for the interferers $u_j, \dots, u_{j+h}$, and this power setting is such that $BL(PA_i, i) \leqslant MBL$. At step 2 of D-FPAV, the power setting PA_i is broadcasted to all the nodes in $CS_{MAX}(i)$, which includes all the interferers $u_j, \dots, u_{j+h}$. Hence, each of the interferers receives from node u_i a power setting PA_i such that the condition on the beaconing load is not violated at node u_i. Since the final power setting of the interferers is at most PA_i (this follows from the minimum operation executed at step 3 of D-FPAV), and assuming a monotonic CS range, we have that the beaconing load at node u_i cannot exceed the MBL threshold – contradiction. This proves that the power assignment computed by D-FPAV is a feasible solution to BMMTxP.
We now prove that the computed power assignment is optimal. Let PA be the power assignment computed by D-FPAV, and let p_{min} be the minimum of the node power levels in PA. Assume PA is not optimal, i.e., that there exists another feasible solution PA' to BMMTxP such that the minimum of the node power levels in PA' is $p' > p_{min}$. Without loss of generality, assume that PA' sets the power level of all the nodes to p'. Since PA' is feasible, we have that $BL(PA', i) \leqslant MBL \ \forall i \in 1, \dots, n$. Hence, each node u_i in the network computes a power setting $P_i \geqslant p'$ at step 1 of D-FPAV. Consequently, the final power setting of every node in the network as computed by D-FPAV is at least $p' > p_{min}$, which contradicts our initial assumption. It follows that the solution computed by D-FPAV is optimal. □

Theorem 3. *D-FPAV has* $O(n)$ *message complexity, where* n *is the number of nodes.*

The straightforward proof of the theorem is omitted.

Let us use the scenario of Figure 5.4 to illustrate D-FPAV execution with a toy example. We have eight vehicles, denoted $u_1, \dots, u_8$, which are placed on a 1km long road, with relative distance varying from 50 m to 150 m. For the sake of clarity, we assume that the carrier sensing range can be represented as a segment centered at the transmitting node, and that CS_{MAX} is 250 m for all nodes. We also assume that all nodes send beacons of the same size with equal frequency and the maximum beaconing load MBL is such that any node can be in the CS range of at most two other nodes.

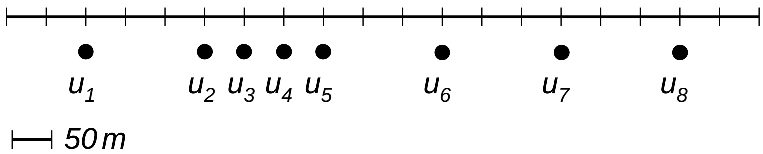


Figure 5.4: Node deployment used in the example of D-FPAV execution.

	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8
u_1	100	100	100	100				
u_2	50	50	50	50	50			
u_3	50	50	50	50	50	50		
u_4	50	50	50	50	50	50		
u_5		50	50	50	50	50		
u_6			100	100	100	100	100	
u_7						250	250	250
u_8							250	250

Table 5.1: Summarization of D-FPAV execution. Entries represent in meters the maximum allowed value of the CS range per node.

We summarize D-FPAV execution with the matrix reported in Table 5.1, where the row corresponding to node u_i reports the values of the transmit power (actually, what is reported in the entries is the value of the CS range, which is defined by a correspondent transmit power level) as computed by node u_i for all the nodes within its maximum CS range. For instance, the first row of the matrix represents the fact that node u_1 computes the maximum allowed CS range to be 100 m for all the nodes within its maximum CS range, i.e., nodes $u_1, \dots, u_4$. On the other hand, columns represent all the values of the allowed CS range that a node receives from the nodes within its CS range. For instance, the first column represents the fact that node u_1 collects a power setting for itself from nodes $u_2, \dots, u_4$. Then, the final power setting for every node in the network as computed by D-FPAV corresponds to taking the minimum over the values in its column. In our example, nodes $u_1, \dots, u_6$ end up with D-FPAV setting the transmit power to a value such that the corresponding CS range is 50 m, while the CS ranges of nodes u_7 and u_8 can go up to 100 m and 250 m respectively.

Estimation of status information

Note that, while a perfect information accuracy from *all* nodes inside $CS_{MAX}(i)$ is required in order to guarantee a strict fairness, it is still impractical in a realistic and dynamic scenario prior to each beacon transmission. In the following, we discuss how node u_i can collect the status information of all its surrounding nodes and the arising trade-off between information accuracy and additional overhead. Clearly, the only option to acquire status information from all nodes in $CS_{MAX}(i)$ is making use of a multi-hop strategy in addition to the existing beaconing, i.e., nodes re-transmit the status of their neighbors (this is because the CS range is larger than the communication rage). In order to determine this strategy, the following criteria should be defined: how often the neighbors' status must be forwarded, what range of neighbors must be included, and which transmission power must be used to transmit this information. Note that D-FPAV also requires delivering the P_i values to all nodes in $CS_{MAX}(i)$. Therefore, we propose to aggregate the P_i values with the status information of the corresponding nodes inside $CS_{MAX}(i)$ and then, to improve efficiency, to piggyback this aggregated information in beacon messages.

Now, other choices must be made for what concerns how often the aggregated information should be piggybacked in the beacons, and which transmit power should be used to send beacons containing this additional information. In making these choices there is a trade-off between additional overhead on the channel and accuracy of the neighbors status information available at the nodes. In order to select the most appropriate option, we perform in Chapter 6 a set of ns-2 based simulations to evaluate their performance. In the following, we provide a brief description of each simulated configuration with their corresponding name:

1. $1over1$: piggyback the aggregated status information with each beacon and transmit it with power $PA(i)$ (the value as computed by D-FPAV).
2. $1over5max$: piggyback the information every 5 beacons and use power P_{max} for sending the extended beacon.
3. $1over5$: piggyback the information every 5 beacons and use power $PA(i)$ for sending the extended beacon.
4. $1over10max$: piggyback the information every 10 beacons and use power P_{max} for sending the extended beacon.
5. $1over10$: piggyback the information every 10 beacons and use power $PA(i)$ for sending the extended beacon.

We considered that sending piggybacked beacons with a lower frequency than one every 10 beacons would cause D-FPAV to deal with too much outdated information.

5.3 Emergency information dissemination

The second main goal of IVC identified in Chapter 4.3 is the dissemination of event-driven emergency information within a geographical area. In order to deliver a message[3] containing information about an existing threat an effective strategy offering short delay is required.

5.3.1 Reference application scenario

We assume a scenario where all nodes are equipped with a positioning system, such as GPS (Global Positioning System). Furthermore, all vehicles are equipped

[3]Unless otherwise stated, in this section by 'message' we mean 'event-driven emergency message'.

with IVC systems and transmit beacons. In such scenario, illustrated in Figure 5.5, a vehicle detecting a hazard in a safety-of-life situation issues an event-driven message in order to warn the drivers approaching the danger. The originating node, according to the corresponding safety application, specifies the relevant area for dissemination of the alert (*dissemination area*). The alert must be distributed up to the border of the dissemination area, possibly via multi-hop transmissions, with high reliability and short delay. In this thesis, we study the case where roads do not comprise intersections (or highway entry/exit), and make the reasonable assumption that the communication range of an emergency message is larger than the road's width. The protocol proposed in this section can be extended with smart strategies such as [LMFH05] or with the use of digital maps in order to support road junctions.

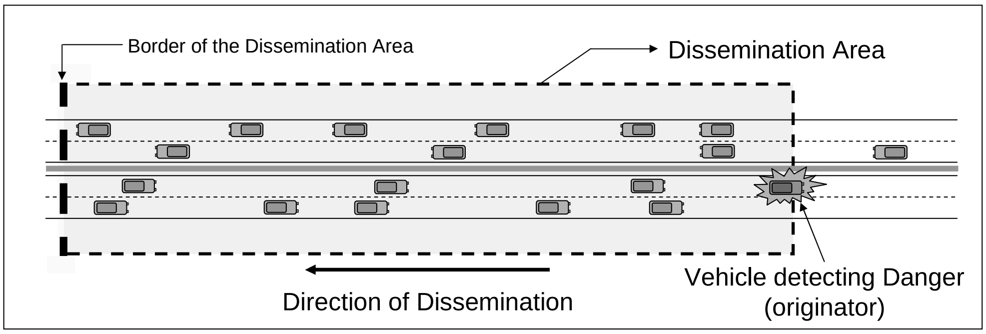


Figure 5.5: Relevant area for dissemination of emergency information after an accident detection in a highway. Vehicles in the opposite direction are included in the dissemination area since they can support the dissemination process.

The main purpose of our dissemination strategy is to select the appropriate nodes to forward the message in the direction of dissemination in order to cover the entire dissemination area. The proposed strategy needs to overcome the challenges existing in a vehicular environment, such as dealing with uncertainties resulting from node mobility, fading phenomena and packet collisions. Furthermore, since the same channel is utilized also for periodic beacon exchange, a relatively busy media can be encountered by event-driven emergency messages in dense vehicular traffic situations.

5.3.2 The EMDV protocol

In previous studies, [TMSEFH06] and [TM07], we showed the satisfactory performance of a forwarding strategy based on the use of the geographical positions of the nodes combined with a contention-based approach. According to this strategy, an event-driven message is transmitted in a broadcast fashion, and all vehicles receiving it are potential forwarders. In order to decide which node actually forwards the message, a contention period is started at each potential forwarder. The length of the contention period is different at each node and inversely proportional to the progressed distance in the direction of dissemination with respect to the actual sender. The advantages of using a contention-based approach for forwarding is that, when compared to unicast-based forwarding, the probability that at least one node receives and, thus, forwards the message is significantly increased.

Additionally, in Chapter 3 we observed how the distances from the sender to where a broadcast message is received with high probability are significantly shorter than the configured communication range, due to the hidden terminal problem and the probabilistic characteristics of radio wave propagation.

Motivated by the idealistic environments assumed to design current forwarding strategies and by the findings of Chapter 3 and [TMSEFH06], we propose the EMDV (Emergency Message Dissemination for Vehicular environments) strategy for dissemination of safety critical information. EMDV is based on the following three design principles:

i) a contention scheme is used after the broadcast transmission of the message in order to deal with uncertainties in terms of reception failure caused by node mobility, channel fading and collisions;

ii) to minimize the delay, the contention strategy is complemented with the selection of one specific forwarder made at transmission time. This is possible due to the status information acquired from safety beacons. The selected node forwards the emergency message immediately in case it is successfully received;

iii) the reliability of the dissemination process is increased by *a)* assuming a forwarding range shorter than the communication range, and *b)* a controlled message retransmission scheme within the dissemination area.

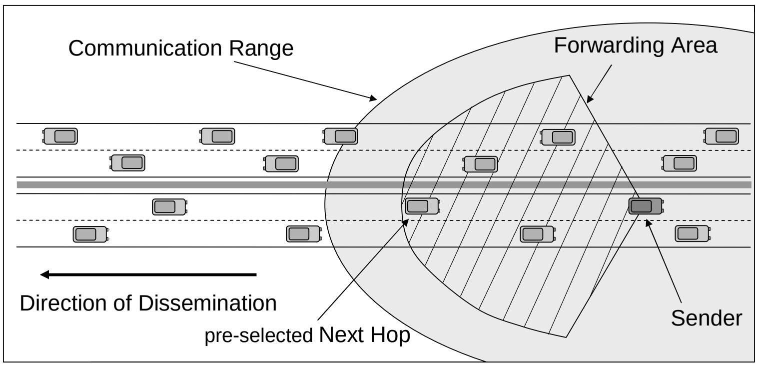


Figure 5.6: Illustration of the sender perspective when utilizing the EMDV protocol.

To satisfy principle *iii)* we restrict the area within the communication range where potential next forwarders may reside, see Figure 5.6. The forwarding area lies in the direction of dissemination and is limited by the *forwarding range*, which must be adjusted according to the probability of reception of one-hop broadcast message in order to increase the reliability of the dissemination scheme.

A pseudo-code description of the protocol is presented in Figure 5.7. Before providing the details, we define the main abbreviations and variables used in the figure for ease of presentation:

- *countMessages*: counter for messages of a specific emergency dissemination process.
- *maxMessages*: maximum amount of message repetitions allowed per node for a specific emergency dissemination process.
- *messageDestinationAddress*: node address of the sender's pre-selected next hop.
- *flag*: indicator to differentiate if the contention is initiated by the reception or the transmission of an emergency message.
- *borderDA*: location on the highway where the dissemination area ends.
- *myFA*: own forwarding area of a node.
- *myNeighborTable*: structure that maintains the positions of the neighboring nodes with the information received in the beacon messages.
- *neighbor*: entry of *myNeighborTable* that contains the most recent position of a specific node, i.e., *neighborPosition*.
- *neighborProgress*: the progressed distance towards destination (*borderDA*) offered by a specific neighbor with respect to a node's own position.
- *senderPosition*: position of the node that sent the emergency message.
- *senderFA*: forwarding area of the node that sent the emergency message.
- *contending*: boolean variable that is *true* when a node is contending to send an emergency message, and *false* otherwise.
- *myPosition*: own node's position.
- *maxContentionTime*: maximum time that a node can contend, i.e., if its distance to the message's sender is equal to *forwardingRange*.
- *maxChannelAccessTime*: expected maximum channel access time that an emergency message can experience.
- *myProgress*: the progressed distance towards destination (*borderDA*) offered by a node with respect to the message's sender.

```
Procedure: PrepareMessage( )
    if countMessages < maxMessages then
      messageDestinationAddress ← FindNextHop( )
      TransmitEMDVMessage( messageDestinationAddress )
      countMessages ++
      PrepareContention( flag = transmission )

Procedure: FindNextHop( )
    address ← broadcastAddress
    if borderDA ∈ myFA then
      return address
    progress ← 0
    for each neighbor ∈ myNeighborTable do
      if neighborPosition ∈ myFA and neighborProgress > progress then
        progress ← neighborProgress
        address ← neighborAddress
    return address

Procedure: ReceiveMessage( )
    if myPosition ∈ disseminationArea then
      if senderPosition ∈ myFA or borderDA ∈ myFA∩senderFA then
        countMessages ++
      if countMessages ⩾ maxMessages then
        CancelContention( )
      else if messageDestinationAddress = myAddress then
        if contending then
          CancelContention( )
        PrepareMessage( )
      else if myPosition ∈ senderFA and not contending then
        PrepareContention( flag = reception )

Procedure: PrepareContention( flag )
    if flag = transmission then
      time ← maxContentionTime + maxChannelAccessTime
    else time ← maxContentionTime×(1−myProgress/forwardingRange)
    contending ← true
    Contend( time )
```

Figure 5.7: The EMDV protocol as pseudo-code for emergency message dissemination.

EMDV is composed of four main procedures. A node transmitting an emergency message invokes the *PrepareMessage()* procedure. This procedure first checks whether the message has already been transmitted for the maximum number of times (*maxMessages*) within the node's forwarding area FA. If not, the *FindNextHop()* procedure is invoked to determine the message's destination node. Note that this address is used only for (possibly) selecting a specific forwarder and speed-up message propagation, but the message sent to the channel still has the broadcast address specified at link layer. This ensures that every node which receives an emergency message passes it to the upper layers, and that no acknowledgment is issued for a received message. Once the message has been transmitted, the message counter is increased, and a contention period is started to verify that at least one neighbor is forwarding the message. Procedure *FindNextHop()* essentially scans the neighbor table of the sender in order to find (if any) the neighbor in the sender's forwarding area with the highest progress in the direction of dissemination within the node's forwarding area. If no neighbor in the dissemination direction can be found, or if the sender's forwarding area is at the border of the dissemination area (see Figure 5.5), no specific forwarder is selected, and *messageDestinationAddress* is set to *broadcastAddress*.

Procedure *ReceiveMessage()* is invoked when a node receives an emergency message. It first ensures that the node lies inside the dissemination area before proceeding further. Then, it is checked whether the received message has been sent by a node which is further away in the direction of dissemination and lies inside the own FA. In this case, the message can be considered as a sort of 'implicit ack' of message forwarding and the corresponding message counter is increased so that contention for forwarding the message can be canceled if enough 'implicit acks' have already been received. If the above conditions are not satisfied, the dissemination criteria is used to determine whether forwarding is needed: if the receiving node's address corresponds with the *messageDestinationAddress* field, then the message is forwarded with no contention by invoking procedure *PrepareMessage()*; otherwise, a contention period is started by invoking the *PrepareContention()* procedure.

Finally, the protocol has to be adjusted with respect to two specific situations. First, the contention period started after delivering the message to lower layers (*PrepareMessage()*) must take into account the time that the message needs to access the channel and to be transmitted. For this purpose, the contention time is set to *maxContentionTime* + *maxChannelAccessTime* when the variable *flag* is set to *sent*. Second, nodes located within *forwardingRange* from the border of the *disseminationArea* should act differently than other nodes since the message must not travel further than *borderDA*. Therefore: *a)* they do not select a neighbor as *next hop*, instead the *broadcastAddress* is utilized; and *b)* they increment *countMessages* when receiving a message from any node that is also located within *forwardingRange* of *borderDA*, instead of only counting the ones coming from their *forwardingArea*.

In this thesis, we study the performance of the protocol in challenging saturation conditions. However, EMDV can easily be adapted to perform well also in sparse network situations. For instance, cases when no vehicle is known in the direction of dissemination can be easily addressed either by storing the emergency message and issuing it when a beacon from a new vehicle is received, or by repeating the EMDV contention until a predefined lifetime timer expires.

6
Evaluation of D-FPAV and EMDV Protocols

In the previous chapter, we have proposed a distributed transmission power control strategy called D-FPAV (Distributed Fair Power Assignment for Vehicular environments) that controls the beaconing load on the channel. D-FPAV operates under a strict fairness criterion which has to be met for safety reasons and also allows a clear prioritization of event-driven over periodic messages. Additionally, we described a strategy called EMDV (Emergency Message Dissemination for Vehicular environments) proposed to ensure a fast and effective dissemination of alerts in a target geographical area.

In this chapter, we make use of the extended version of the network simulator ns-2.28 described in Chapter 3 to evaluate the performance of D-FPAV and EMDV, and show how they achieve their design goals.

First, we study the different design options of D-FPAV outlined in Chapter 5 for acquiring the status information of surrounding nodes and identify the most appropriate one to achieve its purpose. Then, we show the ability of D-FPAV to control the beaconing load on the channel and its effect on the reception rates of both beacon and event-driven messages. A controlled load on the channel achieved by D-FPAV ensures high beacon reception rates at close distances from the transmitter, as specified by the safety design goals in Chapter 4.3.

Additionally, we analyze the dissemination delay and success ratio of emergency information achieved with EMDV. We show that EMDV is a robust protocol for dissemination of emergency information with a low delay in a wireless channel with heavy load. Furthermore, we show the synergetic performance achieved when combining both protocols. EMDV efficiently disseminates emergency information when the beaconing load is controlled by D-FPAV, being capable to achieve a 100% of delivery ratio in a highway segment.

Before presenting the results obtained, we describe the simulation setup, including the scenario utilized, and the communication strategies' configuration.

6.1 Simulation setup

The evaluated vehicular scenario is configured according to the parameters presented in Chapter 2.3 and the values derived in Chapter 3.4. We simulate a 6 km long bidirectional highway with 3 lanes per direction. The selected case for this study consists of an average density of 11 vehicles per kilometer in each lane driving at an average speed of 121.86 km/h, what corresponds to a 'heavy' free-flow fast-moving German highway traffic. As in Chapter 3, we utilize free flow vehicular traffic scenarios due to our interest in highly dynamic environments where high transmission power values and packet generation rates are envisioned. Note though, that the amount of messages sent to the channel could be much higher in many situations, e.g., highways near big cities or temporary working areas. Figure 6.1 illustrates a 12 km long scenario (HWGui tool [HWG]) from which one of our segments was extracted for this analysis.

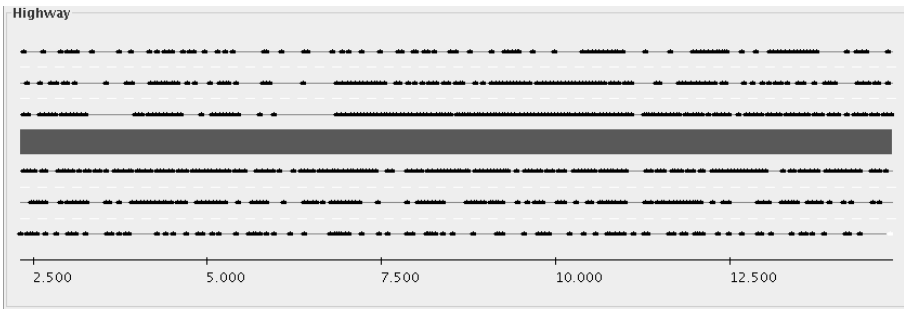


Figure 6.1: Screen-shot of the HWGui tool [FTMK$^+$06] corresponding to a utilized highway scenario, with 3 lanes per direction and 11 nodes per kilometer in each lane.

All vehicles are equipped with wireless communication interfaces and generate 10 beacons per second with a size of 500 Bytes. According to the results obtained in Chapter 3.4, we utilize a data rate of 3 Mbps due to its robustness and set the contention window value to 31. The rest of MAC and PHY layer values are configured according to the parameters defined in Chapter 3.2.3. The communication range for beacon messages is initially configured to 1000 m, what corresponds to the P_{max} in our setup. The corresponding transmission power to achieve a communication range of 1000 m is 9.95 dBm with our models configuration and a data rate of 3 Mbps.

Additionally, the reference node, or originator, generates event-driven messages destined to a dissemination area that comprises a segment of the highway starting at its position and going up to two kilometers opposite to the driving direction. The reference node, as in Chapter 3, is a node located around the kilometer 4 of our highway segment and, accordingly, the 2 km long dissemination area is located in the middle of the 6 km scenario. All event-driven messages, independently if D-FPAV is used or not, are sent with a CR = 1000 m. Also, event-driven messages are configured with a higher link-layer priority than beacons. We make use of differentiated access categories (EDCA mechanism described in IEEE 802.11e [11e]) as configured in Chapter 3.4.4.

With respect to the communication strategies, we set the maximum beaconing load (MBL) of D-FPAV to two different values, 2.5 Mbps and 2 Mbps, in order to evaluate the prioritization of event-driven messages over beacons. We fix each neighbor entry to 15 Bytes, corresponding to vehicle identifier and position. Finally, a node deletes neighbor entries from their neighbor table that are older than 1 second.

With respect to EMDV, we fix the *maxContentionTime* to 100 ms and the *maxChannelAccessTime* to 10 ms as appropriate values for our scenario according to the results obtained in Chapter 3.4.4. The forwarding range is configured to three different values, 300 m, 500 m and 700 m, in order to study the trade-off between reliability, overhead and delay. Last, we study the performance of three different values for the amount of retransmissions (*maxMessages*) in a node's *forwardingArea*, namely 1, 2 and 3.

In order to obtain statistical significance we simulate ten different highway scenarios, with the same average vehicle density, with ten random seeds for every selected configuration. Each simulation consists of 11 s of simulated time where the reference node initiates 10 emergency information dissemination processes. The time between two consecutive event-driven processes is 1 s. The statistics corresponding to the first second of simulation are not taken into account as transitory state. Last, the results obtained are represented with a 95% confidence interval.

The configuration details are summarized in Table 6.1.

6.2 Simulation results

In the following, we present the simulation results obtained in order to evaluate D-FPAV and EMDV performance. First, we discuss the five D-FPAV options to exchange the surrounding vehicle's status information outlined in Chapter 5.2. Then, we analyze the performance of D-FPAV in terms of reception probability and channel access time of beacons and event-driven messages.

Additionally, we study the delivery ratio and delay obtained by the EMDV protocol when used to disseminate emergency information within the selected highway segment. Last, we evaluate the prioritizing effect that two different values of the MBL parameter have on the EMDV performance.

PARAMETER	VALUE
Number of lanes	3 × direction
Vehicle density	11 cars/km per lane
Average speed	121.86 km/h
Propagation model	Nakagami m = 3
802.11p data rate	3 Mbps
Contention window	31
Packet size	500 Bytes
Communication range: Event-driven messages Beacons (without D-FPAV)	 1000 m 1000 m
Beacon generation rate	10 packets/s
D-FPAV	On, Off
D-FPAV *MBL*	2.5 Mbps, 2.0 Mbps
Neighbor entry size	15 Bytes
Dissemination area length	2 km
EMDV *forwardingRange*	300 m, 500 m, 700 m
EMDV *maxMessages*	1, 2, 3
EMDV *maxContentionTime*	100 ms
EMDV *maxChannelAccessTime*	10 ms

Table 6.1: Configuration parameters for D-FPAV and EMDV evaluation.

6.2.1 D-FPAV's performance

In order to evaluate D-FPAV performance we configure two main setups, D-FPAV On and D-FPAV Off. In D-FPAV Off simulations, all beacons are sent at maximum power (CR = 1000 m) since no power control is applied. On the other hand, for D-FPAV On, beacons are sent at the transmit power computed by D-FPAV. In this section, we fix the maximum beaconing load (MBL) to 2.5 Mbps.

The main metrics analyzed to evaluate D-FPAV's performance are: i) the probability of successful reception of a beacon message with respect to the distance, and ii) the average Channel Access Time (CAT). For a definition of these two metrics, please see Chapter 3.3. The CAT is computed for all nodes in the highway and it is used to corroborate the claim that D-FPAV reduces the load on the channel uniformly in the network, i.e., it achieves fairness. The probability of reception is used to assess D-FPAV's effectiveness and the appropriate prioritization of safety-related messages (design goals stated in Chapter 4.3), which is obtained by ensuring a high probability of correctly receiving beacons at close distances from the sender and, at the same time, increase the probability of successful reception of event-driven messages at all distances.

First, we asses the D-FPAV strategies to obtain the status information from vehicles driving inside a node's carrier sense range (CS) described in Chapter 5.2.4.

Figure 6.2 presents the probability of successful reception of beacons for the different strategies as well as with D-FPAV Off for comparison. These strategies are differentiated by the generation rate of the extended beacons and the power used to transmit them. Extended beacons are messages that contain not only the status information of the transmitter, but also the information from its surrounding nodes.

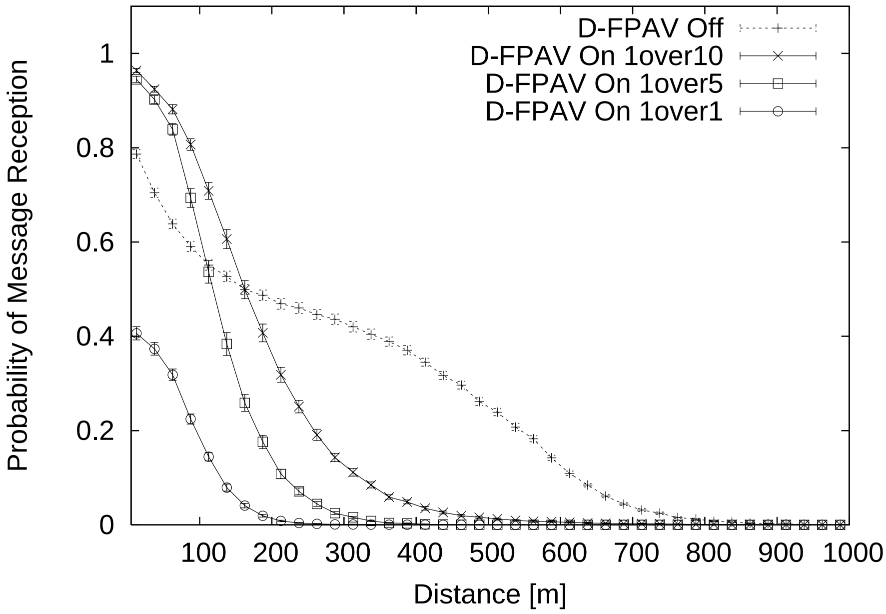
Figure 6.2(a) shows the results obtained by the strategies which extended beacons are sent with the power computed by the D-FPAV protocol. Figure 6.2(b) shows the results of the strategies where extended beacons are sent with full power P_{max}. As described in Chapter 3.4.3 (see Figure 3.10), the reception rates with D-FPAV Off present low reception rates due to the high load existing on the wireless medium and the resulting packet collisions. With a high saturation on the wireless medium the major cause of packet reception failure is packet collisions, what causes the low reception rates at all distances, e.g., below 50% for nodes located located at 200 m and further. As described in Chapter 3.2.2, the near-far effect of radio wave propagation allows higher reception rates at very close distances from the transmitter, i.e., 80% at few meters, and causes the strong decrease up to 150 m.

Adjusting the transmission power of all beacons, including the extended ones, can achieve the result expected (Figure 6.2(a)): an increased probability of reception at close distances from the sender for 1over5 and 1over10. However, an unfavorable result is obtained with 1over1 due to the high overhead corresponding to extending all beacons with the status information of the surrounding nodes.

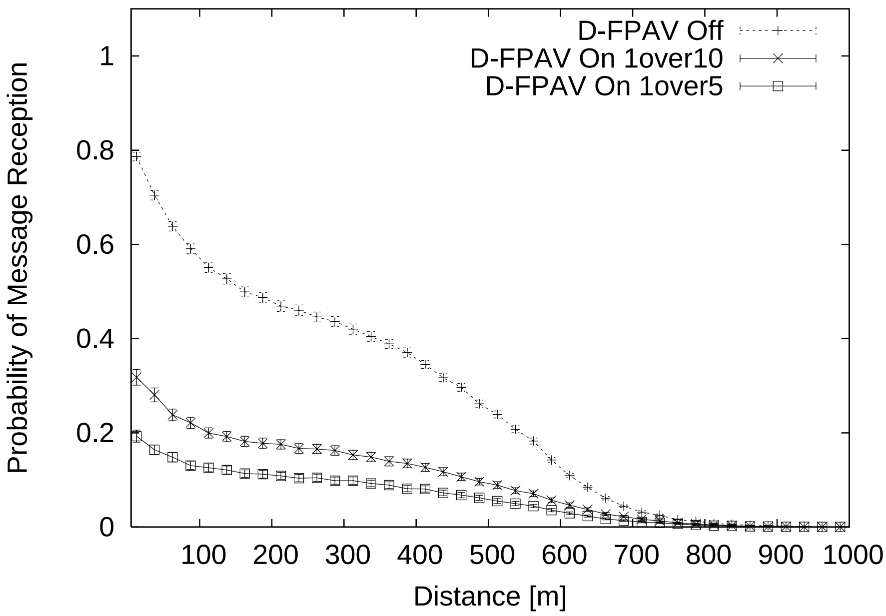
Comparing the 1over10 and 1over5 curves in Figure 6.2(a), we can see how sending a lower number of extended beacons achieves higher reception rates. Note the existing trade-off between information accuracy and message collisions caused by the associated overhead of D-FPAV. Sending a higher amount of extended beacons offers the possibility to obtain more up-to-date information about the status information from surrounding nodes (further than direct communication distances). Indeed, the average amount of entries in the neighbor table, what corresponds to nodes located within the CS_{MAX}, is higher in the case of 1over5 than in the case of 1over10. However, the additional load, i.e., larger size, of these beacons causes a higher amount of collisions from close nodes, what is critical for the detection of dangerous road situations. Note that extended beacons are significantly larger than non extended ones. The average size of extended beacons is, e.g., 2770 Bytes[1] in case of 1over5, what corresponds to the status information from 151.3 neighbors. In case of 1over10, the obtained results show an average extended beacon size of 2391 Bytes, what corresponds to 126.0 neighbors' information.

On the other hand, sending extended beacons with P_{max} does not help improving the probability of successfully receiving messages at close distances, see Figure 6.2(b). Reducing the transmission power of 80%, or 90%, of the beacons and transmitting the other 20%, or a 10%, with extended information and full

[1]The maximum MAC protocol data unit specified in the IEEE 802.11p draft is 4095 Bytes.



(a) Extended beacons transmitted with adjusted power.



(b) Extended beacons transmitted with P_{max}.

Figure 6.2: Probability of successful beacon reception with respect to the distance for different options of the D-FPAV protocol to obtain the status of the surrounding vehicles.

power decreases the probability of beacon reception at all distances with respect to no power adjustment. Both 1over5 and 1over10 curves in Figure 6.2(b) present lower reception rates than D-FPAV Off.

Note that the D-FPAV On curves in Figure 6.2(b) show higher reception rates for far distances, e.g., from 300 m to 600 m, than the ones in Figure 6.2(a) due to the higher power utilized by the extended beacons. However, as outlined above, the reception rates at close distances are dramatically decreased, contrary to the main goal of this strategy.

Therefore, we conclude that sending one extended beacon every 10 transmissions with adjusted power presents the best trade-off between accuracy and overhead among the studied options. Note that due to the high amount of nodes within the communication range of each other, the same information is repeated by several nodes. Thus, extending one beacon of every 10 provides enough accuracy of the neighbor table at a lower price than 1over5 in terms of overhead. In the following, we study the performance of 1over10 D-FPAV strategy in more detail.

Figure 6.3 presents the probability of successful packet reception with respect to the distance of beacons and single-hop event-driven messages for D-FPAV On and Off. As outlined above, not using power adjustment results in a high load experienced on the channel which, in turn, causes a high amount of packet collisions and low reception rates. Note that if beacons and event-driven messages are sent with the same transmission power (D-FPAV Off), event-driven messages achieve higher reception rates at closer distances. As explained in Chapter 3.4.4, a prioritized channel access category decreases the probability to experience collisions with neighboring nodes.

Using the D-FPAV mechanism and setting the maximum beaconing load (MBL parameter) to 2.5 Mbps results in an average reduction of the beacon's transmission power from 9.95 dBm to -1.34 dBm, which decreases their communication range from 1000 m to an average of 491 m. Therefore, the CS range is reduced to 551 m what, according to an average of 66 cars/km in each lane, corresponds to an average of 72.7 vehicles within the CS. Note that 72.7 vehicles correspond to an offered load of 2.9 Mbps. A higher offered load than the fixed MBL (2.5 Mbps) is experienced due to the missing nodes on the neighbor table commented above, i.e., lack of accuracy.

In order to evaluate the saturation on the channel we also computed the average channel busy time ratio. As intended, the reduction of the transmission power decreases the average channel busy time ratio experienced by all nodes in the highway, from about 86.6% with D-FPAV Off to 78.5% with D-FPAV On, a 9.3% decrease.

The resulting power adjustment allows D-FPAV to fulfill its design goal of ensuring high message reception rates at close distances from the sender, corresponding to the safety distance of a vehicle[2]. As outlined in Section 4.3, achieving

[2]As described in Chapter 4, the safety distance of a vehicle driving at 120 km/h has a safety distance of approximately 60m.

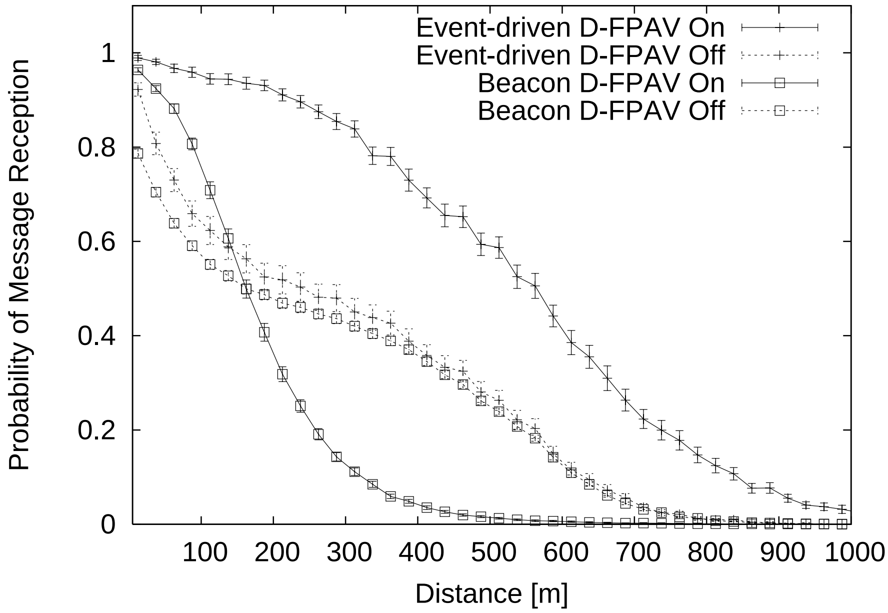
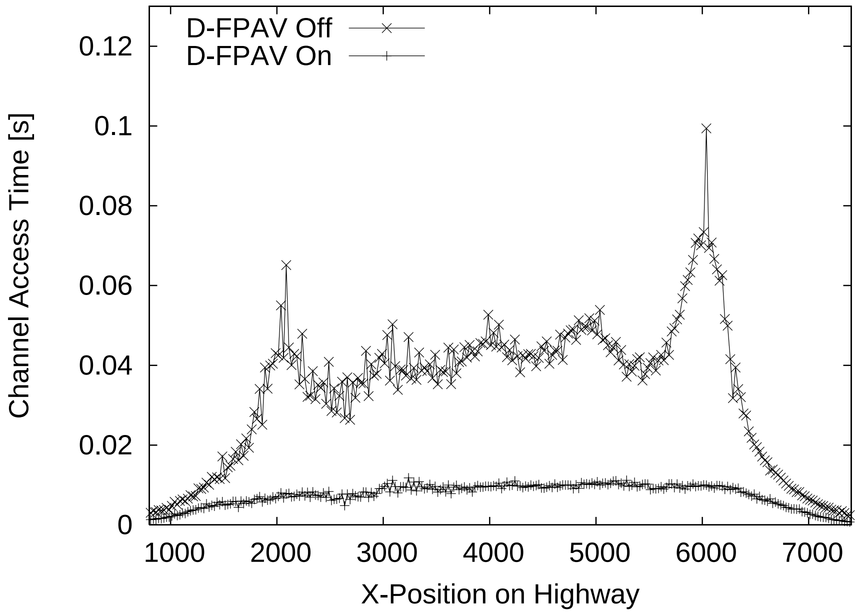


Figure 6.3: Probability of successful reception of beacons and one hop event-driven messages (without retransmission) with respect to the distance to the transmitter, with D-FPAV On/Off and MBL = 2.5 Mbps.

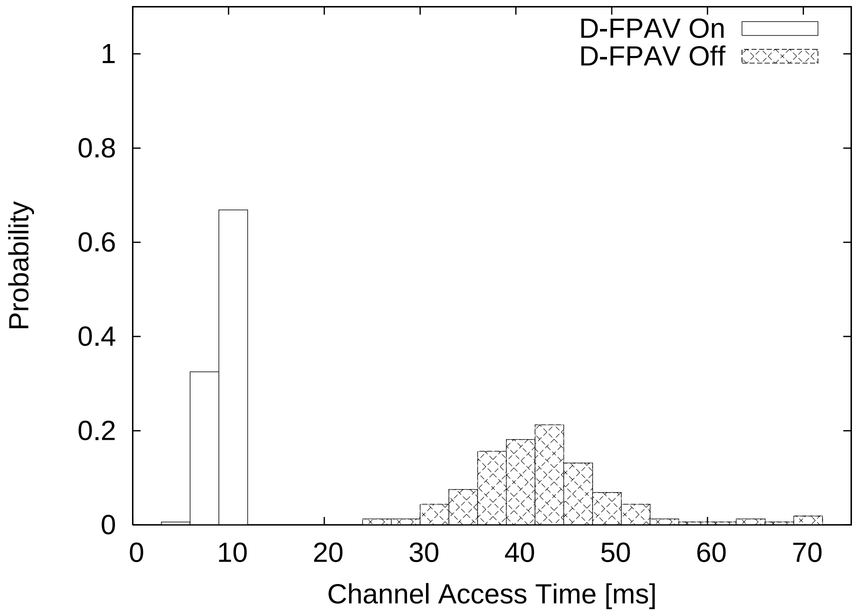
a good estimation of the close environment is critical in order to identify dangerous situations. In our scenario, beacons' probability of successful reception presents higher values up to distances of 160 m with D-FPAV On, e.g., an increase of 33% at 100 m (from 56.8% with D-FPAV Off to 75.6% with D-FPAV On). Additionally, we can observe a significant increase of the reception rates experienced by each transmission of an event-driven message at all distances with D-FPAV On. Experiencing a lower load on the medium allows event-driven messages, which are not restricted in terms of transmission power, to achieve improved reception rates not only at close distances (e.g., a 48.6% increase at 100 m, from 64.0% to 95.1%) but also at further ones (e.g., 117.7% increase at 500 m, from 27.1% to 59.0%). The price to pay for these improvements is the lower reception rates of beacons for distances further than the 160 m, which, however, are distances where the information conveyed by beacons is less relevant compared to the 'closer beacons' and emergency messages.

In order to evaluate the fairness of the algorithm we illustrate in Figure 6.4(a) the average channel access time experienced by all nodes in the highway. We represent each vehicle with their middle position[3] during the simulation run. In this case, the results of only one scenario are presented not to average out different vehicular densities in different segments of our highway. We can observe how the

[3] As in Chapter 3, we compute the middle position of a vehicle as the middle point between its position at the beginning of the simulation and its position at the end.



(a) Average channel access time experienced by each node with respect to its position on the highway.



(b) Probability of experiencing a channel access time.

Figure 6.4: Average channel access time experienced by beacons with and without D-FPAV and an MBL = 2.5 Mbps.

average channel access time has been reduced from an average of 39.8 ms to a 10.3 ms when using D-FPAV.

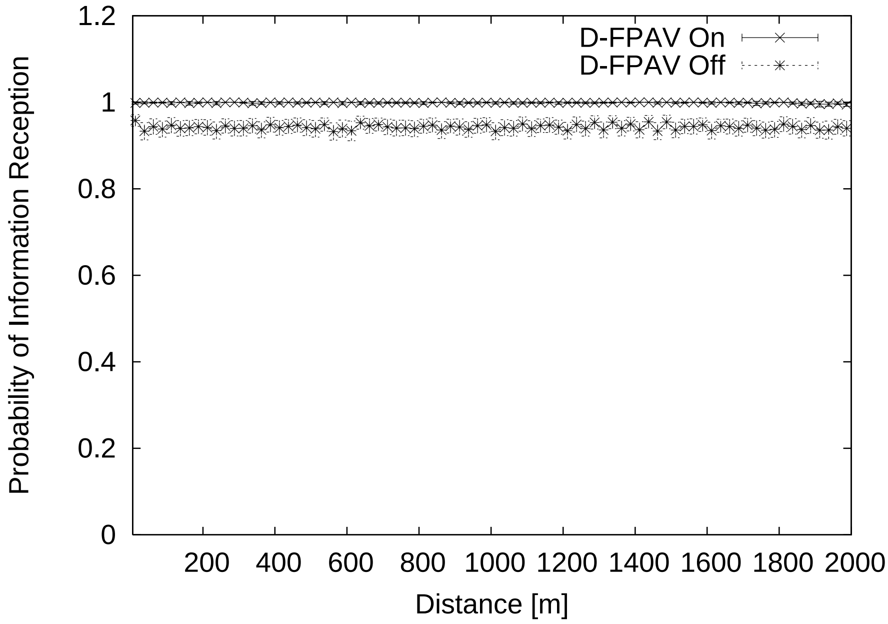
Furthermore, if no power control is applied, nodes can experience considerably different values of CAT, ranging from about 24 ms to 69 ms, see Figure 6.4(b). Taking into account that the CAT obtained reflects the amount of load on the channel at that particular location, the results obtained with D-FPAV Off show that different nodes have different opportunities of sending and correctly receiving messages, impairing fairness. Even worse, nodes traveling in denser areas, where the likelihood of having an accident is higher, experience a higher CAT, which results in a longer expected delay in propagating event-driven messages. On the other hand, when D-FPAV is active all the nodes experience similar CAT values than their neighbors, ranging between 3 ms and 9 ms. Therefore, similar opportunities of sending and correctly receiving safety messages are experienced by the nodes in the network. In other words, D-FPAV achieves its design goal of fairness.

6.2.2 EMDV's performance

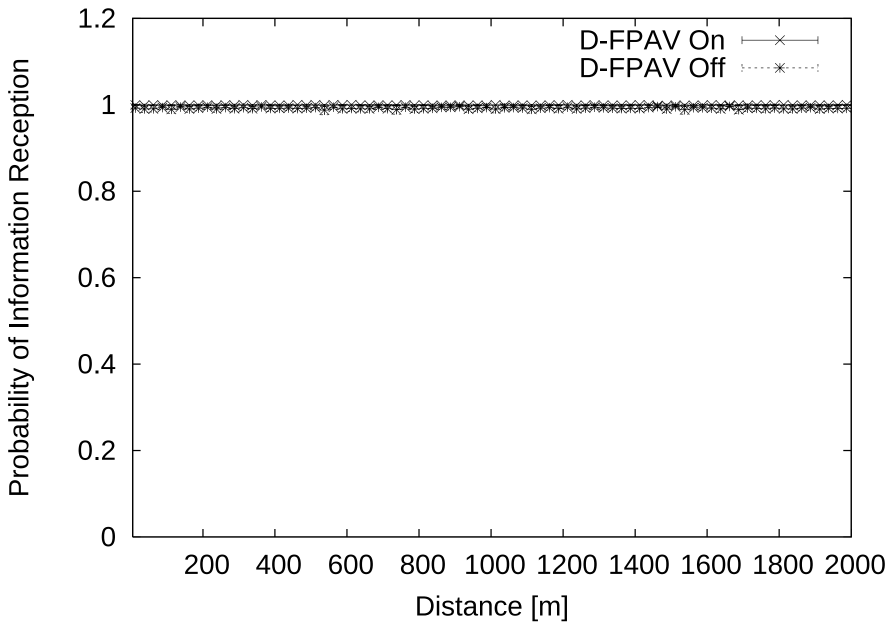
In this section, we evaluate the performance of the EMDV protocol when operating with D-FPAV Off as well as in synergy with the D-FPAV protocol. In our scenario, the reference node generates an emergency message that has to be delivered within the relevant area for dissemination. In our case, the dissemination area is 2 km long and lays in the middle of our highway segment. Additionally, three different values of the *maxMessages* parameter are studied (1, 2 and 3), as well as three values of the *forwardingRange* (300 m, 500 m and 700 m). Unless otherwise stated, the utilized *forwardingRange* will be the middle value, 500 m. Among the different options of D-FPAV, 1over10 with adjusted transmission power is used due to the results obtained in Section 6.2.1.

Figure 6.5(a) presents the probability that the emergency information is successfully received by vehicles located inside the dissemination area and with *maxMessages* = 1. With D-FPAV Off, we observe a reception rate of 94.2% averaged over the dissemination area. The use of the D-FPAV protocol increases the emergency information reception rates up to an average of 99.9%. The result shows the dependency of the success of the dissemination strategy on the channel load conditions.

Figure 6.5(b) shows the probability of reception in the dissemination area obtained when setting *maxMessages* = 2. Note how the curve presenting the reception rates obtained with D-FPAV Off is increased with respect to the values observed in Figure 6.5(a) when *maxMessages* = 1, i.e., from 94.2% to a 99.2% in average. In order to achieve a 100% probability of reception within the dissemination area *maxMessages* must be set to 3 repetitions, see Table 6.2. As intended, allowing more message repetitions within a node's *forwardingRange* enhances the reliability of the protocol at the cost of an increased overhead.



(a) maxMessages = 1.



(b) maxMessages = 2.

Figure 6.5: Probability of information delivery inside the dissemination area with respect to the distance from the message originator (with multi-hop retransmissions) with D-FPAV On/Off and MBL = 2.5 Mbps.

In Table 6.2, we present the average amount of retransmissions caused by the EMDV protocol, i.e., the amount of times that the emergency message is transmitted by any node within the dissemination area. Observe how with D-FPAV Off increasing *maxMessages* from 1 to 2 causes the emergency message to increase from 66.2 to 107.6 repetitions per dissemination process, and to 135.9 in case of allowing 3 repetitions.

maxMessages	**1**		**2**		**3**	
D-FPAV	**Off**	**On**	**Off**	**On**	**Off**	**On**
Prob. reception	94.2%	99.9%	99.2%	99.9%	100%	100%
Retransmissions	66.2	26.1	107.6	41.5	135.9	53.7

Table 6.2: Averages of the probability of reception, the maximum delay and the amount of retransmissions experienced within the dissemination area with a *forwardingRange* = 500 m and for three values of *maxMessages*, 1, 2 and 3.

When using D-FPAV the most efficient EMDV choice is to configure *maxMessages* = 1 since it reaches a 99.9% delivery rate utilizing less messages in average than with *maxMessages* = 2 and 3, i.e., 15.4 and 27.7 messages less than configuring *maxMessages* to 2 and 3 respectively. However, it is the responsibility of the application designer to define the requirements for communication protocols, i.e., *maxMessages* 3 may be preferred due to the 100% reception rates achieved.

Furthermore, we analyzed the effect that event-driven messages have on beacon reception rates during the complete simulation. Figure 6.6 presents the probability of successful reception of beacons sent by the reference node for the three values of *maxMessages* as well as for the case where no EMDV process is started, always with D-FPAV On. The obtained values do not show a significant impact of the different amount of event-driven messages sent to the channel. For example, the probability of successful reception at 100 m from the sender decreases a 1.7% in case information dissemination processes with *maxMessages* = 1 are started, presenting a 75.6% of probability of reception without EMDV processes and a 74.3% otherwise. In turn, when increasing *maxMessages* to 2 and 3, the resulting reception rates present also a small decrease, obtaining a 73.2% and 72.1% respectively. Moreover, the difference between the curves is negligible for further distances than 200 m.

In the rest of the chapter we focus on the performance of *maxMessages* = 1, which provides a 99.9% of delivery ratio with D-FPAV On and utilizes the least amount of overhead.

Figure 6.7 shows the average delay experienced by the nodes in the dissemination area[4] until receiving the emergency information with respect to the distance to the originator. Both curves present higher values for increasing distances, as

[4]Only the set of vehicles that receive the emergency message can be taken into account.

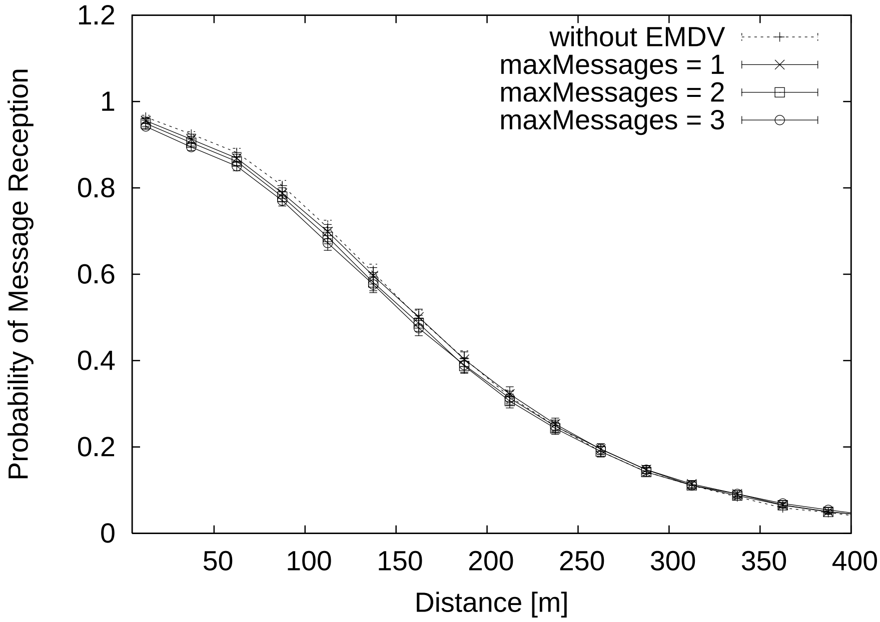


Figure 6.6: Probability of successful reception of beacons with respect to the distance, with D-FPAV On, MBL = 2.5 Mbps and while disseminating emergency information for three values of *maxMessages*, 1, 2 and 3.

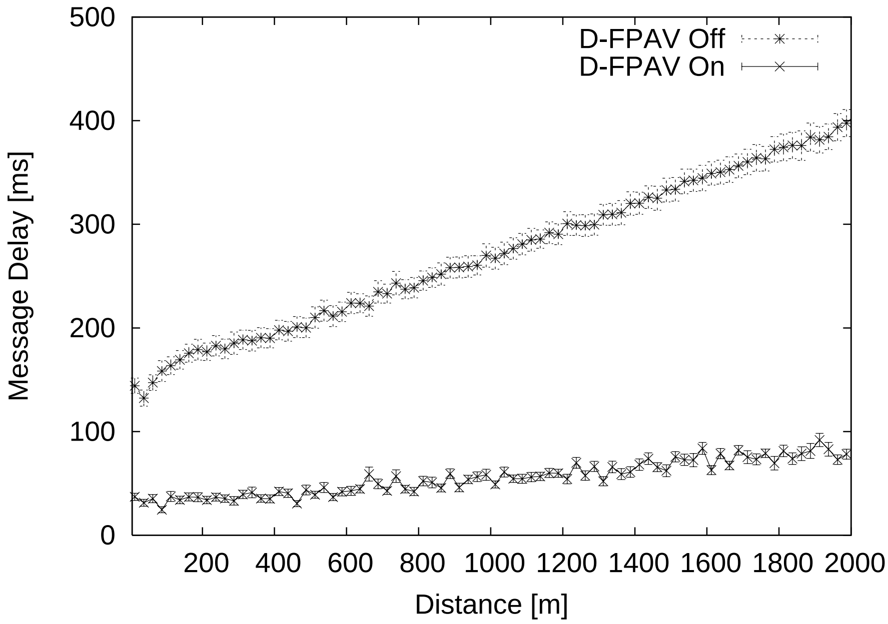


Figure 6.7: Reception delay of the emergency information inside the dissemination area with respect to the distance from the message originator (with multi-hop retransmissions) with D-FPAV On/Off and MBL = 2.5 Mbps.

expected due to the multi-hop dissemination approach. In case of D-FPAV Off, event-driven messages are disseminated up to 2 km with an average delay below 400 ms. This delay should be compared to the estimated driver reaction time, which is on the order of 700 ms and higher [OS86]. Furthermore, in case D-FPAV is utilized, the delay experienced falls significantly: from 144 ms to 37 ms for close distances to the sender and from 397 ms to 78 ms in case of a vehicle located 2 km away from the originator.

Another relevant parameter for safety is the *maximum* delay experienced by the information to be delivered. To account for this, we measured the maximum time of all simulated scenarios that a node located at 2 km of the originator, i.e., at the other edge of the relevant area, has to wait until receiving the emergency information. According to the results obtained, the maximum delay experienced in case of D-FPAV Off is 1224 ms, whereas in case of D-FPAV On it is reduced to 689 ms. Note a difference of 535 ms between both cases, which is a significant value when compared to the driver reaction time mentioned above.

Finally, we study the performance results obtained with a *forwardingRange* of 300 and 700 m. Setting a smaller range forces shorter hops, i.e., shorter distances between two consecutive forwarders, in the direction of dissemination. Accordingly, a smaller range causes a higher amount of message retransmissions, see Table 6.3.

forwardingRange	**300 m**		**500 m**		**700 m**	
D-FPAV	**Off**	**On**	**Off**	**On**	**Off**	**On**
Prob. reception	91.7%	99.8%	94.2%	99.9%	93.6%	99.6%
Avg. delay at 2 km	552 ms	100 ms	397 ms	78 ms	405 ms	77 ms
Retransmissions	77.4	27.8	66.2	26.0	63.1	20.3

Table 6.3: Averages of the probability of reception, the maximum delay and the amount of retransmissions experienced within the dissemination area for three values of the *forwardingRange*, 300 m, 500 m and 700 m.

Let us focus on the values obtained with D-FPAV Off first. We can observe that increasing the *forwardingRange* from 300 m to 500 m enhances the dissemination reliability, i.e., the probability of reception within the dissemination area increases from 91.7% to 94.2%. Note that increasing *forwardingRange* also increases the amount of potential next forwarders along the dissemination process. Furthermore, utilizing a *forwardingRange* = 500 m results in a shorter average delay at 2 km distance, 397 ms instead of 552 ms, and a smaller amount of overhead generated, 66.2 instead of 77.4 retransmissions.

On the other hand, configuring the *forwardingRange* to 700 m does not present a clear advantage for safety with respect to the 500 m case. Although the amount of retransmissions generated are lower, 63.1 instead of 66.2, extending the *forwardingRange* from 500 m to 700 m presents higher values for the average delay at 2 km (8 ms more) and slightly lower reliability (it decreases a 0.6%). The reason for a lower dissemination reliability with a 700 m *forwardingRange* are the low one-hop reception rates experienced at these distances from a transmitter, see the 'Event-driven D-FPAV On' curve in Figure 6.3.

When D-FPAV is active, the observations outlined above are also valid. Increasing the *forwardingRange* from 300 m to 500 m results in lower values for the average delay at 2 km from the sender (100 ms and 78 ms respectively) as well as for the message retransmissions (27.8 and 26.0 respectively). Moreover, the higher amount of messages do not result on a higher reliability. Further extending the *forwardingRange* to 700 m does not present an advantage, as in the case of D-FPAV Off, due to the low one-hop probability of reception of a message at these distances. Although the amount of retransmissions are lower with *forwardingRange* = 700 m than with 500 m, the probability of reception is decreased a 0.3% within the dissemination area.

6.2.3 Effect of the MBL parameter

Finally, we evaluated the prioritization effect that a different choice of the MBL value has on both types of messages and, therefore, on the performance of our protocols. We simulated the same scenario as in the previous section with an MBL set to 2 Mbps and describe the results obtained in the following. A smaller MBL value further restricts the transmission power utilized for beacons, i.e., it achieves a more strict prioritization of event-driven messages over periodic messages.

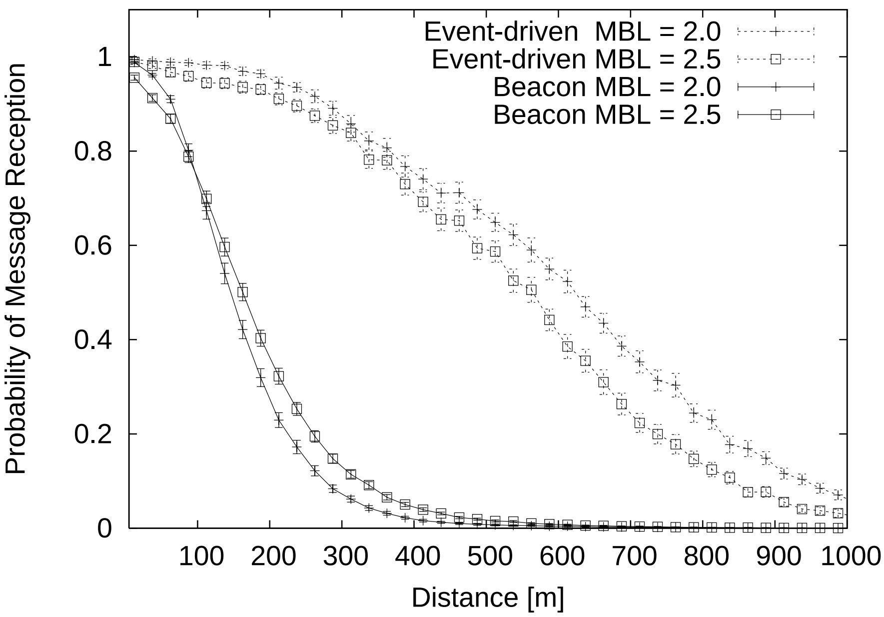


Figure 6.8: Probability of successful reception with respect to the distance of beacons and one hop event-driven messages (without retransmission) with D-FPAV On for MBL=2.0 Mbps and MBL=2.5 Mbps.

In case of configuring MBL = 2.0 Mbps (instead of 2.5 Mbps), the average transmission range of beacons is decreased down to 373 m (instead of 491 m) and the channel busy time ratio to 68.0% (instead of 78.5%). Figure 6.8 presents the effect of configuring MBL with the two selected values on the reception rates of single-hop messages. We can observe how with MBL = 2.0 Mbps event-driven messages benefit from a lower load on the medium, which increases their probability of being successfully received over the distance, e.g., achieving a 98.5% of successful receptions at 100 m and 66.2% at 500 m, instead of 95.1% and 58.9% respectively. On the contrary, beacons suffer the corresponding reduction of reception rates at distances higher than 100 m due to the lower transmission power. It is worth noting, though, that they also experience a small increase at close distances according to the lower load delivered to the wireless medium.

With a lower MBL, the EMDV protocol achieves a more efficient performance due to the lower channel load and the increased event-driven messages' reception rates. The probability of information reception with *maxMessages* = 1 and *forwardingRange* = 500 m obtains a 99.9% along the dissemination area, as with MBL = 2.5 Mbps. However, the average amount of messages sent per dissemination process with MBL = 2.0 Mbps is 18.6, i.e., 7.4 packets less than with the higher MBL value.

Furthermore, a lower load on the channel results in a smaller channel access time for event-driven messages in every hop, which results in an average delay of 39 ms to deliver the emergency information at 2 km from the information originator, half the time when compared with an MBL = 2.5 Mbps. Also, the maximum delay experienced by nodes located at the edge of the dissemination area is reduced, down to 395 ms in this case (294 ms lower than with MBL = 2.5 Mbps).

6.3 Conclusions

In this chapter, we have evaluated the performance of D-FPAV and EMDV. The selected scenario corresponds to a high speed heavy traffic German highway where all vehicles send 10 beacon messages per second. Additionally, one node starts emergency information dissemination processes.

The simulation results show how D-FPAV achieves to control the beaconing load in the wireless channel while ensuring fairness. We saw, on the one hand, how the reduced load on the channel ensures high beacon reception probability within the vehicle's safety distance. On the other hand, the channel access time experienced by all nodes in the network was reduced down to similar values in comparison to not using D-FPAV. Adjusting the beaconing load results in a fair environment where vehicles have the same opportunities of sending and correctly receiving safety messages.

With respect to EMDV, we showed how it achieves its design goal of delivering information within a geographical area in a rapid and efficient manner. EMDV is a robust strategy able to cope with received power fluctuations, node mobility and high channel load conditions. Furthermore, we saw how to adjust its parameters to favor the reliability of the dissemination process at the cost of a higher overhead.

Last, we showed that D-FPAV is a valuable mechanism to balance the trade-off between periodic and event-driven traffic. The synergistic effects can be clearly observed when combining both protocols since EMDV benefits from D-FPAV's ability to lower the channel load in terms of delay and efficiency.

7

Design Guidelines for an IVC System Architecture

Within the Network on Wheels project [NoW], one of our responsibilities was to identify the key aspects of a protocol architecture for inter-vehicle communication (IVC) systems as well as to propose design guidelines. Our main goals were to achieve a simple and modular structure, identify relevant functions for information dissemination (the main goal of IVC) and define a proper assignment of the functions to the different modules. As a result, we achieved a robust system model with low complexity as a basis for implementation, whose design process is presented in this chapter.

The main requirements for an appropriate system design must be identified according to the main purpose and characteristics of the corresponding communication protocols as well as applications. As stated in Chapter 4, a flexible information exchange scheme is required since the same information is beneficial by different protocols and entities, e.g., status information of neighboring vehicles such as their position. Additionally, a high interaction among protocols is needed to obtain the versatility required to provide a reliable and efficient information delivery, and to control transmission parameters on a per-packet basis, as outlined also in Chapter 4.

In the following, and in order to depict an appropriate protocol architecture design, we consider two potential (and extreme) approaches for IVC systems. On the one hand, following the traditional approach, the overall functionality can be de-composed and organized in layers such that protocols fulfill well-defined tasks and form a protocol stack as in TCP/IP [JP81, RFC81] and ISO/OSI [Zim80]. On the other hand, one could try to build a customized solution to meet the requirements of IVC with such a non-layered, but still modular approach. In the latter case, we are not restricted to the assignment of functions to particular layers and their limited layer interactions. In the following, we will describe both –fundamentally feasible but extremely opposite– approaches and briefly outline their advantages and disadvantages. Afterwards, having learned the benefits of both systems, we will describe a third approach emphasizing its key features that makes this protocol architecture be better suited for an IVC system.

Additionally to the protocol architecture of a communication technology, the assignment of responsibilities to its different layers is a relevant task. Indeed, it is a key aspect for communication systems developers as well as for application designers to have their responsibilities well specified. More in detail, the question we wanted to answer in the NoW project was whether (safety) applications should include message forwarding capabilities or if they can assume all functionality to be implemented in lower layers. For this reason, we discuss two different approaches, Packet-Centric Forwarding (PCF) and Information-Centric Forwarding (ICF), both aimed to disseminate information in a vehicular environment. Afterwards, it is argued where and how functions related to node connectivity should be implemented. This analysis is based on our previous work [TMFH06].

7.1 Protocol architecture design

In general, a protocol architecture achieves interoperability for communication among network nodes and provides the framework for implementation. In designing the communication suite for IVC, two approaches can be taken.

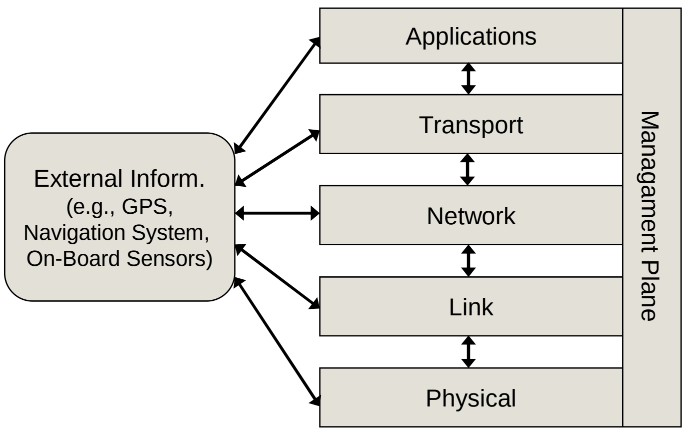


Figure 7.1: Layered approach for an IVC system.

The first approach, called a *layered approach* and depicted in Figure 7.1, attempts to retain the order of functions and protocol layers with well-defined interfaces between them, as in the Internet protocol stack (as described in [Hal05]). It adapts system functionalities to the needs of an IVC system, resulting in protocol layers for single-hop and multi-hop communication. The limitations and inflexibility of traditional network stacks when used in ad hoc networks are well known and have been previously addressed in several approaches, e.g., Protocol Heap [BFH03], Flexible Protocol Stacks [Tsc91], and Sensor Stack [KPCJR04], which influenced the design of our later proposal.

In a layered approach, each layer is implemented as an independent module with interfaces, or Service Access Points (SAPs) [JA90], only to the adjacent above and below layers. Consequently, protocols can not easily access state or metadata of a protocol on a different layer, which makes data aggregation difficult. It is also worth noting that every layer accesses external information separately with no common interface, which might lead to problems when this information influences the protocol flow. The latter point is relevant in IVC systems due to the existence of vehicular on-board sensors such as GPS.

The second approach, called *un-layered approach*, would be the result of tailoring a whole new system to the needs of IVC's main focus, i.e., safety applications. Having accurate specifications of these applications and the intention to use the unreliable channel in the most efficient manner leads to having a highly coupled set of protocols. Therefore, all application and communication protocols are placed in one single logical block right over the physical interface and connected to the external sensors, see Figure 7.2. Inside this block, all protocol elements are modularized such that there are no restrictions on interaction, and state information is arbitrarily accessible. Note though, that due to arbitrary and complex interactions of their modules this 'architecture' inherits a high design complexity. This makes protocol specification a complicated matter and so, once designed, it becomes an extremely inflexible system for other types of application. Also, it would be difficult to systematically avoid control loops, which is rather easy in the layered approach with its clean top-down or bottom-up packet traversal.

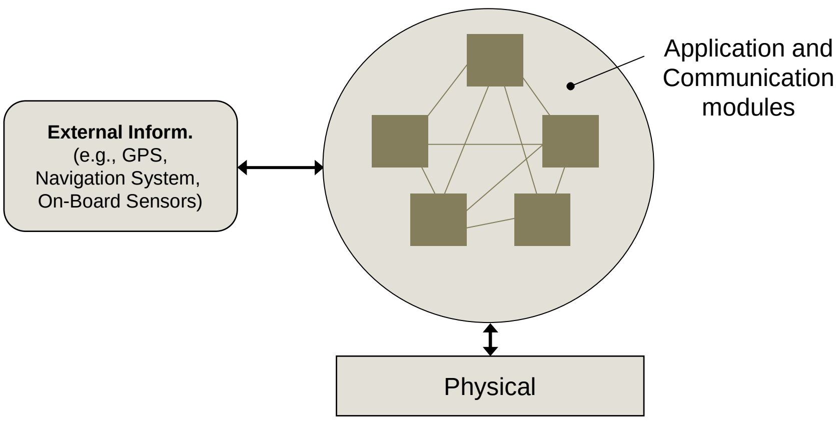


Figure 7.2: Un-layered approach for an IVC system.

While both approaches would certainly be feasible, each has strengths and weaknesses with respect to assignment of functions, information sharing, flexibility, complexity, and other IVC-specific requirements. In summary, the unlayered approach may lead to an unacceptable degree of complexity in terms of interactions among the modules and of inflexibility when trying to combine it with other types of applications. The traditional layered approach is potentially too restrictive with respect to assignment of functionality, protocol interaction, and exchange of state information inside a stack.

Figure 7.3 presents a concept in between the two 'extreme' options discussed above. In this proposal we intend to use the most adequate features of both options: *i)* having a layered approach that gives us a clear and modular structure in which to build our applications and protocols, but also offering *ii)* a clean way of sharing information and to cooperate between any protocol module on any layer as needed. Indeed, we consider a key feature the capability to share information in an efficient and clean manner without creating complex control interactions.

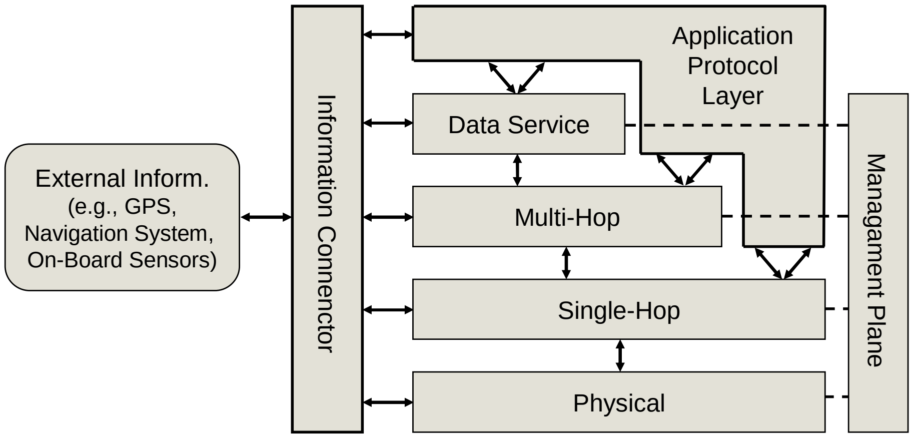


Figure 7.3: Sketch of the proposed protocol architecture for inter-vehicle communication systems.

In more detail, we identify the following key features:

Presence of layers: To facilitate a structured protocol design, we use the same core structure as in the layered approach. The original design purpose of each layer is still valid for IVC, however, modifications or extensions are required. Note that the traditional ISO/OSI [Zim80] names have been replaced in each layer to give a fundamental understanding on what has to be handled. The *physical layer* provides the means to transmit/receive a data frame over/from the wireless medium. The *single-hop layer* incorporates all functionality dealing with communication to direct radio neighbors. The *multi-hop layer* contains protocol elements for forwarding packets to non-neighboring nodes, using neighbors as forwarders. The *data service layer* allocates reliability mechanisms between multi-hop packet-forwarding and the application.

Staircase approach: An application can select from among multiple service access points to interact with lower layers. Depending on its requirements, an application can choose whether to use or to bypass a service offered by a lower layer, logically expressed by a staircase shape. This is a relaxation of the ISO/OSI protocol architecture where applications can only access the directly adjacent layer. This proposal, which is already used by certain applications within the Internet (see [PD03]), offers more flexibility to send packets although the standard path for outgoing packets is still top-down through the layers accessing the available service access points. This scheme facilitates a finer granularity of control, per packet-basis, from the applications or multi-hop strategies to the appropriate transmission parameters. When a data packet traverses the stack bottom-up, every protocol layer has to decide whether the packet should be given to the next higher protocol layer or to one or more application protocols. A packet header element such as a port/protocol number is required to allow for multiple applications.

Information connector: All protocols can connect to an 'information connector', which is a common interface that efficiently exchanges sensor update information, data extracted from packets, and state information (and their change) of protocol layers. The information crossbar basically follows a publisher/subscriber pattern: published information services can be subscribed by any entity. Indeed any entity, protocols and vehicular sensors, can utilize the offered interface to publish and subscribe to events such as 'Position Update Event' or 'Neighbor Position Change Event'. The information connector does not only provide a clean and potentially portable interface for sharing information, it also addresses most of the 'cross-layering' issues occurring in recent protocol proposals. This interface collects information from each source and in turn (synchronously or asynchronously) notifies subscribers of corresponding information.

External management plane: The external management plane symbolizes a configuration interface to set long-term system settings. In the sense of this proposal, it is not involved in the dynamic self-organization motivated by the different network conditions.

7.2 Discussion of layers' responsibilities

In this section we intend to identify the communication related responsibilities that should be assigned to (safety) applications and to the communication system as well as their interoperability. Therefore, for clarity reasons, we take a simplifying assumption about a node's model for the rest of the chapter: we consider that a node is basically comprised of two main interconnected entities, a communication domain (composed by the four lower layers described in Section 7.1) and an application domain. With this simple approach, we discuss the benefits and drawbacks to assign communication responsibilities with respect to the main goal of IVC, information dissemination.

In the following, we first list the most relevant aspects and assumptions that have to be taken into account when designing an inter-vehicle communication system. Then, we describe two approaches for information dissemination, which help identifying the most appropriate assignment of communication responsibilities in IVC systems. Finally, we describe and justify the derived assignment of responsibilities.

7.2.1 Relevant characteristics and assumptions

Two different types of nodes: In vehicular environments we distinguish between *smart* and *dumb* nodes. A smart node has relatively strong computational resources, typically access to on-board sensors of cars, and executes a number of applications for traffic safety and driving comfort. In contrast, a dumb node is a cost-efficient device with limited computational capabilities, typically but not only, installed as low cost road-side unit. From a complete system perspective, a dumb node works as a simple forwarder required to improve network connectivity with low penetration rates or in situations with low traffic density. Dumb nodes, therefore, will not be able to process the information contained in the message payload.

Diverse types of applications: As outlined in Chapter 2, we can classify IVC applications in three main groups with respect to the relevance of their information: *safety-of-life*, *safety* and *non-safety*. All three, as their names suggest, present very different requirements with respect to reliability and delay. Hence, not only a prioritization but also different communication strategies might be required to satisfy their specific demands in a shared communication medium.

Hazard detection: We consider two different ways of detecting a hazard that potentially compromises road safety:

- *On-board sensors and/or state information.* A node's safety application detects a new hazard processing the different state information gathered from other nodes and/or the on-board sensor's state, e.g., hard deceleration of the vehicle or two vehicles driving in different roads approaching an intersection at high speed.

- *Warning message.* A vehicle receives a wireless message from another node that detected an existing hazard. This 'warning' message already includes information about the detected hazard, e.g., car crash message or icy road message.

The main difference between both groups is the node originating the information, i.e., one detects the hazard directly, by its 'own means', and the other is informed by another node.

Two opposite and challenging network situations: As outlined in Chapter 4, in vehicular environments two scenarios can be identified that require two opposite communication strategies: sparse and dense networks. In dense networks, such as cities or major highways with a large portion of equipped vehicles, the data load on the channel should be controlled in order not to exceed the limited wireless bandwidth. Furthermore, any forwarding strategy is required to be very efficient in terms of overhead while ensuring high reliability to messages with the most relevant payload, i.e., *safety-of-life* messages.

In contrast, channel saturation is not an issue in sparse networks, such as in the introduction phase of such a technology. Moreover, messages should be re-transmitted since equipped vehicles are most likely out of wireless radio range of each other, i.e., vehicles inside a hazard's area of influence, but not reachable at the time it is detected, should also be notified.

Safety information must be kept 'alive': Safety hazards can be associated with a time duration and geographical area while/where they can potentially affect vehicular safety state. Therefore, and taking into consideration the existence of sparse network scenarios, we assume that the distribution of some state information will be repeated (e.g., periodically or at detection of a new neighboring vehicle) for a defined duration of time while being inside a specific geographical area. We refer to this time and area as *time of validity* and *area of validity* respectively.

7.2.2 Information- and packet-centric forwarding approaches

We identify two opposite approaches for information dissemination in vehicular scenarios: *packet-centric forwarding* and *information-centric forwarding*. Packet-centric forwarding (PCF) refers to the conventional approach for packet-switched communication where the source breaks the information into data packets and address them to one or more network nodes. With PCF the responsibility of information dissemination resides on the network (or 'multi-hop', see Section 7.1) layer, i.e., specific forwarding algorithms, located at the multi-hop layer, should provide an efficient delivery of these packets over potentially multiple wireless hops. A vehicle detecting a hazardous situation by its 'own means' (i.e., not from a warning message) generates a data packet containing the application payload (commonly, type of emergency and location and time it was noticed). In order to disseminate the packet geographically by the multi-hop layer the application also determines the *area of validity* and the *time of validity*, and includes them into the packet header. In order to keep an information 'alive' inside the *area of validity* a 'store and forward' strategy (see [LA05]) can be implemented in the multi-hop layer.

In contrast, information-centric forwarding (ICF) does not rely on an end-to-end semantic implemented in multi-hop layer. With ICF, which can be considered as an adaption of the well-known concept in sensor networks 'data centric routing' [KEW02], the responsibility of information dissemination resides on the application. Basically, when a vehicle detects a hazard it 'single-hop' broadcasts a packet (containing the type of hazard, the point of time and the location when and where the hazard was noticed). A vehicle that receives this message will deliver the message directly to the correspondent application, without any further action required from the multi-hop layer. Then, the application in turn merges the new information with the (locally-stored) safety information and decides about further procedures with respect to the hazard, i.e., whether and when to issue a new one-hop broadcast to the wireless channel.

Motivation for a hybrid approach

In the previous sections we have presented relevant aspects to take into consideration in the design process of IVC systems and two valid approaches for information dissemination, ICF and PCF. In this section we will point different benefits and drawbacks of both strategies due to the different IVC's aspects and scenarios in order to assist the design process of the most appropriate communication system.

Existence of dumb nodes: *Dumb nodes* are an extremely important requirement for a successful initial deployment of an IVC, when only a small portion of equipped vehicles exist. Dumb nodes can act as simple data forwarder being able to temporary cache information and adapt its forwarding behavior to changing conditions in their vicinity. The limitation of dumb nodes is the fact that applications are not available as in smart nodes. The required compatibility with nodes that are not able to process or understand the information in a message payload makes a solution inappropriate where solely ICF is implemented. Consequently, the required existence of dumb nodes favors the use of the PCF approach, especially in the first years of deployment of such a system.

Scalability: ICF presents a clear benefit with respect to *scalability*. We assume that the available wireless bandwidth is limited and also that, in dense networks, vehicles in the vicinity might detect same or related safety events. Since with ICF the application would process the payload of a data packet, ICF facilitates the aggregation, modification, and invalidation of information. These procedures can considerably reduce the overhead created by redundantly transmitted information. Consequently, some portion of wireless bandwidth can be 'saved' with respect to a same hazard being noticed by different sources, especially when keeping a (variable over time) information 'alive'.

***Safety-of-life* messages in dense network situations:** In case an emergency is detected in a dense network a strategy capable to disseminate the information in an extremely reliable and rapid manner is required. In this situation, where a *safety-of-life* message is handled, ICF capabilities (aggregation, modification, and invalidation) may present a disadvantage in terms of forwarding delay. PCF offers the benefit of easily track the messages to avoid redundant –harmful– message duplicates in a simple and rapid way at multi-hop layer, i.e., safety critical packets should not be modified nor processed by the application before being forwarded. Therefore, this strategy can be implemented as a service of the (common to all applications and types of nodes) communication domain.

The conclusion of this argumentation points to a hybrid approach. A strategy combining both PCF and ICF would enable receivers of a safety message to include both remote and local knowledge before forwarding the safety information. At the same time, geo-addressing capabilities are offered from the multi-hop layer, e.g., for dissemination of *safety-of-life* data, and the compatibility of *smart* and *dumb* nodes is ensured. In the following section we present a proposal of an appropriate system design for information dissemination that fulfills all requirements presented above while trying to keep a clean and modular architecture.

7.2.3 Hybrid model for a vehicular node

In this section, we introduce a software architecture that allows a clear system design and an unambiguous assignment of functions. The software architecture structures the function set of an IVC node in the two different architectural domains, an *application domain* and a *communication domain*.

We regard the *application domain* as a component that comprises all safety applications. These applications gather all safety information available to inform the driver of unsafe situations and trigger the process of sending or forwarding relevant safety data to other nodes.

The *communication domain* is composed of all mechanisms and protocols needed to deliver the relevant information to the correspondent destinations with the reliability required by the different applications (when possible).

Note that a strong coupling between the *application* and the *communication domain* is implied. Applications must assist the *communication domain* in their task of delivering information respecting its relevance. At the same time, applications can benefit from the knowledge of the capacity limitations and actual status of the wireless channel.

Figure 7.4 depicts a high level structure of the proposed system. The figure basically shows the two main building blocks of an IVC node, the *application domain* and the *communication domain*, with the most relevant functions for dissemination of safety information. *Application domain* and *communication domain* interact via interfaces for the exchange of safety data to be sent to, or received from, other nodes and state information (via SAPs and the information connector). While the detailed specification of both domains and the correspondent interfaces is beyond the scope of this thesis, the rest of the chapter describes *i)* how the required functions in an IVC node are assigned to appropriate domains and structured into functional blocks (Figure 7.5), and *ii)* how the compatibility with dumb nodes can be achieved.

Communication Domain

The *communication domain* is common to smart and dumb nodes, and provides the following main functions:

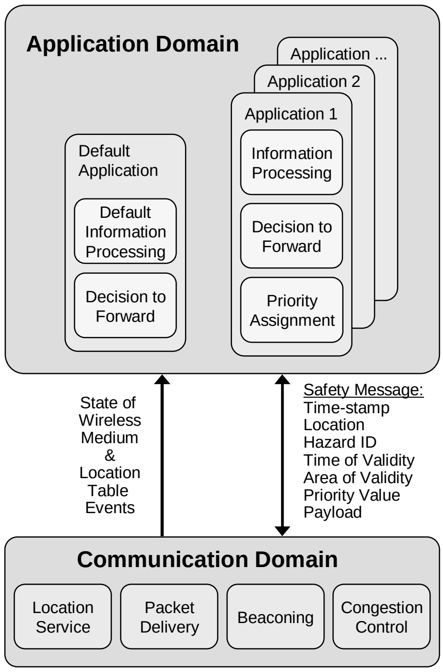


Figure 7.4: High level view of the proposed model for IVC nodes.

Location Service: The *communication domain* has to provide to the application a distributed algorithm that resolves the location of other nodes in the network. This module is also responsible of maintaining the *Location Table* (LT, where positions of other nodes are maintained as soft state) to assist both routing/forwarding protocols and applications.

Packet delivery: The *communication domain* is capable of different addressing schemes. A unicast address identifies a single node and it is used for point-to-point communication. A broadcast address refers to all nodes within one wireless hop. A geocast address identifies all nodes that are located inside of a geographical area. Note that these addressing schemes also serve packets coming from the wireless medium (through the forwarding condition in Figure 7.5).

Also notice that we consider different instances of geocast packet delivery strategies, see Figure 7.5. This decision responds to the different requirements of future applications (including safety and non-safety related) and the existing trade-off between reliability and overhead. As shown in Chapter 6.2.2, the EMDV protocol, which should be implemented in this module, can provide a higher reliability for *safety-of-life* messages at the cost of higher, but controlled, redundancy.

Beaconing: Beacons are periodic messages broadcasted by the *communication domain* to support both, the ad hoc routing/forwarding protocols and the applications. Apart from the position of a vehicle, beacons also contain state information common to relevant applications, e.g., speed and direction, as described in Chapter 2. Note that due to the different requirements between safety applications and routing/forwarding protocols, applications should motivate the in-

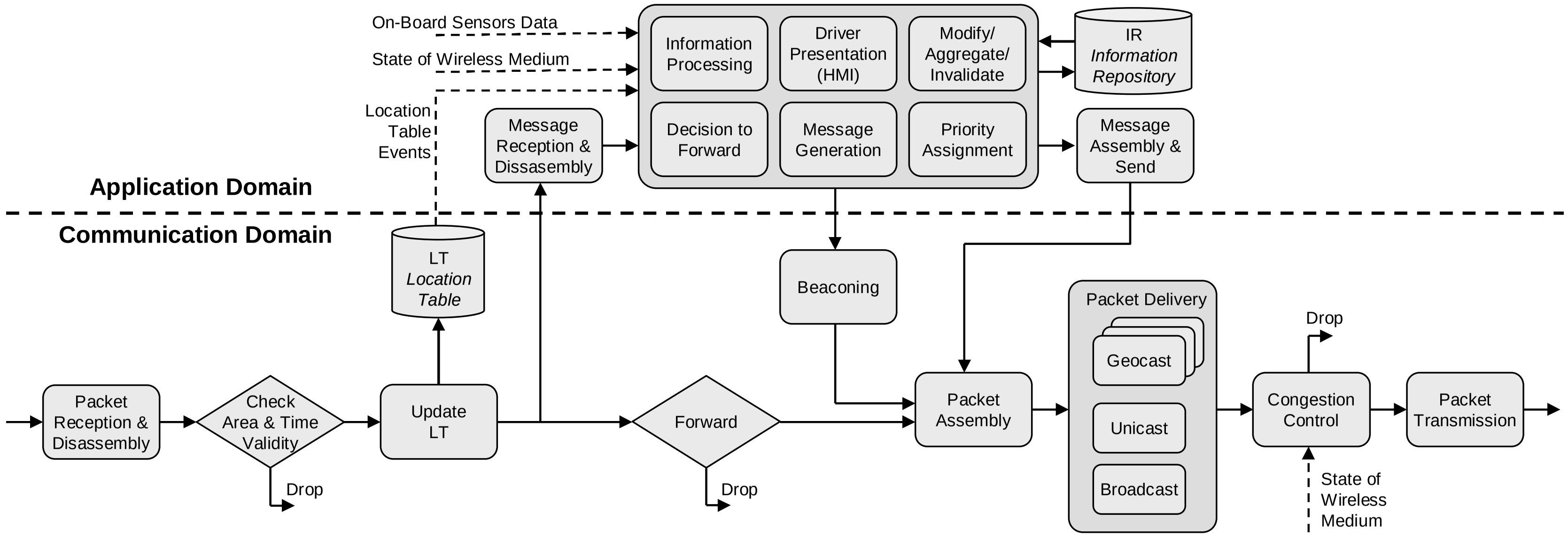


Figure 7.5: IVC's node information flow with a generic smart application. Dashed arrows represent information to/from the information connector. Solid arrows between the application and communication domains represent interfaces via service access points.

crease of the message generation period, e.g., at high speeds or in the vicinity of an intersection (see the arrow at Figure 7.5 between th application domain and the beaconing module).

Congestion control: The *communication domain* has the goal of ensuring a perfect stability of the network at all times: it avoids network congestion by monitoring the network utilization and controlling the physical layer for packets transmission. Applications should assist the congestion control in order to ensure that the safety relevance of the different communications is respected. For this reason, we propose as a first approach the use of a simple priority value (supported by IEEE 802.11p [11p]); the application determines the priority based on the relevance of the information and assigns the value to each message. This value is used by the *communication domain* to take adequate decisions when controlling the load on the channel. Additionally, we consider that congestion control strategies combine a set of mechanisms including deferring packet transmission, smart discard of low-priority packets, and dynamic setting of transmission parameters on a per packet basis.

Although we expect different congestion control mechanisms implemented in different protocol entities, we assign a main congestion control module to the single-hop layer (Section 7.1). This congestion control strategy should serve as a bottleneck to all packets heading to the wireless link and it is, thus, able to control the packet flow based on its queue and the information gathered by the information connector. In Chapter 5.2, we defined the the congestion control strategy for beacon messages, D-FPAV, which should be implemented in this module.

Application Domain

The *application domain* is where all applications reside. Apart from the *default application* (addressed later in Section 7.2.4), all safety-related applications include the following key functionalities:

Information repository (IR): In order to detect certain unsafe situations and be able to take the optimal decision in case an emergency occurs, each application contains a repository where information relevant to this specific application is kept. Local mechanisms and processes enable aggregation, modification, or invalidation of cached information when the IR is updated. Note that a higher benefit can be accomplished when a central IR common to all applications exists. Possible benefits are: memory efficiency, improved aggregation capabilities and interoperability between applications.

Information processing: When receiving state (safety) information, either from local sensors or through the *communication domain*, applications process the information and update the safety state of the IR.

Driver presentation: When detecting an unsafe situation the application assists the driver in preventing a potential accident. The presentation methods, e.g., the Human Machine Interface (HMI), can differ between car manufacturers and implementations.

Forwarding state/safety information: An application that detects or is aware of a certain hazard can decide to forward it either immediately (safety-of-life) or to trigger a forwarding process to periodically issue the information in application-specific intervals (safety). Also, it could motivate a higher frequency of *communication domain*'s beacons if necessary.

Priority determination: Once the decision to issue some safety information to other vehicles is taken, applications determine a safety value based on a priority function. This function takes into account the type of hazard, duration of time that has passed since the hazard occurred, distance between the local position and the position where the hazard occurred, and the local state of the wireless channel (network congestion). The result of the function is a single priority value that is assigned to the message and passed to the communication system. The priority value is used by the *communication domain*, within its congestion control module, in order to handle the message from a safety perspective.

Finally, another capability common to all applications should be considered. In order to save some bandwidth and channel access time, a module able to join different applications payloads into a single message should be implemented (*Message Assembly* in Figure 7.5). The same capability could be implemented in the *communication domain*'s module *Packet Assembly* in order to also combine beaconing information. Recently, the authors of [RCCL06] proposed a module referred to as 'Message Dispatcher', which was contributed to the Society of Automotive Engineers (SAE) [SAE], to efficiently combine the data generated by multiple safety applications.

7.2.4 Compatibility with dumb nodes and default application

The *application domain* of a dumb node is much simpler than of a smart node since many functions are not available, such as complex application logic, presentation to the driver, etc. Also, due to the requirement for cost efficiency the dumb node has limited processing resources. We propose that a dumb node contains a common *default application* that, at least, is able to interpret time and area of validity. In particular, a dumb node is not required to process and interpret the message payload. The default application is able to temporarily cache and to re-broadcast cached messages.

In contrast to a smart node's *application domain*, a dumb node caches a safety message in a *Message Repository (MR)*. This message is re-broadcasted periodically while its time and area of validity are still valid. The re-send interval is either fixed with a default period or dynamic depending on the priority value. Note that safety-of-life messages will not be stored in the *MR*.

We recall that the described default application should also be part of the *application domain* of smart nodes. This way, the compatibility among nodes having different implementations or versions of future safety applications would be ensured.

7.3 Conclusions

In this chapter, we have presented an architectural concept for inter-vehicle communication systems. Motivated by IVC's main goal of disseminating safety-related information, we identified the main building blocks and proposed design guidelines which satisfy the needs of safety-related communications.

The design is organized in protocol layers to avoid complex interactions among protocol entities and provide a clean and modular structure. At the same time, it allows a versatile exchange of information among different modules, a finer granularity of control on transmission parameters and ensures the compatibility between smart and dumb nodes. Furthermore, the different communication responsibilities as well as the D-FPAV and EMDV protocols (proposed in Chapter 5) are assigned to the different building blocks.

As a result, we achieve a simple and robust system model with low complexity as a basis for implementation.

8
Summary, Conclusions and Outlook

Improving the safety of drivers and passengers by wirelessly exchanging information between vehicles represents a major driving force for the design of vehicular networks. This thesis has proposed inter-vehicle communication (IVC) protocols and system design guidelines to overcome existing challenges and support active safety applications improving road safety.

We assumed that vehicular networks will use IEEE 802.11p, or an 802.11 variant, and the market penetration will be high. Under these assumptions, we first intended to identify the major challenges to design IVC systems with the goal of improving vehicular safety. We started with classifying two types of communications that can support active safety applications: the periodic transmission of broadcast 'status' messages, also called beacons, and the dissemination of event-driven messages. Both types of communications have been studied from a safety perspective in order to identify the existing challenges and characterize them in detail. Our study included a detailed simulation analysis of one-hop broadcast communications in vehicular environments using an extended version of the network simulator ns-2.28. The implementation work on the network simulator consisted of more accurate and updated models for radio wave propagation, wireless interfaces following the IEEE 802.11p draft standard and realistic vehicular movement patterns corresponding to fast-moving German highway scenarios.

On the one hand, the obtained results outline the hidden terminal problem, a high channel load, and the adverse radio propagation phenomena as the main challenges to reliably deliver broadcast messages. On the other hand, we identified the arising challenges caused by the high saturation conditions expected in dense fast-moving vehicular networks and the fact that both beacons and event-driven messages share one common channel.

Based on the analysis realized, we identified the need of a mechanism to control the resulting beaconing load on the channel. High load on the channel results in a high amount of packet collisions, which decreases the probability of receiving these beacon messages. In turn, a lower probability of reception results in a lower 'safety level' as seen by the applications, particularly at close distances from the transmitter where they are most important. In the case of event-driven messages, a robust emergency dissemination strategy able to satisfy the time-critical safety requirements in spite of all the challenges is needed. This strategy has to deliver the information to all vehicles in a geographical area in an efficient and rapid manner.

Thus, we have proposed two protocols respectively for the two types of vehicle safety messages to overcome the main challenges identified. The D-FPAV (Distributed Fair Power Adjustment in Vehicular environments) mechanism limits the beaconing load on the channel below a predefined threshold while ensuring a high probability of beacon reception at close distances from the sender. The EMDV (Emergency Message Dissemination in Vehicular environments) strategy disseminates emergency information within a geographical area. Additionally, we evaluated the performance of the protocols with the extended simulator.

The key elements of the design of these two communication schemes and their main properties can be summarized as follows:

– We make use of the max-min fairness criterion and apply it to the power control of beacon messages since in our opinion it is the criterion that best addresses safety.

– We have shown that fairness with respect to power control can be achieved in a distributed fashion. The communication overhead required is reasonable to achieve fairness.

– For robust and effective information dissemination we make use of the idea of contention-based forwarding that can very well deal with the unreliability of the channel and with the mobility of the nodes.

– For delay reduction in the dissemination process we also make use of the beacon information and use standard position-based forwarding techniques in combination with the contention-based approach.

– Synergy is gained when using both protocols together since D-FPAV ensures that the channel load is kept on a level such that EMDV can achieve an improved performance in terms of efficiency as well as delay.

Furthermore, according to the results obtained from their evaluation, we can conclude that we accomplished our goals of supporting active safety applications by: *i)* ensuring a high reception probability of beacon messages within the 'safety distance' of vehicles and *ii)* achieving to deliver emergency information to vehicles within a geographical area reliably and with short delay.

Last, assuming safety as the main goal of inter-vehicle communications, we have proposed a versatile protocol architecture that provides a clear modular structure with flexibility for protocol interaction and information exchange at a reasonable complexity. Among the key features of this protocol architecture are IVC-specific protocol layers, a staircase approach to interaction among layers and the use of an information connector for cross-layer information exchange with a publisher/subscriber pattern.

The results achieved in this thesis constitute a fundamental contribution to the development of inter-vehicle communications by providing a robust design to cope with unreliable and saturated wireless channel conditions. The proposed system architecture and communication protocols compose an integrated solution to support safety applications to reduce the amount and severity of vehicular traffic accidents.

Moreover, the results obtained compose a basis for future IVC design and deployment decisions. Although we have shown how satisfactory results can be achieved with one transceiver in a vehicle, the performance could be further improved with the utilization of multiple transceivers in each vehicle. The trade-off between cost and benefit of a multi-transceiver solution should be balanced by application designers together with the electronic and the automotive industries.

As future work, an appropriate configuration of the communication protocols should be performed once safety requirements are specified by vehicular active safety applications. To adjust the protocols' configuration parameters, the following trade-offs have to be addressed: *i)* priority of periodic vs. event-driven messages, *ii)* beaconing fairness vs. overhead, and *iii)* dissemination reliability vs. overhead.

Also, some effort should be devoted to designs targeting at specific safety-critical road situations. These particular scenarios have not attracted much attention from researchers so far. However, solving specific cases can have a significant benefit in terms of improving vehicular safety. These situations should be identified (e.g., last car on a traffic jam or stopped car behind a curve) and tailored solutions should be proposed.

Furthermore, safety-related IVC design should be ultimately developed coupling applications with communication protocols. Only with the combination of both, they can be evaluated and configured with respect to their beneficial effect on road safety. To the best of our knowledge, there are no existing methodologies and application-specific metrics which are capable of quantifying the performance of inter-vehicle communications with respect to their ultimate goal, i.e., reduce the amount of accidents and fatalities on roads.

A
IEEE 802.11p MAC and PHY Values

Here, we present the main characteristics of the physical (PHY) and medium access control (MAC) layers of the IEEE 802.11p draft [11p], which are relevant for the extensions performed in the network simulator described in Chapter 3. Additionally, we provide a short description of the parameters as well as the IEEE 802.11a [11a] (also OFDM-based) values for comparison.

Characteristic	**802.11p WAVE**	**802.11a**
Channel bandwidth	10 MHz	20 MHz
Data rates	3 to 27 Mbps	6 to 54 Mbps
SlotTime	16 μs	9 μs
SIFSTime	32 μs	16 μs
CHSwitchTime	$\leqslant$ 2048 μs	–
AirPropagationTime	$<$ 4 μs	$<<$1 μs
PreambleLength	32 μs	20 μs
PLCPHeaderLength	8 μs	4 μs
CW_{min}	15	15
CW_{max}	1023	1023

Table A.1: IEEE 802.11p characteristics.

- **SlotTime:** Time that the MAC utilizes to define the DCF interframe space and to decrement in steps the backoff interval. It is computed as the sum of: *i)* the minimum time necessary to assess whether the medium is busy, *ii)* the maximum time required by the PHY to switch from receiving state to start transmitting a frame, *iii)* the AirPropagationTime, and *iv)* the nominal time that the MAC needs to process a frame and prepare its response.

- **SIFSTime:** Nominal time required by the MAC and PHY to receive the last symbol of a frame at the air interface, process it, and answer with the first symbol on the air interface.

- **CHSwitchTime:** Time required by WAVE systems to switch between two channels.

- **AirPropagationTime:** Anticipated time that the transmitted signal needs to arrive at the receiving station.

- **PreambleLength:** Time necessary to transmit the PLCP (Physical Layer Convergence Procedure) preamble by the PHY.

- **PLCPHeaderLength:** Time necessary to transmit the PLCP (Physical Layer Convergence Procedure) header by the PHY.

- **CW_{min}:** Minimum value of the contention window size.

- **CW_{max}:** Maximum value of the contention window size.

As outlined in Chapter 2, the decision to operate in 10 MHz channels, instead of 20 MHz ones, was taken in order to reduce the symbol interference. Indeed, vehicular scenarios present more 'adverse' communication conditions than conventional 802.11-based ones in terms of node mobility, node density, and environment. Note that the utilization of 10 MHz channels affect the data rates supported, the PreambleLength and the PLCPHeaderLength.

Additionally, inter-vehicular communications are designed to provide larger communication distances. Note the higher AirPropagationTime value and, accordingly, the longer SlotTime required for coordination among transmitting nodes.

Finally, the time CHSwitchTime parameter is introduced due to the multi-channel capabilities of WAVE systems. Note though, that this feature is not implemented in the simulator since it is not relevant for our purposes.

B
The Impact of Hidden Nodes under a Deterministic Channel Model

Here, we provide a detailed explanation about the effect of hidden nodes on IEEE 802.11-based broadcast reception rates. We focus on the scenario described in Chapter 3, where nodes are vehicles located on a highway and send periodic one-hop broadcast messages. To develop our explanation we utilize the deterministic radio propagation model 'two ray ground' as implemented in ns-2.28 [NS2] and described also in Chapter 3. Moreover, we use the terms:

- Transmitter (T): node transmitting a message.
- Receiver (R): node intended to receive the message sent by the transmitter.
- Hidden node (HN): node that does not sense the message sent by the transmitter and generates an interfering signal.

Due to the nature of CSMA/CA and the interference model of the simulator, a hidden node is outside of the carrier sense range of the transmitter and inside of the carrier sense range of the receiver[1] (as seen in Figure 3.7). The effect that a hidden node can have on an ongoing transmission differs depending on the

[1] The interference model of our extended version of the ns-2.28 simulator takes into consideration interferences with a power equal or above the thermal noise level. However, in this Appendix we do not take into account interferences with power level below the CSTh (Carrier Sense Threshold) for simplicity.

distance between nodes. A hidden node can cause a collision only if it is located close 'enough' to the receiver.

Figure B.1 illustrates, in case of assuming the same transmission power for all packets, how to compute the range around the transmitting node where a hidden node can not cause a collision, which we refer to as 'robust range against hidden nodes'[2]. At the figure, HN represents the closest hidden node to node R able to interfere with T's transmission. As specified in Chapter 3, in order for node R to be able to capture T's message and discard the interference from HN, the difference between T's message power (P_T) and HN's power (P_{HN}) must be higher than the capture threshold CpTh, i.e., $P_T - P_{HN} \geqslant CpTh$. The distance d_r where $P_T - P_{HN} = CPTh$ fixes the border where hidden nodes can prevent captures, i.e., cause collisions. For a CR = 500 m and a data rate of 6 Mbps we obtain a transmission distance 'robust' against hidden nodes d_r = 205.0 m. In case of probabilistic propagation models, the robustness of this range clearly depends on the experienced attenuation variance and the resulting performance of the CSMA/CA mechanism.

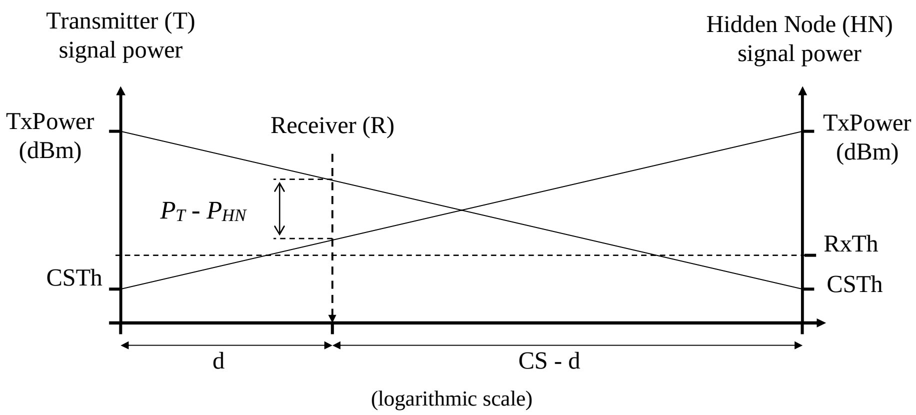


Figure B.1: Illustration of the 'robust range against hidden nodes' with a deterministic propagation model.

Figure B.2 presents the probability of reception of a broadcast message in the lower vehicular density scenario, with 36 cars/km and the two ray ground model, that corresponds to the curve represented in Figure 3.6. All cars are configured to send 10 broadcast messages per second with a 6 Mbps data rate and a communication range of 500 m. Observe how the probability that two neighboring nodes select the same slot for transmission is very low, below 1.5%. Therefore, the probability of successful reception stays above the 98.5% within the robust range

[2]Note that in the case where more than one hidden node transmits to the medium simultaneously, the accumulated power of the interference could cause a packet reception to fail also within the robust range against hidden nodes.

against hidden nodes[3]. Outside of this range, probability of reception values decrease due to the collisions caused by hidden nodes.

Moreover, the slope of the curve in Figure B.2 reflects the amount of hidden nodes capable to cause a collision at that distance between sender and receiver. To explain the shape of this slope and its change around 300 m, we plot the length of the range where hidden nodes can be located which can cause a collision at the receiver, see Figure B.4.

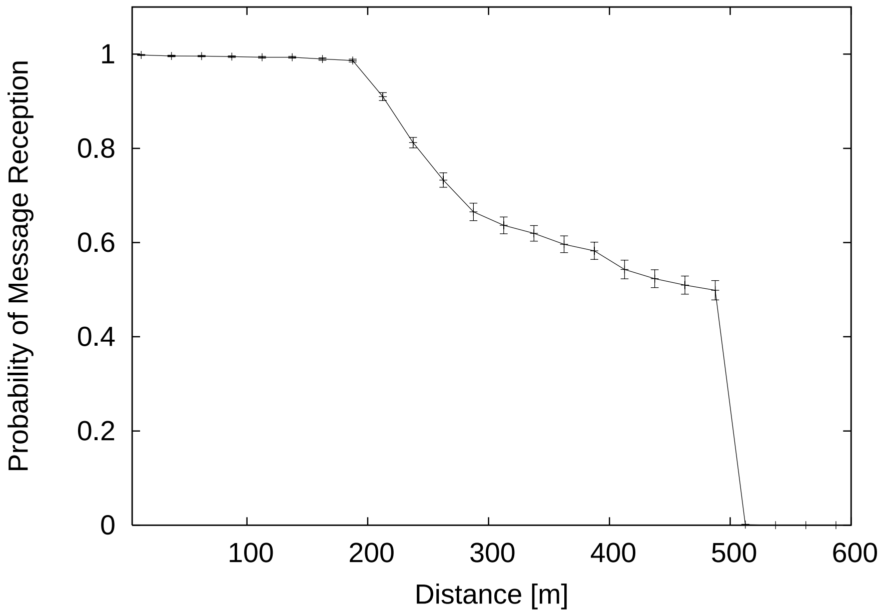


Figure B.2: Probability of successful beacon reception with respect to the distance in a 3-lane per direction highway scenario with 36 vehicles/km, data rate of 6 Mbps, intended communication range of 500 m, packet generation rate of 10 pckts/s and the two ray ground model.

Assuming that all nodes are placed on a straight line, the spatial location where a hidden node can be found corresponds to the range limited by the borders of the transmitter and the receiver carrier sense ranges, which we call HN range, see Figure B.3. However, only a ratio of that range corresponds to hidden nodes that can cause a collision, which we call CHN (Colliding Hidden Nodes) range. Nodes inside the HN range but outside of CHN range do not satisfy the condition $P_T - P_{HN} < CpTh$.

In Figure B.4 we represent the longitude of the HN and CHN ranges with respect to the distance between a sender and a receiver. This ranges are proportional

[3]Note that the distance where the reception curve starts decreasing is at 187.5 m instead of at 205.0 m. The closer distance is caused by the averaging performed to present the data. In this case, each point in the figure represents the average over 25 m.

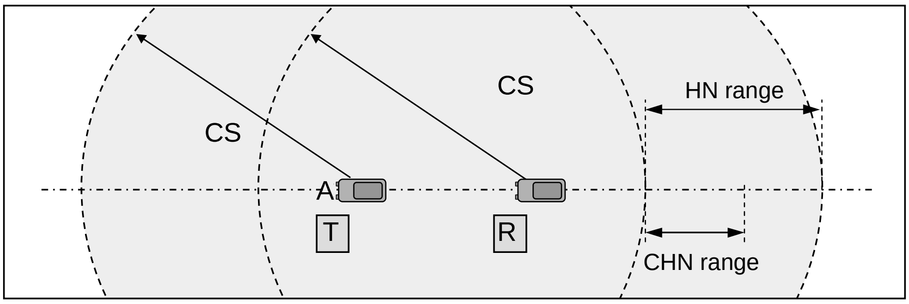


Figure B.3: Illustration of the HN (Hidden Nodes) range and the CHN (Colliding HN) range.

to the amount of hidden nodes and colliding hidden nodes, when assuming a uniform node distribution. The HN range corresponds to the distance between sender and receiver. The CHN range, on the other hand, is equal to 0 for values within the robust range against hidden nodes. At this distance, CHN starts increasing with a higher slope than the HN range.

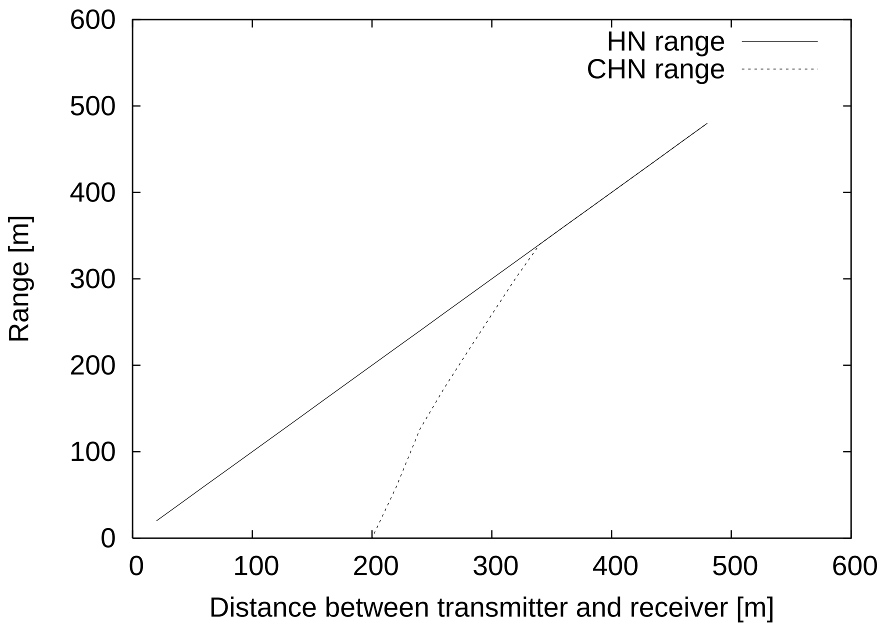


Figure B.4: HN and CHN ranges with respect to the distance between the transmitter and the receiver.

At 338 m, the HN and CHN curves meet, and present the same values for further distances. This 'artifact' is caused by the interference model of the simulator: only messages that arrive with a reception power above a certain level are taken into account, see Chapter 3. Therefore, as Figure B.3 shows, CHN range can not be larger than HN range, what causes the slope of the CHN range to be smaller for distances above 338 m. This effect can be observed in Figure B.2, the probability of reception decreases with a smaller slope at the corresponding distances between sender and receiver. Note though, that the change of slope in Figure B.2 occurs at a closer distance due to the low vehicular density (one car every 27.7 m in average) together with the averaging over 25 m realized to present our results.

Finally, the change of slope of CHN range at 243 m corresponds to the case where the distance between right limit of CHN range (in Figure B.3) and the receiver is equal to the cross-over distance[4]. From 243 m, therefore, the slope of CHN range is slightly lower due to the stronger decrease of the received signal strength from hidden nodes located at further distances.

[4]As described in Chapter 3.2.2, the cross-over distance corresponds to the distance where the two ray ground path loss exponent from 2 to 4.

Bibliography

[11] IEEE Std 802.11-1997, 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, June 1997.

[11a] IEEE Std 802.11a-1999, Amendment 1: High-Speed Physical Layer in the 5 GHz Band, September 1999.

[11e] IEEE Std 802.11e-2005, Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, November 2005.

[11p] IEEE P802.11p/D0.21, Draft Amendment for Wireless Access in Vehicular Environments (WAVE), January 2006.

[9.1] IEEE P1609.1/D12 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - WAVE Resource Manager, November 2005.

[9.2] IEEE P1609.2/D3 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages, November 2005.

[9.3] IEEE P1609.3/D18 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, December 2005.

[9.4] IEEE P1609.4/D07 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation, December 2005.

[AC01] I. Aad and C. Castelluccia. Differentiation Mechanisms for IEEE 802.11. In *Proceedings of the 20th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Anchorage, AK, USA*, volume 1, pages 209–218, April 2001.

[ARP05] M. Artimy, W. Robertson, and W. Phillips. Assignment of Dynamic Transmission Range Based on Estimation of Vehicle Density. In *Proceedings of the 2ns ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Cologne, Germany*, pages 40–48, September 2005.

[ASV] The Fourth Phase of Advanced Safety Vehicle Project. ITS Hand Book 2006-2007, http://www.its.go.jp/ITS/index/ index-HBook2006.html.

[BD91] W.R. Braun and U. Dersch. A Physical Mobile Radio Channel Model. *IEEE Tranasactions on Vehicular Technology*, 40(2):472–482, May 1991.

[BFH03] R. Braden, T. Faber, and M. Handley. From Protocol Stack to Protocol Heap: Role-Based Architecture. *ACM SIGCOMM Computer Communication Review (CCR)*, 33(1):17–22, January 2003.

[BG87] D. Bertsekas and R. Gallager. *Data Networks*. Prentice Hall, 1987.

[Bia00] G. Bianchi. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal on Selected Areas in Communications (JSAC)*, 18(3):535–547, March 2000.

[BM05] S. Biswas and R. Morris. ExOR: Opportunistic Routing in Multi-Hop Wireless Networks. In *Proceedings of the ACM Conference of the Special Interest Group on Data Communication (SIGCOMM), Philadelphia, PA, USA*, pages 133–144, August 2005.

[BSH00] L. Briesemeister, L. Schäfers, and G. Hommel. Disseminating Messages among Highly Mobile Hosts based on Inter-Vehicle Communication. In *Proceedings of the IEEE Intelligent Vehicles Symposium (IVS), Dearborn, MI, USA*, pages 522–527, October 2000.

[BTD06] S. Biswas, R. Tatchikou, and F. Dion. Vehicle-to-Vehicle Wireless Communication Protocols for Enhancing Highway Traffic Safety. *IEEE Communications Magazine*, 44(1):74–82, January 2006.

[C2C] Car2Car Communication Consortium. http:// www.car-to-car.org/.

[CB05] D.R. Choffnes and F.E. Bustamante. An Integrated Mobility and Traffic Model for Vehicular Wireless Networks. In *Proceedings* *of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Cologne, Germany*, pages 69–78, September 2005.

[CEN04] Result of resolution by correspondence TC 278/C07/2004: New work item: Road transport and traffic telematics "Multi-standard automatic dynamic debiting systems and automatic access control systems using dedicated short-range communication at 5,8 GHz" Part 4: Application layer electronic fee collection application service objectst. Comité Européen de Normalisation (CEN), TC 278 Road Transport and Traffic Telematics, N1634, July 2004.

[CFK03] X. Chen, M. Faloutsos, and S.V. Krishnamurthy. Power Adaptive Broadcasting with Local Information in Ad hoc Networks. In *Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP), Atlanta, Georgia*, pages 168–178, November 2003.

[CGM06] M. Caliskan, D. Graupner, and M. Mauve. Decentralized Discovery of Free Parking Places. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, USA*, pages 30–39, September 2006.

[Cha74] U. Charash. A study of multipath reception with unknown delays. Ph.D. dissertation, University of California, Berkeley, CA, January 1974.

[CJTD06] C. Chen, D. Jiang, V. Taliwal, and L. Delgrossi. IEEE 802.11 based Vehicular Communication Simulation Design for NS-2. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, USA*, pages 50–56, September 2006.

[COM] The COMeSafety project. http://www.comesafety.org/.

[CSK05] J. Choi, J. So, and Y.B. Ko. Numerical Analysis of IEEE 802.11 Broadcast Scheme in Multihop Wireless Ad Hoc Networks. *Lecture Notes in Computer Science, Springler*, 3391:1–10, 2005.

[CSW03] Y. Chen, E.G. Sirer, and S.B. Wicker. On Selection of Optimal Transmission Power for Ad hoc Networks. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI, USA*, volume 09, page 300c, January 2003.

[DDB05] M. Durresi, A. Durresi, and L. Barolli. Emergency Broadcast Protocol for Inter-Vehicle Communications. In *Proceedings of the 11TH International Conference on Parallel and Distributed Systems (ICPADS), Fukuoka, Japan*, volume 2, pages 402–406, July 2005.

[DPIK05] A. Durresi, V.K. Paruchuri, S.S. Ivengar, and R. Kannan. Optimized Broadcast Protocol for Sensor Networks. *IEEE Transactions on Computers*, 54(8):1013–1024, August 2005.

[DSR05] White Paper: DSRC Technology and the DSRC Industry Consrotium (DIC) Prototype Team, January 2005.

[EGH+06] T. ElBatt, S.K. Goel, G. Holland, H. Krishnan, and J. Parikh. Cooperative Collision Warning Using Dedicated Short Range Wireless Communications. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, USA*, pages 1–9, September 2006.

[ETS] ETSI - Intelligent Transportation Systems. http:// portal.etsi.org/radio/IntelligentTransportSystems/ITS.asp.

[ETS05] ETSI TR 102 492-1, Electromagnetic compatibility and Radio spectrum Matters; Intelligent Transportation Systems; Part 1: Technical characteristics for pan-European harmonized communications equipment operating in the 5 GHz frequency range and intended for ciritcal road-safety appplications; System Reference Document, June 2005.

[ETS06] ETSI TR 102 492-2, Electromagnetic compatibility and Radio spectrum Matters; Intelligent Transportation Systems; Part 2: Technical characteristics for pan-European harmonized communications equipment operating in the 5 GHz frequency range and intended for road safety and traffic management, and for non-safety related ITS appplications; System Reference Document, March 2006.

[FB04] Z. Fang and B. Bensaou. Fair Bandwidth Sharing Algorithms based on Game Theory Frameworks for Wireless Ad-hoc Networks. In *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), Hong Kong*, volume 2, pages 1284–1295, March 2004.

[FCC99] Federal Communications Commission, News Release. http://www.fcc.gov/Bureaus/Engineering_Technology/News_Releases/1999/nret9006.html, October 1999.

[FCC06] Federal Communications Commission. FCC 06-110. Memorandum Opinion and Order, July 2006.

[Fle] The Fleetnet Project. http://www.et2.tu-harburg.de/fleetnet/.

[FTMK+06] H. Füßler, M. Torrent-Moreno, R. Krüger, M. Transier, H. Hartenstein, and W. Effelsberg. MobiCom Poster Abstract: Studying Vehicle Movements on Highways and their Impact on Ad-hoc Connectivity. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, 10(4):26–27, October 2006.

[FTMT+05] H. Füßler, M. Torrent-Moreno, M. Transier, A. Festag, and H. Hartenstein. Thoughts on a Protocol Architecture for Vehicular Ad-Hoc Networks. In *Proceedings of the 2nd International Workshop on Intelligent Transportation (WIT), Hamburg, Germany*, pages 41–45, March 2005.

[FWK+03] H. Füßler, J. Widmer, M. Käsemann, M. Mauve, and H. Hartenstein. Contention-Based Forwarding for Mobile Ad-Hoc Networks. *Elsevier's Ad Hoc Networks*, 1(4):351–369, November 2003.

[GK00] P. Gupta and P.R. Kumar. The Capacity of Wireless Networks. *IEEE Tranasactions on Information Theory*, 46(2):388–404, March 2000.

[GK04] N. Gupta and P.R. Kumar. A Performance Analysis of the 802.11 Wireless LAN Medium Access Control. *Communications in Information and Systems*, 3(4):279–304, September 2004.

[Glo] GloMoSim - Global Mobile Information Systems Simulation Library. http://pcl.cs.ucla.edu/projects/glomosim/.

[GNB01] X. Gao, T. Nandagopal, and V. Bharghavan. Achieving Application Level Fairness Through Utility-based Wireless Fair Scheduling. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM), San Antonio, TX, USA*, volume 6, pages 3257–3261, November 2001.

[Hal05] F. Halsall. *Computer Networking and the Internet (5th Edition)*. Addison Wesley, March 2005.

[HFFB06] J. Haerri, M. Fiore, F. Filali, and Christian Bonnet. Poster Abstract: VanetMobiSim: Generating Realistic Mobility Patterns for VANETs. In *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, USA*, pages 96–97, September 2006.

[HWG] The HWGui project. http://www.informatik.uni-mannheim.de/pi4.data/content/projects/hwgui/.

[Int] Internet ITS Consortium. http://www.internetits.org.

[ISO] ISO TC204 WG16 Portal. http://www.tc204wg16.de/.

[JA90] B.N. Jain and A.K. Agrawala. *Open Systems Interconnection: Its Architecture and Protocols*. Elsevier, 1990.

[JP81] Ed J. Postel. RFC 791 - Internet Protocol, September 1981.

[KEW02] B. Krishnamachari, D. Estrin, and S. Wicker. Modelling Data-Centric Routing in Wireless Sensor Networks. Technical Report CENG 02-14, Department of Electrical Engineering, University of Southern California Los Angeles, February 2002.

[KK05] V. Kawadia and P.R. Kumar. Principles and Protocols for Power Control in Wireless Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications (JSAC)*, 23(1):76–88, January 2005.

[KKW+03] M. Kubisch, H. Karl, A. Wolisz, L.C. Zhong, and J. Rabay. Distributed Algorithms for Transmission Power Control in Wireless Sensor Networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA*, volume 1, pages 558–563, March 2003.

[KLS+02] V. Kanodia, C. Li, A. Sabharwal, B.Sadeghi, and E. Knightly. Ordered Packet Scheduling in Wireless Ad Hoc Networks: Mechanisms and Performance Analysis. In *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Lausanne, Switzerland*, pages 58–70, June 2002.

[KMT98] F.P. Kelly, A.K. Maulloo, and D.K.H. Tan. Rate control in communication networks: shadow prices, proportional fairness and stability. *Journal of the Operational Research Society (JSTOR)*, 49(3):237–252, March 1998.

[KPCJR04] R. Kumar, S. Pal-Chaudhuri, D. Johnson, and U. Ramachandran. Network Stack Architecture for Future Sensors. Technical Report TR-04-447, Computer Science Department, Rice University, December 2004.

[KVSA04] A. Kochut, A. Vasan, A.U. Shankar, and A. Agrawala. Sniffing Out the Correct Physical Layer Capture Model in 802.11b. In

Proceedings of the 12th IEEE International Conference on Network Protocols (ICNP), Berlin, Germany, pages 252–261, October 2004.

[LA05] T.D.C. Little and A. Agarwal. An Information Propagation Scheme for VANETs. In *Proceedings of the International IEEE Intelligent Transportation Systems Conference (ITSC), Vienna, Austria*, pages 155–160, September 2005.

[LL02] J. Liu and B. Li. MobileGrid: Capacity-aware Topology Control in Mobile Ad Hoc Networks. In *Proceedings of the 11th IEEE International Conference on Computer Communications and Networks (ICCCN), Miami, FL, USA*, pages 570–574, October 2002.

[LMFH05] C. Lochert, M. Mauve, H. Füßler, and H. Hartenstein. Geographic Routing in City Scenarios. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, 9(1):69–72, January 2005.

[LNM04a] X. Li, T. Nguyen, and R. Martin. An Analytic Model Predicting the Optimal Range for Maximizing 1-Hop Broadcast Coverage in Dense Wireless Networks. In *Proceedings of the 3rd International Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW), Vancouver, Canada*, July 2004.

[LNM04b] X. Li, T. Nguyen, and R. Martin. Using Adaptive Range Control to Maximize 1-Hop Broadcast Coverage in Dense Wireless Networks. In *Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON), Santa Clara, CA, USA*, pages 397–405, October 2004.

[LNT02] H. Lundgren, E. Nordström, and C. Tschudin. Coping with communication gray zones in IEEE 802.11b based ad hoc networks. In *Proceedings of the 5th ACM International Workshop on Wireless Mobile Multimedia (WoWMoM), Atlanta, GA, USA*, pages 49–55, September 2002.

[Lot02] M. Lott. Performance of a Medium Access Scheme for Inter-Vehicle Communication. In *Proceedings of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), San Diego, CA, USA*, July 2002.

[LZG04] W. Li, H. Zhang, and T.A. Gulliver. Error Probability for Maximal Ratio Combining on Correlated Nakagami Fading Channels. In *Proceedings of the 60th IEEE Vehicular Technology*

Conference (VTC-Fall), Los Angeles, CA, USA, volume 3, pages 1786–1790, September 2004.

[MFW05] J. Maurer, T. Fügen, and W. Wiesbeck. Physical Layer Simulations of IEEE 802.11a for Vehicle-to-Vehicle Communication. In *Proceedings of the IEEE 62nd Vehicular Technology Conference (VTC-Fall), Dallas, TX, USA*, volume 23, pages 1849–1853, September 2005.

[MLJ03] M. Meincke, M. Lott, and K. Jobmann. Reservation Conflicts in a Novel Air Interface for Ad Hoc Networks based on UTRA TDD. In *Proceedings of the 58th IEEE Vehicular Technology Conference (VTC-Fall), Orlando. FL, USA*, volume 5, pages 2985–2989, October 2003.

[MLS04] T.K. Mak, K.P. Laberteaux, and R. Sengupta. A Multi-Channel VANET Providing Concurrent Safety and Commercial Services. In *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Cologne, Germany*, pages 1–9, September 2004.

[MML04] K. Matheus, R. Morich, and A. Lübke. Economic Background of Car-to-Car Communications. Symposium on Informationssysteme für mobile Anwendungen (IMA), Braunschweig, Germany, October 2004.

[Nak60] M. Nakagami. The m-Distribution, a General Formula of Intensity Distribution of the Rapid Fading. Statistical Methods in Radio Wave Propagation, W.C. Hoffman, Ed. Oxford, England: Pergamon, 1960.

[NoW] The NoW: Network on Wheels Project. http:// www.network-on-wheels.de.

[NS2] Network Simulator ns-2. http://www.isi.edu/nsnam/ns/.

[NSI06] T. Nadeem, P. Shankar, and L. Iftode. A Comparative Study of Data Dissemination Models for VANETs. In *Proceedings of the 3rd Annual International Conference on Mobile and Ubiquitous Systems (MOBIQUITOUS), San Jose, CA, USA*, July 2006.

[NTCS99] S.-Y. Ni, Y.-C. Tseng, Y.-S. Chen, and J.-P. Sheu. The Broadcast Storm Problem in a Mobile Ad Hoc Network. In *Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking (MobiCom), Seattle, WA, USA*, pages 151–162, August 1999.

[OS86] P.L. Olson and M. Sivak. Perception-response time to unexpected roadway hazards. *Human Factors*, 28(1):91–96, January 1986.

[PD03] L. Peterson and B. Davie. *Computer Networks: A Systems Approach (3rd Edition)*. Morgan Kaufmann, May 2003.

[PR99] C. E. Perkins and E. M. Royer. Ad-Hoc On-Demand Distance Vector Routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, USA*, pages 90–100, Februray 1999.

[PS02] S.-Y. Park and R. Sivakumar. Quantitative Analysis of Transmission Power Control in Wireless Ad-hoc Networks. In *Proceedings of the International Conference on Parallel Processing Workshops (ICPP), Vancouver, Canada*, page 56, August 2002.

[PS03] S.-Y. Park and R. Sivakumar. MobiHoc Poster: Adaptive Topology Control for Wireless Ad hoc Networks. *ACM SIGMOBILE Mobile Computing and Communications Review (MC2R)*, 7(3):37–38, July 2003.

[Rap02] T.S. Rappaport. *Wireless Communications*. Prentice Hall, second edition, 2002.

[RCCL06] C.L. Robinson, L. Caminiti, D. Caveney, and K. Laberteaux. Efficient Coordination and Transmission of Data for Cooperative Vehicular Safety Applications. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, USA*, pages 10–19, September 2006.

[RFC81] RFC 793 - Transmission Control Protocol, September 1981.

[RH05] M. Raya and J.P. Hubaux. The Security of Vehicular Ad Hoc Networks. In *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Alexandria, VA, USA*, pages 11–21, November 2005.

[RNT03] L. Romdhani, Q. Ni, and T. Turletti. Adaptive EDCF: Enhanced Service Differentiation for IEEE 802.11 Wireless Ad-Hoc Networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, LA, USA*, volume 2, pages 1373–1378, March 2003.

[RRR05] H.-J. Reumerman, M. Roggero, and M. Ruffini. The Application-Based Clustering Concept and Requirements for

Intervehicle Networks. *IEEE Communications Magazine*, 43(4):108–113, April 2005.

[SAE] Society of Automotive Engineers International (SAE). http://www.sae.org/.

[SELMTMH06] F. Schmidt-Eisenlohr, J. Letamendia-Murua, M. Torrent-Moreno, and H. Hartenstein. Bug Fixes on the IEEE 802.11 DCF module of the Network Simulator ns-2.28. Technical Report TR-2006-1, Department of Computer Science, University of Karlsruhe, January 2006.

[SETMMH07] F. Schmidt-Eisenlohr, M. Torrent-Moreno, J. Mittag, and H. Hartenstein. Simulation Platform for Inter-Vehicle Communications and Analysis of Periodic Information Exchange. In *Proceedings of the 4th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS), Obergurgl, Austria*, pages 50–58, January 2007.

[SETMT+06] F. Schmidt-Eisenlohr, M. Torrent-Moreno, T. Tielert, J. Mittag, and H. Hartenstein. Cumulative Noise and 5.9GHz DSRC Extensions for ns-2.28. Technical Report TR-2006-21, Department of Computer Science, University of Karlsruhe, October 2006.

[SFL+00] M. Sun, W. Feng, T. Lai, K. Yamada, and H. Okada. GPS-Based Message Broadcasting for Inter-vehicle Communication. In *Proceedings of International Conference on Parallel Processing (ICPP), Toronto, Canada*, pages 279–286, August 2000.

[SM00] J. Sucec and I. Marsic. An Efficient Distributed Network-Wide Broadcast Algorithm for Mobile Ad Hoc Networks. CAIP Technical Report 248, Rutgers University, November 2000.

[SMSA00] M.K. Simon and M.-S-Alouini. *Digital Communicaiton over Fading Channels: A Unified Approach to Performance Analysis*. John Wiley & Sons, Inc., 2000.

[STC+06] D. Sormani, G. Turconi, P. Costa, D. Frey, M. Migliavacca, and L. Mottola. Towards Lightweight Information Dissemination in Inter-Vehicular Networks. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, USA*, pages 20 – 29, September 2006.

[STMHE04] R. Schmitz, M. Torrent-Moreno, H. Hartenstein, and W. Effelsberg. The Impact of Wireless Radio Fluctuations on Ad Hoc Network Performance. In *Proceedings of the IEEE International Con-*

ference on Local Computer Networks (LCN), Tampa, FL, USA, pages 594–601, November 2004.

[TAF00] K. Tokuda, M. Akiyama, and H. Fuji. DOLPHIN for Inter-Vehicle Communications System. In *Proceedings of the IEEE Intelligent Vehicles Symposium (IVS), Dearborn, MI, USA*, pages 504–509, October 2000.

[TJM+04] V. Taliwal, D. Jiang, H. Mangold, C. Chen, and R. Sengupta. Poster Abstract: Empirical Determination of Channel Characteristics for DSRC Vehicle-to-vehicle Communication. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Philadelphia, PA, USA*, page 88, October 2004.

[TK75] F. Tobagi and L. Kleinrock. Packet Switching in Radio Channels: Part II–The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution. *IEEE Transactions on Communications*, 23(12):1417–1433, December 1975.

[TM07] M. Torrent-Moreno. Inter-Vehicle Communications: Assessing Information Dissemination under Safety Constraints. In *Proceedings of the 4th IEEE/IFIP Conference on Wireless On demand Network Systems and Services (WONS), Obergurgl, Austria*, pages 59–64, January 2007.

[TMB01] M. Takai, J. Martin, and R. Bagrodia. Effects of Wireless Physical Layer Modeling in Mobile Ad Hoc Networks. In *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MOBIHOC), Long Beach, CA, USA*, pages 87–94, October 2001.

[TMCSEH06] M. Torrent-Moreno, S. Corroy, F. Schmidt-Eisenlohr, and H. Hartenstein. IEEE 802.11-Based One-Hop Broadcast Communications: Understanding Transmission Success and Failure under Different Radio Propagation Environments. In *Proceedings of the 9th ACM/IEEE International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM), Torremolinos, Spain*, pages 68–77, October 2006.

[TMFH06] M. Torrent-Moreno, A. Festag, and H. Hartenstein. System Design for Information Dissemination in VANETs. In *Proceedings of the 3rd International Workshop on Intelligent Transportation (WIT), Hamburg, Germany*, pages 27–33, March 2006.

[TMJH04] M. Torrent-Moreno, D. Jiang, and H. Hartenstein. Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Philadelphia, PA, USA*, pages 10–18, October 2004.

[TMKH05] M. Torrent-Moreno, M. Killat, and H. Hartenstein. Broadcast Reception Rates and Effects of Priority Access in 802.11-Based Vehicular Ad-Hoc Networks. In *Proceedings of the 62nd IEEE Vehicular Technology Conference (VTC-Fall), Dallas, TX, USA*, volume 1, pages 319–323, September 2005.

[TMM06] M. Torrent-Moreno and J. Mittag. Poster Abstract: Adjusting Transmission Power and Packet Generation Rate of Periodic Status Information Messages in VANETs. In *Proceedings of the 3rd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Los Angeles, CA, USA*, pages 90–91, September 2006.

[TMSEFH06] M. Torrent-Moreno, F. Schmidt-Eisenlohr, H. Füßler, and H. Hartenstein. Effects of a Realistic Channel Model on Packet Forwarding in Vehicular Ad Hoc Networks. In *Proceedings of the IEEE Wireless Communication and Networking Conference (WCNC), Las Vegas, NV, USA*, volume 1, pages 385–391, April 2006.

[TMSH05] M. Torrent-Moreno, P. Santi, and H. Hartenstein. Fair Sharing of Bandwidth in VANET. In *Proceedings of the 2nd ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Cologne, Germany*, pages 49–58, September 2005.

[TMSH06] M. Torrent-Moreno, P. Santi, and H. Hartenstein. Distributed Fair Transmit Power Assignment for Vehicular Ad Hoc Networks. In *Proceedings of the 3rd Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Reston, VA, USA*, volume 2, pages 479–488, September 2006.

[Tsc91] C. Tschudin. Flexible Protocol Stacks. In *Proceedings of the Conference on Communications architectures and protocols (SIGCOMM), Zürich, Switzerland*, pages 197–205, September 1991.

[VII] Vehicle Infrastructure Integration (VII) project. http://www.its.dot.gov/vii/.

[VO07] R. Vuyyuru and K. Oguchi. Vehicle to vehicle Ad Hoc communication protocol evaluation using Realistic Evaluation Framework. In *Proceedings of the 4th IEEE/IFIP Conference on Wireless*

On demand Network Systems and Services (WONS), Obergurgl, Austria, pages 100–107, January 2007.

[VSC] Vehicle Safety Communications Consortium. http:// www-nrd.nhtsa.dot.gov/pdf/nrd-12/CAMP3/pages/VSCC.htm.

[WAV] 'WAVE' Radio Communicaiton Standard Announcement. http://standards.ieee.org/announcements/pr_P1609.0_new.html.

[WER05] L. Wischhof, A. Ebner, and H. Rohling. Information Dissemination in Self-Organizing Intervehicle Networks. *IEEE Transactions on Intelligent Transportation Systems*, 6(1):90–101, March 2005.

[WFGH04] H. Wu, R. Fujimoto, R. Guensler, and M. Hunter. MDDV: a Mobility-Centric Data Dissemination Algorithm for Vehicular Networks. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Philadelphia, PA, USA*, pages 47–56, October 2004.

[WR05] L. Wischhof and H. Rohling. On Utility-Fair Broadcast in Vehicular Ad Hoc Networks. In *Proceedings of the 2nd International Workshop on Intelligent Transportation (WIT), Hamburg, Germany*, pages 47–51, March 2005.

[Xiu04] W. Xiuchao. Simulate 802.11b Channel within NS2. Technical report, Communication and Internet Research Lab, University of Singapore, 2004.

[XMKS04] Q. Xu, T. Mak, J. Ko, and R. Sengupta. Vehicle-to-Vehicle Safety Messaging in DSRC. In *Proceedings of 1st the ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Philadelphia, PA, USA*, pages 19–28, October 2004.

[XYLW05] W.-Z. Song X.-Y. Li and Y. Wang. Efficient Topology Control for Wireless Ad Hoc Networks with Non-Uniform Transmission Ranges. *ACM Wireless Networks*, 11(3):255–264, May 2005.

[YEY+04] J. Yin, T. ElBatt, G. Yeung, B. Ryu, S. Habermas, H. Krishnan, and T. Talty. Performance Evaluation of Safety Applications over DSRC Vehicular Ad Hoc Networks. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks (VANET), Philadelphia, PA, USA*, pages 1–9, October 2004.

[ZC03] H. Zhu and I. Chlamtac. An Analytical Model for IEEE 802.11e EDCF Differential Services. In *Proceedings of the 12th International Conference on Computer Communications and Networks (ICCCN), Dallas, TX, USA*, pages 163–168, October 2003.

[Zha99] Q.T. Zhang. Maximal-Ratio Combining over Nakagami Fading Channels with an Arbitrary Branch Covariance Matrix. *IEEE Tranasactions on Vehicular Technology*, 48(4):1141–1150, July 1999.

[Zim80] H. Zimmermann. OSI Reference Model-The IS0 Model of Architecture for Open Systems Interconnection. *IEEE Transactions on Communications*, 28(4):425–432, April 1980.

Universität Karlsruhe (TH)
Institut für Telematik

ISBN: 978-3-86644-175-0

www.uvka.de