Data Dissemination in Vehicular Environments

Cristhian Iza Paredes

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Departament d'Enginyeria Telemàtica

Data Dissemination in Vehicular Environments

Design and performance evaluation of smart dissemination of emergence messages in vehicular ad-hoc networks

Cristhian Iza Paredes

Ph.D. Advisor:

Mónica Aguilar Igartua

Thesis submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Network Engineering
in the
Department of Network Engineering

Wednesday 11th April, 2018

To my family. For their unconditional love and support.

Acknowledgements

For her encouragement and patience, I would like to express my gratitude to my main supervisor, Prof. Mónica Aguilar Igartua. I appreciate all her contributions of time, ideas, and funding to make my Ph.D. experience productive and stimulating. If this thesis has any virtue is due, to a great extent, to her wise direction not being responsible, in any case, of the mistakes that this could contain and that Mónica sure tried to avoid. I also would like to thank Thomas Begin and Isabelle Guérin-Lassous, for their support during my stay in Lyon. It was a pleasure to work with them. I would like to thank all my colleagues for fruitful discussions and their assistance. Special thanks to the Smart Services for Information Systems and Communication Networks (SISCOM) and everyone involved for giving me priceless experiences. Finally, I thank my family and friends for their continued support and encouragement throughout my work on this project.

Cristhian Iza Paredes
May 2018

Abstract

The growing demand to improve road safety and optimize road traffic has generated great interest in vehicular ad-hoc network (VANETs). Serious traffic accidents can cause financial losses, physical disability, and even death. However, if drivers were informed about the danger in advance through a warning message, this would give drivers enough time to react appropriately to the situation. There are many approaches that can prevent car accidents, and VANETs have been conceived as an excellent solution to improve road safety, through the use of a variety of applications enabled by vehicle communications. The key objective of this research is to achieve information dissemination from a vehicle to other vehicles around that migth be interested in receiving the content. We focus on the network layer and application layer protocols, which are discussed and developed as a protocol over the respective access technologies. We primarily present the research results of our proposals, and also provide a comprehensive review of existing challenges and solutions in data dissemination in VANETs. Our proposals include the design of three dissemination protocols compatible with the IEEE 802.11p standards for road safety applications. These dissemination protocols can be differentiated by their application trigger condition and the broadcast scheme. All three dissemination protocols have been implemented in the simulator VEINS to perform several large-scale experiments. The results of the experiments have shown that all three dissemination protocols are able to cope with an increasing number of vehicles in large scale scenarios without suffering a noticeable loss in performance. Finally, we have investigated solutions to increase the driver's privacy because VANETs can also introduce some location privacy risk by periodically broadcast beacon messages that include the vehicle's position. We evaluate the performance of the privacy schemes, described the experiments and discussed the results.

Resumen

La creciente demanda para mejorar la seguridad vial y optimizar el tráfico vial ha generado gran interés en las redes vehiculares ad-hoc (VANETs). Los accidentes de tráfico graves pueden causar pérdidas financieras, discapacidad física e incluso la muerte. Sin embargo, si los conductores fueran informados por anticipado sobre el peligro a través de un mensaje de advertencia, esto daría a los conductores el tiempo suficiente para reaccionar de manera apropiada a la situación. Hay muchos enfoques que pueden prevenir accidentes automovilísticos, y las VANET se han concebido como una excelente solución para mejorar la seguridad vial, a través del uso de una variedad de aplicaciones habilitadas por las comunicaciones vehiculares. El objetivo principal de esta investigación es lograr la diseminación de la información desde un vehículo a otros vehículos que estén interesados en recibir el contenido. Nos enfocamos en la capa de red y los protocolos de capa de aplicación, que se discuten y desarrollan como un protocolo sobre las respectivas tecnologías de acceso. Principalmente presentamos los resultados de investigación de nuestras propuestas, y también proveemos una revisión exhaustiva de los desafíos y soluciones existentes en la diseminación de datos en las VANETs. Nuestras propuestas incluyen el diseño de tres protocolos de diseminación compatibles con los estándares IEEE 802.11p para aplicaciones de seguridad vial. Estos protocolos de diseminación se pueden diferenciar por la condición de activación de la aplicación, el patrón de recepción y el esquema de difusión. Los tres protocolos de diseminación se han implementado en el simulador VEINS para realizar varios experimentos a gran escala. Los resultados de los experimentos han demostrado que los tres protocolos de difusión son capaces de hacer frente a un número creciente de vehículos en escenarios de gran escala sin sufrir una pérdida notable en el rendimiento. Finalmente, hemos investigado soluciones para aumentar la privacidad del conductor porque las VANETs también pueden introducir algún riesgo de privacidad de la ubicación mediante mensajes beacon emitidos periódicamente que incluyen la posición de los vehículos. Evaluamos las prestaciones de los esquemas de privacidad, describimos los experimentos y discutimos los resultados.

Resum

La creixent demanda per millorar la seguretat viària i optimitzar el trànsit viari ha generat gran interès en les xarxes vehiculars ad-hoc (VANETs). Els accidents de trànsit greus poden causar pèrdues financeres, discapacitat física i fins i tot la mort. No obstant això, si els conductors van ser informats per endavant sobre el perill a través d'un missatge d'advertència, això donaria als conductors el temps suficient per reaccionar de manera apropiada a la situació. Hi ha molts enfocaments que poden prevenir accidents automobilístics, i les VANET s'han concebut com una excellent solució per millorar la seguretat viària, a través de l'ús d'una varietat d'aplicacions habilitades per les comunicacions vehiculars. L'objectiu principal d'aquesta investigació és aconseguir la disseminació de la informació des d'un vehicle a altres vehicles que estiguin interessats en rebre el contingut. Ens enfoquem en la capa de xarxa i els protocols de capa d'aplicació, que es discuteixen i desenvolupen com un protocol sobre les respectives tecnologies d'accés. Principalment vam presentar els resultats d'investigació de les nostres propostes, i també provem una revisió exhaustiva dels desafiaments i solucions existents en la disseminació de dades en les VANETs. Les nostres propostes inclouen el disseny de tres protocols de disseminació compatibles amb els estàndards IEEE 802.11p per a aplicacions de seguretat viária. Aquests protocols de disseminació es poden diferenciar per la condició d'activació de l'aplicació, el patró de recepció i l'esquema de difusió. Els tres protocols de disseminació s'han implementat en el simulador VEINS per a realitzar diversos experiments a gran escala. Els resultats dels experiments han demostrat que els tres protocols de disseminació són capaços de fer front a un nombre creixent de vehicles en escenaris de gran escala sense patir una pèrdua notable en el rendiment. Finalment, hem investigat solucions per augmentar la privacitat del conductor perquè les VANETs també poden introduir algun risc de privacitat de la ubicació mitjanant missatges beacon emesos periòdicament que inclouen la posició dels vehicles. Avaluem l'acompliment dels esquemes de privacitat, descrivim els experiments i discutim els resultats.

Contents

Part IV Annexes

List of Figures

List of Tables

Glossary

ABE	available bandwidth estimation
ADD	adaptive distributed dissemination
AI	artificial intelligence
AIFS	arbitration inter-frame spacing
AMD	adaptive multi-directional data dissemination
APAL	adaptive probability alert protocol
ATB	adaptive traffic beacon
ASS	anonymity set size
AVC	advanced video coding
BSM	basic safety message
BO	broadcast overhead
CAM	cooperative awareness message
CJ	critical junction
CCH	control channel
CRF	constant rate factor
CTS	clear to send
CW_{max}	maximum contention window
CW_{min}	minimum contention window
DE	dissemination efficiency
DSRC	dedicated short range communication
DV-CAST	distributed vehicular broadcast
ECPP	efficient conditional privacy preservation
EDCA	enhanced distributed channel access
EV	electric vehicle
EVCS	electric vehicle charging-scheduling
FCC	federal communication committee
FDR	frame delivery ratio
GPS	global positioning system
GoP	group of pictures
HEVC	high efficiency video coding
ITS	intelligent transport systems
JSF	junction store and forward
LQ	link quality factor
LTE	long term evolution

MAC	medium access control
ML	machine learning
MANET	mobile ad-hoc network
MOS	mean opinion score
NCP	number of collision packets
NSF	neighbour store and forward
NNPDA	nearest neighbour probabilistic data association
NJL	nearest junction located
PCA	principal component analysis
PDR	packet delivery ratio
PLR	packet loss ratio
PPC	periodical pseudonym change
PSNR	peak signal-to-noise ratio
QoS	quality of service
QoE	quality of experience
QP	quantization parameter
RCP	road casting protocol
RERs	Renewable Energy Resources
RoI	region of interest
RSP	random silent period
RSU	road side unit
RTS	request to send
SCH	service channel
SCF	store-carry-forward
SCCF	store-carry-cooperative forwarding
SG	smart grid
SNR	signal-to-noise ratio
SPC	slow pseudonym change
SUMO	simulation of urban mobility
TraCI	traffic command interface
TTL	time-to-live
UDP	user datagram protocol
UMTS	universal mobile telecommunications system
V2G	vehicle-to-grid
V2I	vehicle-to-infrastructure
V2N	vehicle-to-network
V2P	vehicle-to-pedestrian
V2V	vehicle-to-vehicle
VANET	vehicular ad-hoc network
VEINS	vehicles in network simulation
VoDi	volunteer's dilemma
WAVE	wireless access in vehicular environments
WHO	world health organization
WiMAX	worldwide interoperability for microwave access
WSMP	wave short message protocol

Part I
Initial research work

Chapter 1
Introduction

In recent years, vehicular ad-hoc networks (VANET) has become an area of intense investigation as part of the intelligent transportation system (ITS). VANET is one of the most actual and challenging research topic in automotive companies and ITS designers. In general, a VANET can offer a platform for issuing and exchanging emergency messages, extending the driver assistance through the development of active safety applications. This chapter first explains the basic definitions and concepts in data dissemination over VANETs. In Section 1.1, we identify the main types of communication in vehicular networks. In section 1.2, we outline application requirements for data dissemination in vehicular networks. Next, several advantages of vehicle-to-vehicle communications in specific scenarios are shown in section 1.3. In section 1.4, we identify the main challenges in our research. The motivation for this research is presented in section 1.5. The main objective and the main contributions are presented in section 1.6 and 1.7, respectively. Finally, contents and organization of this thesis are presented in section 1.8.

1.1 Vehicular communications

Vehicular communications are classified in the forms of intra-vehicle (InV), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P). In Figure 1.1, we can see how vehicular communications will enable a variety of applications for safety, traffic efficiency, driver assistance, as well as infotainment. An intelligent vehicular network is a network of vehicles that interact with each other and with an infrastructure to transmit and receive data. V2I communications need deployment of a telecommunication network infrastructure where some roadside units (RSUs) are distributed along the road, each one connected to other through a wired network. Because it is hard to deploy infrastructures over all roadways considering the financial aspects, another type of communication is

required. V2V communications allow a vehicle to communicate directly with another vehicle when there are no central infrastructures in the vicinity of vehicles. V2V communication provides fault tolerance in a highly distributed environment because of the highly-distributed nature of the network. [24]

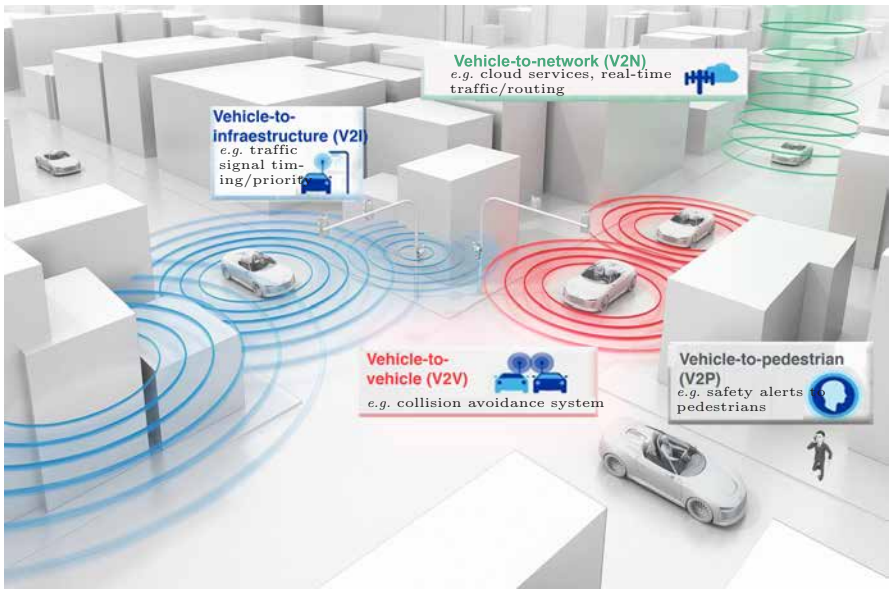


Fig. 1.1: Types of communications in vehicle networks

Vehicle communications are established through dedicated short-range communications (DSRC) devices installed in individual vehicles that allow high speed communications between vehicles and infrastructure. In October 1999, the Federal Communications Committee (FCC) in the United States granted the use of a frequency of 5.9 GHz with a broad spectrum of 75 MHz for DSRC with a provision for priority uses of public safety [66]. The purpose of DSRC is to provide high data transfers and low communication latency in a small communication area on vehicular networks. DSRC devices have a range of up to 1000 meters and after taking into account several obstacles in the transmission of messages, the range of wireless connectivity can be around 300 meters [47]. Therefore, communication over DSRC allows vehicles to exchange data with other vehicles that are outside the visibility distance and even line of sight. Vehicles can retransmit and forward messages to form a multi-hop network where the range of connectivity can go beyond the range of the radio [67]. The physical (PHY) and medium access control (MAC) layers for vehicular communication are specified in the IEEE 802.11p standard. The standard defines data rates from 3 to 27 Mbps. Efforts on the standardization of additional layers include the IEEE 1609 set of standards that specify the

multichannel operation, networking services, resource manager and security services. The combination of IEEE 802.11p and the IEEE 1609 protocol suite is denoted as wireless access in vehicular environments (WAVE) [15, 16].

1.2 Vehicular network applications

According to [99] the specific properties of VANETs allow the development of attractive new services related to road driving, which are divided into two categories:

Safety applications: This kind of applications increases the safety of passengers by exchanging relevant information among vehicles. The information is presented to the driver or is used for the active safety system of the vehicle itself. This type of applications is usually delay-sensitive. Thus, we can use vehicle-to-vehicle communication due to its low latency message delivery in local spread, as depicted in Figure 1.2.

Comfort applications: This type of application improves passenger comfort and traffic efficiency. Some examples of this category are road traffic, gas station location, gas station location, restaurant location, interactive communication (Internet access), among others.

A summary of the main applications of safety applications is presented in Table 1.1.

Safety Applications	**Features**		
	Communication	**Latency [ms]**	**Messaging Type**
Emergency Electronic Brake Lights	V2V	100	Event-triggered, time-limited broadcast
Slow Vehicle Warning	V2V	100	Periodic permanent broadcast
Pre-Crash Sensing	V2V	50	Periodic permanent broadcast, unicast
Lane Change Warning	V2V	100	Periodic broadcast
Intersection Collision Warning	V2V-V2I	100	Periodic permanent broadcast
Hazardous Location Warning	V2V-V2I	100	Event-triggered, time-limited Geocast

Table 1.1: Features of safety applications in vehicular networks [30]

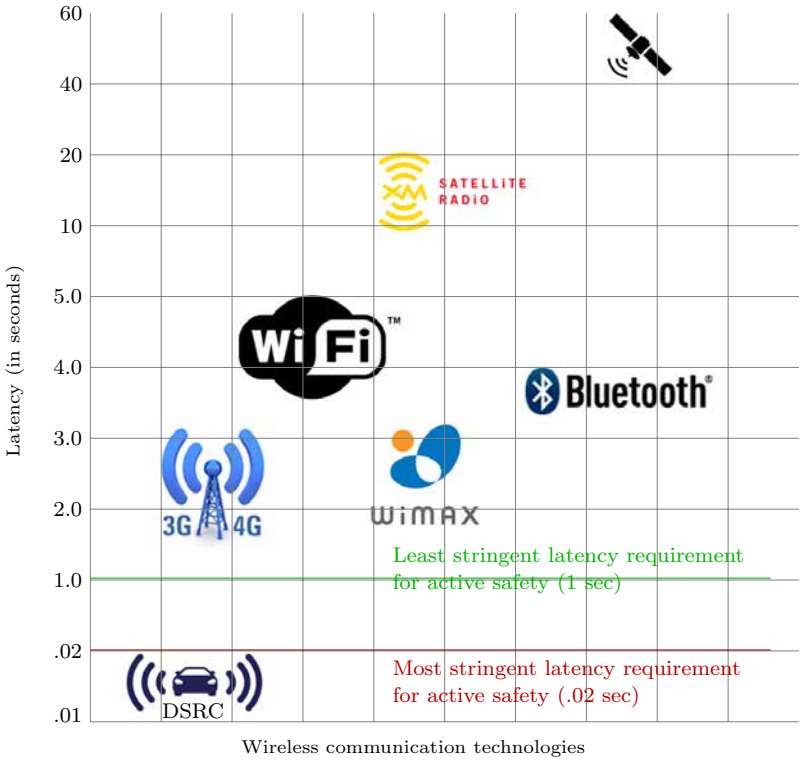


Fig. 1.2: End-to-end delay comparison between wireless communication technologies.

1.3 Advantages of vehicle-to-vehicle (V2V) communications

In the context of disseminating emergency messages on road safety applications, V2V communications have several advantages over conventional wireless networks. First, V2V communications have a low cost of implementation and maintenance compared to other wireless technologies such as Worldwide Interoperability for Microwave Access (WiMAX), Universal Mobile Telecommunications System (UMTS), and Long Term Evolution (LTE). Clearly, V2V does not require infrastructure or service provider, thus, service charges are completely avoided. Furthermore, V2V communications have lower local information dissemination time. This is corroborated by the end-to-end delay comparison between wireless communication technologies in Figure 1.2.

According to Table 1.2, since vehicles communicate directly without any intermediate base stations, V2V is suitable for the distribution of time-critical data such as emergency notifications in the area of an accident due to its low

delay and high data rate. Also, vehicles can communicate even in remote areas where other wireless technologies fail with their service [95]. Despite all these advantages, many factors (rapidly changing topology, signal shadowing from roadside buildings, intermittent connectivity) may interrupt the communication between vehicles. As a result, V2V communications could be used for local areas or as a component of other architectures.

Properties		**Approaches**		
		V2V	**V2I**	**UMTS-LTE**
Communication latency		Low	Medium	High
Link availability		Medium to High	Low	Low to Medium
Data rate		High	Medium to High	Low to Medium
System availability	Local	High	High	High
	Global	High	Low	Medium
Cost issue	Initial	Medium to High	High	High
	Operational	Null to low	Medium	Medium to High
Communication service area		Small to medium	Medium	Large
Exploit geographic relevance of data		Yes	No	No
Support for traffic safety applications		High	Low to Medium	Low

Table 1.2: Relative comparisons among communicating approaches [72]

1.4 Research challenges

The emergency message dissemination in VANET is a field of research that still contains many relevant unsolved problems. In this section we discuss specific challenges that are still left open. These challenges will be the focal points of our research. In environments of V2V communication, two approaches can be considered in order to disseminate emergency messages: **flooding** and **relaying**. The fundamental idea of flooding is to broadcast generated and received data by all vehicles. This approach usually is considered good for delay sensitive applications and suitable for sparse networks; however the main challenge is how to avoid the problem of broadcast storm[1] for dense networks (*e.g.*, traffic jam). On the other hand, the relaying scheme selects a forwarding vehicle (next hop). The relaying vehicle forwards data to the next hop, and it is repeated successively. Its main advantage is the reduction of contention allowing scalability in dense networks. With this approach, there are two challenges that can be found: how to select the relaying neighbours and how to ensure reliability. Several safety applications need solutions that provide emergency message dissemination to all vehicles within a certain

[1] severe contention at the link layer, packet collisions, inefficient use of bandwidth, and service disruption due to high contention.

area even though they are not connected. Unfortunately, network partition or topology fragmentation frequently occurs in vehicular environments due to sparse vehicle distribution, signal shadowing from roadside buildings or intersections. Consequently, the challenges of emergency message dissemination include the network partition, in addition to the broadcast storm and problems related to relaying. Moreover, we have contemplated the special case of disseminating video emergency messages, since the reception of an even light and short video clip, can give more information to the driver than a simple text message. The driver with a quick look can be better warned of the level of seriousness of the incident and take a proper action (e.g., turn to another road). Nonetheless, the transmission of video frames is more challenging than just send a text message, since the quality of the service has been met to ensure a certain quality of experience (QoE) of the end user that receives the video stream. Finally, a critical challenge is the privacy concerns of vehicular communication, where the identity, position, and movement track of vehicles should not be obtained by an unauthorized third party. In fact, a vehicle could be identified and tracked by eavesdropping its messages (*e.g.*, beacons) by an adversary.

1.5 Motivation of the Doctoral Thesis

Vehicular ad-hoc networks (VANETs) enable numerous applications to enhance traffic safety, traffic efficiency, and driving experience. Driving a vehicle is one of the most hazardous human activities. More than 1.25 million people die each year in traffic accidents worldwide, according to the Global Road Safety Report 2015 [2] released by the World Health Organization (WHO). The report also criticizes the fact that only 40 countries in the world sell vehicles that meet their safety requirements. While it is true that vehicles have brought comfort to people, there other worrying problems such as the increasing level of pollution and a lot of hours wasted in traffic jams. Against to those problems, VANETs have been deployed with the goal of enabling several applications to improve the level of traffic safety, to reduce the environmental impact of traffic, and to reduce congestion. Safety applications rely on broadcast algorithms and on routing protocols. These protocols have the task of disseminating emergency messages quickly and efficiently through the network. To achieve this goal, an efficient broadcast protocol specially designed for vehicular environments is needed. On the other hand, it is is obvious that any malicious behaviour of users could be fatal for other users. An adversary may trace a vehicle through information analysis. Since drivers are concerned about the leakage of the sensitive information to the public, the resolution of such concerns becomes one of the main problems in the design of VANETs.

1.6 Main objective

We focus our scope of research to the case of V2V communication, assuming the presence of vehicular networks without infrastructure. This is reasoned by the fact that, especially in roads and during deployment in the first phases in urban environments, it is desirable that solutions of disseminating emergency messages work in the absence of any support infrastructure. The main objective of this thesis is to evaluate and design solutions to disseminate emergency messages that fulfil the requirements of safety applications. Considering the scope depicted above, the main research question of this thesis is: *How to achieve smart dissemination of emergency messages for road safety applications in vehicular environments without infrastructure*?

1.7 Main contributions

The main contributions of this thesis can be summarized as follows:

- **Performance evaluation of dissemination protocols for emergency messages in vehicular ad-hoc networks**. We have identified the principal mechanisms of dissemination and have examined those factors that most impact on the simulation results. In addition, we have investigated the effects of the shadows of buildings and other vehicles in the performance of the dissemination protocols in urban scenarios. Simulation results suggest the need to include scenarios with fixed and mobile obstacles to increase the confidence of the performance results of the evaluated protocols.
- **Adaptive video-streaming dissemination in a realistic highway scenario**. We have proposed an efficient delay-based forwarding mechanism. It selects a set of forwarding vehicles with regard to the distances between the sender, the forwarder and the intersections formed by streets; as well as the link quality, including channel quality, signal quality, and collision probability. We have conducted simulations using real video traces to compare the performance between HEVC (High Efficiency Video Coding) codec and the previous AVC (Advanced video coding) codec in VANETs.
- **Game-theoretical design of an adaptive distributed dissemination protocol for VANETs**. We have proposed an adaptive distributed dissemination (ADD) protocol to perform data dissemination in VANETs. This approach lays out a decentralized stochastic solution for the data dissemination problem through two game-theoretical mechanisms. Given the non-stationarity induced by a highly dynamic topology, diverse network densities, and intermittent connectivity, a solution for the formulated game requires an adaptive procedure able to exploit environmental

changes. ADD is designed to operate without any roadside infrastructure in urban scenarios under diverse road traffic conditions.

- **Performance comparison of H.265/HEVC, H.264/AVC and VP9 encoders in video dissemination over VANETs**. In this work, we aimed to evaluate the efficiency of the video compression standards H.265/HEVC, H.264/AVC and VP9. Our interest is focused on using a video dissemination mechanism in an urban scenario where vehicles' traffic is relatively dense and the communications are more exposed to interferences and radio obstacles.
- **Performance evaluation of a location privacy system in VANETs** We have investigated solutions to increase the driver's privacy. Vehicles periodically broadcast their local knowledge to neighbouring vehicles. These messages typically contain plaintext information, such as vehicle's position and speed, which can be used by adversaries to determine which messages are from the same vehicle in order to track the vehicle. We have evaluated the performance of privacy systems such as temporary pseudonyms, time-varying pseudonym pools, and exchange of pseudonyms.

1.8 Contents and organization

The content of this document is organised into five chapters including this introductory chapter.

- Chapter 2 covers a literature review of main articles that present mechanisms specially designed to enhance message dissemination in vehicular communications. Also, We provide an overview of security and privacy issues in VANETs, as well as the challenges facing VANETs in addressing those issues.
- Chapter 3 presents a qualitative and quantitative evaluation of dissemination protocols. We describe a realistic framework and model structure for the evaluation of protocols in vehicular environments. The modelling framework is generalised to be expanded into an integrated approach in the future.
- Chapter 4 presents the diverse cross-layer metrics considered in our research proposals for data dissemination in urban scenarios.
- Chapter 5 introduces a delay based multi-hop broadcast called RCP+.
- Chapter 6 presents the proposal of two game-theoretical models to perform data dissemination.
- Chapter 7 evaluates the efficiency of the video compression standards H.265/HEVC, H.264/AVC and VP9 using RCP+ as a data dissemination protocol.
- Chapter 8 introduces the location privacy issue and outlines how the drivers' privacy can be increased.

- Chapter 9 presents a summary of the main contributions of this thesis. In addition, we point out some future work that can be done to continue our research work.

Chapter 2
Literature review

Data dissemination is one of the most indispensable requirements of several safety applications in VANETs. The algorithm used for data dissemination affects the message delivery ratio, transmission delay, and message communication overhead. The literature on the data dissemination solutions for vehicular environments needs to be reviewed to understand state-of-the-art practices and gain insights on the potential of the V2V technology to improve the performance of safety applications for VANETs. Data dissemination searches to alert drivers about any hazardous situation. A timely message disseminated can help other drivers around to avoid an accident on the road. In order to gain sufficient depth and clarity in the dynamics of this problem, we need to:

- Gain brief understanding of types of V2V applications.
- Review the associated standards.
- Review the features and characteristics of VANETs and their implications towards message dissemination.
- Discussion of the PHY layer, the MAC layer (as addressed in IEEE 802.11p), and the multi-channel coordination mechanism used.
- Review the challenges and existing schemes for robust message dissemination from the perspective of different protocol layers.
- Review possible security solutions, privacy systems and their impact on VANETs.

In this chapter, we review state-of-the-art solutions related to data dissemination in vehicular networks. First, we present an overview of message dissemination in VANETs in section 2.1. After, we discuss media access control for broadcast frames in section 2.2. Next, in section 2.3 we present different basic mechanisms that disseminate broadcast messages used at higher layers. Also, we investigate solutions to increase the driver's privacy in section 2.4. Next, we discuss different solutions designed for safety applications in section 2.5. Finally, section 2.6 closes this chapter with concluding remarks.

2.1 Data dissemination in vehicular ad-hoc networks (VANETs)

The most promising applications of VANETs are safety applications. All safety applications assume that exchanging messages come from an infrastructure or from the vehicles themselves. In this context, data dissemination typically refers to the process of spreading data over distributed wireless networks. According to [58], if we analyze the dissemination of messages from the networking point of view, it requires broadcast capabilities at the link layer, allowing a message to be transmitted to all the vehicles in the radio scope. It also assumes implementation of network mechanisms to disseminate the message in the whole network. The message will be disseminated in a multi-hop technique when V2V communications are enabled. Besides, the message will be broadcasted by all the RSU when V2I communications are used. Also, RSUs broadcast the messages to some selected vehicles to forward the message to complete the dissemination. These messages can be flooded at a certain number of hops or in a given area depending on the application purposes.

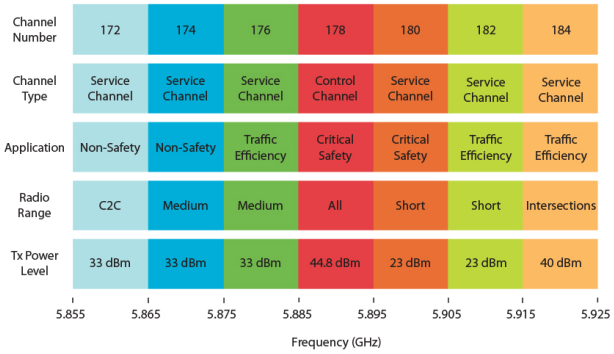
In safety applications for VANETs, vehicles broadcast two types of messages: critical and beacon messages. While critical messages usually contain safety-related information, beacon messages are periodically sent to all vehicles within the vehicle's range and contain vehicle's state information such as speed, acceleration, direction, and position. Safety-critical messages are being standardized for the dissemination of information when detecting dangers or abnormal situations. This type of messages is broadcast periodically at 1 Hz to 25 Hz in the form of basic safety messages (BSMs) [47] and cooperative awareness messages (CAMs) [39] in the U.S., and in Europe respectively. Beacon messages have to be sent with high frequency due to highly dynamic network topology to ensure up-to-date information [98]. Usually, emergent safety messages are generated occasionally but need a fast and guaranteed transmission. Therefore, this type of messages has a higher priority than beacon messages [35].

2.2 Broadcast in the link layer. IEEE 802.11p standard

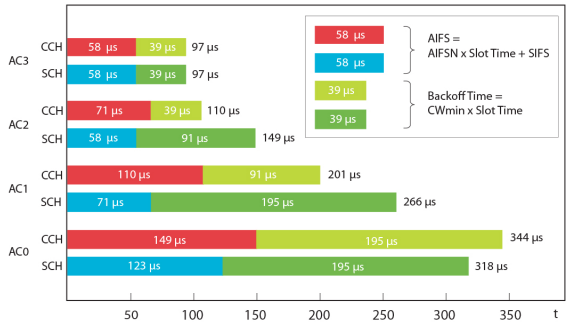
As noted in section 1.1, IEEE 802.11p/WAVE standard has a set of physical (PHY) and medium access control (MAC) layer specifications to enable communications in VANETs. The broadcast message is directly sent by the source vehicle to the vehicles in the radio range. In IEEE 802.11p, vehicles use a multichannel concept for the delivery of safety-related and infotainment applications (see Figure 2.1a). Each vehicle periodically switches on a common control channel to monitor control and warning messages, and tunes onto

one of the available service channels to exchange non-safety-related data. An important point of vehicular communications will be the prioritization of important safety- and time-critical messages over other messages. In fact, safety applications require higher priority with regard to non-safety applications in order to avoid their possible performance degradations. For this reason, IEEE 802.11p uses enhanced distributed channel access (EDCA) mechanism for coordinating channel access introducing quality of service (QoS) support. The medium access rules are defined by EDCA, where four different access categories (AC) are defined. Each regular data transmission will be assigned to an access class (AC), influencing its contention window, transmission opportunity limit, and the arbitrary inter-frame spacing (AIFS) to delay channel accesses. This way, it is more likely that higher-priority services will be able to access the channel [83]. Figures 2.1b and 2.1c give an overview of the EDCA architecture in vehicle communications. For a more in-depth discussion of MAC layer and scalability aspects of vehicular communication networks, the reader is referred to [37].

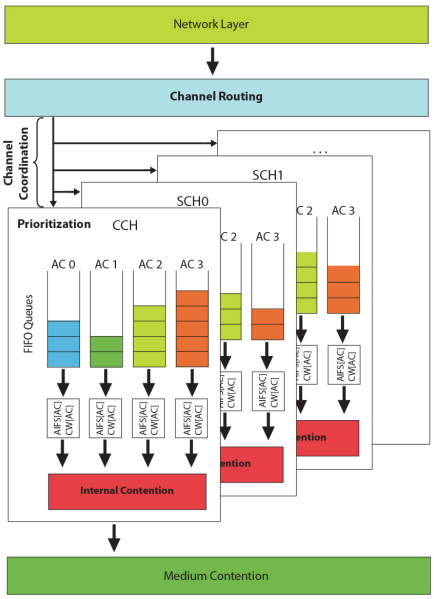
Providing reliable delivery of broadcast messages in a VANET introduces several key technical challenges. Authors in [63] provide some important challenges such as: lack of acknowledgment, contention window size, hidden terminal problem, and multi-hop broadcasts. First, no retransmission is possible for failed broadcast transmissions. A failed unicast transmission is detected by the lack of an acknowledgment (ACK) from the receiver. However, for a broadcasted frame, it is not suitable to receive an ACK from each vehicle receiving that frame. Indeed, if the receptions are acknowledged, each vehicle receiving the frame will send, almost at the same instant, an ACK back to the transmitting node. This process may lead to a high collisions rate when multiple receivers coexist [34]. Next, the contention window (CW) size fails to change because of the lack of MAC-level recovery. As a result, the CW is held constant for broadcast transmissions. This results in excessive collisions, if a large number of vehicles are contending for access. Likewise, the hidden terminal problem exists because of the lack of the RTS (request to send) and CTS (clear to send) exchange. This problem is the main cause of collisions in a wireless network. Finally, a simple approach, such a flooding a broadcast frame can result in a broadcast storm leading to a significant number of frames colliding and to a poor of the network resources. For all the above, we can conclude that MAC layer based on IEEE 802.11p/WAVE plays a key role for data access control channels on the channel access mechanism. Channel access mechanism is directly related to congestion, channel access delay and reliability particularly in case of broadcast messages. In this thesis, we concentrate on network-layer and application layer protocols, which are discussed and developed as a single protocol above the IEEE 802.11p/WAVE.



(a) Channel defined in the WAVE standard for multichannel operation in vehicular networks



(b) The arbitration inter-frame space durations used in the EDCA settings for IEEE 802.11p for different channel types and access categories.



(c) Scheme of enhanced distributed channel access (EDCA).

Fig. 2.1: Overview of IEEE WAVE and IEEE 802.11p [33].

2.3 Vehicular multi-hop broadcast. Basic techniques

As noted in the previous chapter, this research focuses on the dissemination of emergency messages in V2V mode. This kind of dissemination consists in selecting a pertinent set of vehicles to disseminate the emergency message and defining retransmission procedures to guarantee the entire safety applications requirements on reliability, delay, etc. In this section, we introduce the basic mechanisms used to disseminate messages to all the vehicles at several hops or in a certain geographic area. These mechanisms rely on the broadcast service offered by the IEEE 802.11p, and must consequently compensate its lack of reliability. These solutions are the basic mechanisms used in more complex dissemination protocols.

1. **Blind flooding scheme**. A straight-forward approach to perform broadcast is by flooding. This scheme works as follows: the first time a vehicle receives a broadcast message, it rebroadcasts it immediately, *i.e.* several vehicles rebroadcast the same messages with the same ID at the same time. Clearly, this costs n transmissions in a network of n vehicles.
2. **Counter-based scheme**. This scheme assumes that after a message reception, the vehicle has to wait for a while before its transmission. This delay is due to the back-off and MAC procedures or to a timer implemented by the protocol itself. Consequently, the vehicle senses the medium while it is waiting for the messages sent by its neighbours and counts the number of times it receives the same message. At the end of the waiting time, the vehicle rebroadcasts the message if it has received the message less than k times and discards it otherwise; k being a predefined threshold. The main benefit of this approach is that it bounds the number of transmissions and receptions whatever the vehicles' density is. The value of k may be chosen according to the aimed redundancy.
3. **Distance-based scheme**. This scheme uses the relative distance between vehicles to make the decision whether to drop the broadcast message or to rebroadcast it. This scheme works as follows: when a vehicle receives a message, it is able to measure the distance to the transmitter. It can be simply obtained from a global positioning system (GPS). The position of the transmitter is then included in the message and the distance computed as the difference between the receiver and the transmitter locations. In some cases, distance can also be evaluated from the radio signal strength of the received message at the receiver.
4. **Location-based scheme**. This scheme uses the relative location of broadcasting vehicles to make the decision whether to drop a rebroadcast or not. This scheme works as follows: Vehicles evaluate extra coverage area based on their location, if the additional area is greater than a threshold, a vehicle will rebroadcast the message; otherwise, it discards it. Such an approach may be supported by positioning devices such as GPS. In the context of VANET, this scheme is very similar to the distance based scheme. How-

ever, the additional coverage is difficult to estimate in practice, since it depends on the radio environment (fading, shadowing, etc.) which is not known by the vehicles.

5. **Neighbour knowledge scheme**. This scheme is implemented via periodic hello messages to determine whether to rebroadcast or not the message based on information gathered from the neighbours. Most protocols require vehicles to share 1-hop or 2-hop neighbourhood information with other vehicles.
6. **Probability scheme**. In this scheme, vehicles use probabilities in order to rebroadcast messages. In this case when a vehicle receives a message for the first time, it forwards it with probability P with $0 < P <= 100\%$. This mechanism limits the number of forwarders to a proportion P of the vehicles. When the probability is 100%, the scheme is equivalent to blind flooding. The selection of P is a design problem in this type of schemes.
7. **Cluster-based scheme**. In this scheme, the vehicles are divided into clusters and each one has a cluster head vehicle and a cluster gateway vehicle. Once created the clusters, the broadcasting algorithm will only allow the gateway or head using one of the earlier mentioned schemes: Probability, Counter, Distance, or Location, to retransmit emergency messages while the member will be inhibited from broadcasting, which minimizes broadcasts.

2.3.1 Store-carrry-forward mechanism

If vehicles are briefly disconnected, pure flooding approaches will never be able to disseminate messages successfully through the vehicles of the VANET. The approach to cope with disconnected networks is known as store-carry-forward (SCF). The main purpose of this mechanism is to assign selected vehicles the task of storing, carrying, and forwarding messages when new opportunities emerge. Many protocols for message dissemination complement their performance with store- carry-forward paradigm. However, this comes at a price of additional delay in message delivery due to the effect of message buffering. In this work, we will propose a novel scheme employing an SCF mechanism to tackle the network partition and broadcast storm problems, which are two major challenges in VANETs.

2.4 Security and privacy in VANETs

Because VANETs work in an open shared medium, illegal collection and processing of information is facilitated. Security is an important factor and confidentiality, integrity, availability, authenticity and non-repudiation are the

major security service requirements in vehicular networks [71]. In this sense, there are several possible security attacks in VANETs. Figure 2.2 summarizes several varieties of possible attacks in a vehicular network. Modern cryptography offers several security techniques to satisfy these security services such as encryption/decryption algorithms, keys generation and exchange protocols, hash functions, digital signature and a lot of other techniques.

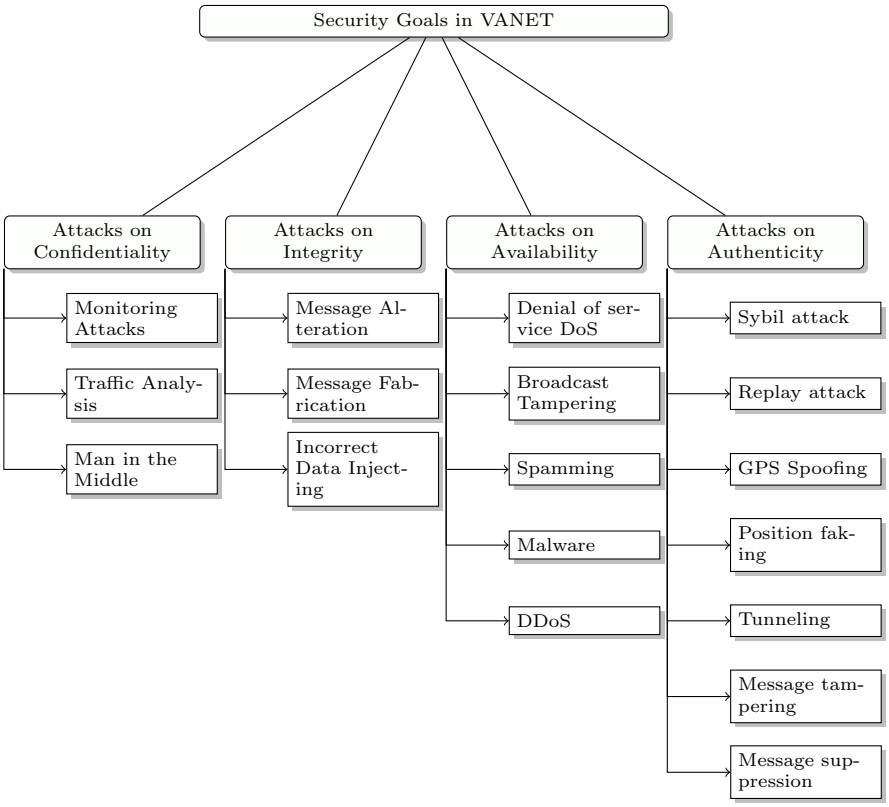


Fig. 2.2: Possible attacks on security goals in VANETs

According to [49] the specific requirements to protect VANETs against the threats presented in Figure 2.2 should satisfy the following security services:

1. **Availability**. The most dangerous attacks taking place in VANETs address availability. In the presence of an infrastructure both cryptography-based and trust-based approaches allow securing the network; however, trust-based approaches are better options for fully distributed scenarios.
2. **Authentication**. Message authentication is of vital importance in VANETs because it gives us an assurance that the information is gener-

ated by a legitimate and authorized vehicle in the network. It includes identification, authentication, and access control. Vehicle authenticity can be achieved by using cryptographic solutions.

3. **Integrity**. Data integrity and trustiness are about ensuring that information received has not been modified by any unauthorized user. It can be ensured through the public key infrastructure and cryptography revocation mechanisms.
4. **Confidentiality**. Sensitive data should not be accessed by an unauthorised user; however, in a VANET context, safety messages and neighbouring discovery messages should remain clear and readable by all receiving vehicles.
5. **Non-repudiation**. It is a critical property to prevent an authorized vehicle from denying the existence or contents of the message sent by itself. Digital signatures provide an effective solution to avoid this kind of attack.
6. **Privacy**. It is the ability to protect private information from an unauthorized party. In VANETs, security measure must ensure privacy of all genuine vehicles. The real identity of any individual vehicle is blind only to other vehicles and roadside units (RSU) but should be transparent to a trusted authority (TA). Pseudonym changing techniques are the main solution adopted to provide this security service.

Security Requirement	**Unicast**	**Broadcast**	**Security Mechanisms**
Privacy	☑	☑	Pseudonymity, ID-based system for user privacy
Authentication	☑	☑	Message signature
Integrity	☑	☑	Message signature
Confidentiality	☑		Encryption on sensitive messages
Authorization	☑	☑	Certificate and message signature
Availability	☑	☑	Pseudo-random frequency hopping Access control and signature-based authentication
Non-repudiation	☑	☑	Message signature

Table 2.1: Security requirements *vs.* V2X communication types.

Table 2.1 presents a summary of security mechanisms in response to security requirements and different vehicular communication types. Note that it is unnecessary to maintain the confidentiality of each broadcast message since everybody has the right to know the content of the message. Also, protecting the users' privacy such as driver-id, the license plate, position, and travelling routes needs something more than encrypting the data, indeed sophisticated mechanisms are required to conceal those users' attributes such as using a periodical pseudonym change approach. In this work, we focus on evaluating some privacy-preserving techniques.

2.5 Related work

In this section, we will explore some of the most important works that have been proposed in the literature. The main challenges in the dissemination of messages is maximising the packet delivery rate and minimising the average packet delay while keeping the channel at an acceptable level of congestion in dense or sparse networks. For instance, in [96], authors presented three techniques known as **Weighted *p*-Persistence**, **Slotted 1-Persistence** and **p-Persistence**. The overall objective of these solutions is to assign the highest relaying priority to the most distant vehicles in the direction of the message. In the Weighted p-Persistence scheme, the highest probability of retransmission is assigned to the farthest vehicles inside the communication range of the transmitter vehicle. In the Slotted 1-Persistence scheme, vehicles are allocated at different time intervals to wait before retransmission. Each time interval is calculated according to the number of intervals, the distance between vehicles (transmitter-receiver) and the transmission range. The farthest vehicles from the vehicle sender of the message have the highest priority and the shortest possible waiting time before retransmission. Slotted p-Persistence mixes probability and delay by giving vehicles with the highest priority the shortest delay and highest probability to rebroadcast. This would be an indication that the information has already been disseminated and redundant rebroadcasts can be suppressed. The proposed techniques are distributed and relay on GPS information, but they do not require any other prior knowledge about network topology.

Several dissemination protocols usually require external information about the network topology to select the vehicles to relay messages. For example, in [90] authors presented the protocol called DV-CAST. This protocol mitigates the broadcast storm and network partitions. The protocol uses the local topology information (list of neighbouring vehicles) as the main criterion for message relay. The diffusion process is adapted according to the density of neighbouring vehicles, their position and moving direction. If the local topology information has a high density of vehicles, DV-CAST applies the suppression of broadcast (Weighted p-Persistence). Conversely, if the vehicle density is low, this protocol uses the opportunistic forwarding mechanism known as store-carry-forward (SCF). This mechanism can take advantage of the mobility of vehicles to store and forward messages when vehicles are separated geographically.

Due to possible changes in direction of vehicles at intersections, it is not obvious which vehicles should be responsible for forwarding the warning message. Unlike highway scenarios, where the temporal relay node is usually the farthest vehicle travelling in the direction opposite to the message direction, the same method may not work in urban scenarios where vehicles can choose different directions of movement. Thus, protocols should take into account the challenges of dissemination in urban environments. For example, authors proposed a protocol called UV-CAST for urban areas in [93]. The protocol

uses digital map information to verify if it is at an intersection or not. The waiting time to relay the message is less at intersections. Once the timer expires the vehicle relays the message only if it does not receive duplicate messages, otherwise the relay is inhibited. Additionally, UV-CAST can assign to more than one vehicle the responsibility for opportunistic forwarding (SCF), so these vehicles can forward the message more than once.

Despite numerous dissemination protocols in the literature, there are only a few protocols developed to scale properly in various network densities in both realistic highway and urban scenarios. For example, authors in [81] presented a protocol called Adaptive multi-directional data dissemination (AMD). The protocol disseminates the message to multiple addresses, which are adjusted adaptively according to the local map and the GPS information. DV-CAST [90], UV-CAST [93] and AMD [81] handle a similar scheme that combines broadcast suppression and store-carry-forward technique, *i.e.* these proposals tackle the broadcast storm and the disconnected network problems simultaneously. According to the good results, this combination is an important basis for the development of new protocols for road safety applications.

Some dissemination protocols also adapt to the vehicles' density for message dissemination strategy. Indeed, in [74] authors presented two approaches for dissemination: Neighbour store and forward (NFS), a protocol for scenarios with low traffic density; and Nearest junction located (NJL), a scheme for vehicular scenarios with high density. Both protocols maintain a list of neighbours which is constructed by exchanging beacon messages. NJL is designed to relay the message only if the vehicle is the closest to an intersection. NSF is based on the mechanism of opportunistic forwarding. The region of interest (RoI) for disseminating emergency messages in an urban area is deepened in [101]. They propose the protocol called Road Casting Protocol (RCP). It is designed for sending emergency messages to a group of vehicles identified by the road segment on which they are located. Each emergency message receiver decides to forward the message based on the incident and the receiver's location relative to a point called Critical Junction (CJ). This point is an intersection beyond which a vehicle cannot avoid the blocked road segment. To select the vehicle to forward the message, the protocol is based on two factors: distance and link quality. The distance factor considers the position of vehicles (receiver - transmitter) and the next intersection. The link quality factor takes into account the signal quality, the channel quality and the probability of packet collision.

So far, all proposals assume the availability of global positioning system. However, some authors present solutions that do not use the information provided by the GPS. For example, in [89] authors presented a protocol called adaptive probability alert protocol (APAL). This protocol uses adaptive probability and time intervals to trigger retransmission. Another dissemination protocol that avoids the use of GPS is proposed in [59] where the nongeographical knowledge broadcasting protocol (NoG) is presented. This interesting proposal based on graph theory consists of three main modules:

A beacon mechanism, a broadcast mechanism and a waiting time mechanism. These latter mechanisms depend on the accuracy of the information provided by the beacons. For this, the authors incorporate a mechanism to adapt beacon frequency to the vehicular density.

On the other hand, we have analyzed some video warning message dissemination proposals. A video warning message provides an accurate overview of the emergency situation. However, the reliable dissemination of video content using multi-hop broadcast techniques also suffers of the broadcast storm problem and the interference from the existing periodic single-hop beacon messages. The main purpose of most articles on video transmission is entertainment on highways, so the video is streamed from road side units (RSU) to the vehicular network. However, we focus on urban scenarios where the vehicles' traffic is relatively dense and the communications are more exposed to interferences and fading phenomena. In this sense, authors in [22] proposed a rebroadcasters selection mechanism for video-streaming over VANET in urban scenarios. This solution selects a subset of vehicles to rebroadcast the content, based on their strategic location in the network and their capacity to reach a maximum amount of vehicles in a minimum number of hops. The recent adoption of high-efficiency video coding (HEVC) known as H.265 standard [4] provides many opportunities for new multimedia services in VANETs. For instance, one of the works where the use of H.265 codec was evaluated in VANET environments was presented in [91]. In this work, authors combined different flooding techniques and different video codecs to assess the effectiveness of long–distance real–time video-streaming. According to the results presented by the authors, H.265 shows to perform better than the H.264 codec, being more robust under high packet loss levels.

Although several published works addressed the problems of video content delivery in VANETs, few works have been reported on real–world measurements of visual quality for video. One of them is presented in [68] where authors propose a system called the see-through system (STS) that relies on VANET and video-streaming technology. The STS allows the overtaking vehicle to have the visual perspective of the road of the preceding vehicle, enhancing the driver's visual perception of vehicles traveling in the opposite direction lane. Authors also implemented a realistic driving simulator where the usability of the system is further evaluated.

During the past decade, game theory experienced a strong surge of interest in the area of wireless communications. Wireless networks have evolved enormously during this time, making game theory especially relevant in their analysis and design. Among all the protocols proposed in the literature, the most similar to the one presented in this work are detailed below. An optimized utility function based on distance and mobility was proposed in [79] for enhancing data dissemination in VANETs. A Nash bargaining proposal for data dissemination in VANETs was presented in [80]. A technique to mitigate the broadcast storm problem through a game-theoretical mechanism was proposed in [73]. With this mechanism, the forwarding probability is a

symmetrical game where all players compute an identical cost-benefit ratio. However, few researches can be found that address the asymmetric information as the basis for decision making; that is, all players compute a forwarding probability under different costs or utilities.

Privacy preservation is a very important design requirement for VANETs, where the source privacy of safety messages is envisioned to emerge as a key security issue because some privacy-sensitive information, such as the driver's name and car license plate, position, and driving route, could be intentionally deprived so that the personal privacy of the driver is compromised. In the following, we review the location privacy as a security objective as well as techniques to prevent tracking. Many pseudonyms changing strategies have been proposed to provide protection against the pseudonyms linking attack. The effectiveness of changing pseudonyms has been discussed in the literature. The main purpose of a pseudonym changing strategy is to determine where and when a vehicle should change its pseudonyms to achieve the unlinkability between them. For instance, a solution presented by Xiaodong Lin et al. [50] proposed an effective pseudonym changing at social spots (PCS) strategy for location privacy in VANETs. In particular, authors developed two anonymity set-analytic models in terms of anonymity set size (ASS) to formally analyze the achieved location privacy level, and they used game-theoretic techniques to prove its feasibility. Another solution is proposed by Xiaodong et al. [48], which addresses the use of the efficient conditional privacy preservation (ECPP) protocol for secure vehicular communications. The ECPP protocol can efficiently deal with the growing revocation list while achieving conditional traceability by the authorities. The proposed protocol can keep the minimal anonymous key storage without losing the security level. Meanwhile, this approach gains merits in the rapid verification of safety messages and provides an efficient conditional privacy-tracking mechanism. Various other effective works have been done to provide security and privacy solutions in VANETs, however, a realistic evaluation framework is still needed in order to facilitate evaluating the security and privacy impact whether on communication protocols or different applications.

2.6 Summary

In this chapter, some basic concepts of data dissemination in VANETs have been discussed. We have presented how broadcast is performed at the link layer to conclude that MAC layer based on IEEE 802.11p/WAVE plays a key role in data access control channels. Also, we summarize the basic schemes for the dissemination of messages. The privacy-preserving techniques also were discussed to increase the level of privacy. Finally, this chapter has presented a survey of relevant work in the area of data dissemination and privacy for VANETs.

Chapter 3
Performance evaluation of dissemination protocols for VANETs

One of the objectives of our research focuses on the evaluation of multi-hop dissemination protocols in VANETs. In this chapter, we evaluate the performance of several dissemination schemes that already have been published in the literature. We have selected some of the most representative dissemination protocols proposed in the literature for VANETs. Our work gives a qualitative assessment of the analysed protocols. For this, first we have summarized the main schemes used in dissemination of messages in VANETs. Next, we have used realistic scenarios which take into account the factors that most impact on the performance evaluation of dissemination protocols in VANETs. Finally, a quantitative evaluation of dissemination protocols are presented. The rest of the chapter is organized as follows: section 3.1 describes potential requirements for assessing the performance of vehicular networking protocols in realistic scenarios. Section 3.2 describes the qualitative analysis of the protocols. Afterwards, section 3.3 discusses the performance evaluation and includes the results of our analysis. Finally, section 3.4 presents a summary of this chapter.

3.1 Fair evaluation in realistic scenarios

The deployment and testing of VANETs involve high investments, and in most cases, it is economically prohibitively. For that reason, in the academic community communication protocols for vehicles are usually evaluated through simulation techniques. Many advances have been made toward making realistic simulations, but still, there are factors that are not usually taken into account in the simulations. According to the authors in [84], five factors have a strong influence on the quality of performance evaluation of protocols in vehicular environments:

1. A realistic mobility pattern of vehicles in the simulation.

2. A realistic scenario.
3. Realistic propagation models of the radio signal.
4. Appropriate evaluation metrics.
5. Realistic human driver behavior.

In this thesis, we selected VEINS [11] to carry out our simulations. VEINS is a simulation framework that couples the real-time network simulator OMNeT++ [8] with the mobility generator SUMO [10]. VEINS has important features such as simulation framework for vehicular networks, online reconfiguration and re-routing of vehicles, fully detailed models of the IEEE 802.11p standard, IEEE 1609.4 WAVE [16] supports realistic maps and realistic traffic. SUMO is capable of assuming a different motion to each vehicle to attain scenarios close to real environments.

The selection of the simulation scenario has a great influence on the results of a performance evaluation of vehicular communication protocols. The first step towards the definition of the scenario is the selection of the roads. To be as much realistic as possible, we use real maps extracted from OpenStreetMap [9] to prepare scenarios with highways and roads in urban environments.

One of the biggest challenges facing VANET networks in urban scenarios is the presence of buildings and other artificial structures that affect wireless connectivity. It is important that obstacles can be modelled in the simulation to obtain accurate results and to evaluate how the protocol takes special measures to overcome the building issue. Shadows in radio communication produced by buildings is an important factor for road safety-critical applications. In [83], authors presented a computationally affordable simulation model for obstacles with IEEE 802.11p in urban environments. It is an empirical model based on measurements of the real world, and it only considers the line of sight between transmitter and receiver. This model of obstacles is integrated with the framework of VEINS. Commonly available geodata is used to model buildings and the respective radio signal shadowing in vehicular network simulation; for instance, OpenStreetMap provides this kind of information.

The impact of shadows on the radio communication caused by vehicles was evaluated in [21]. The aim of the study was to show that the impact of the blockage of vehicles on the radio communications is not negligible. Based on this model, algorithm 1 shows how we have added an additional calculation of the attenuation due to vehicles in the framework of VEINS. To compute the impact of moving vehicles on the power loss, we employ a similar technique to the ones presented in [21] and [84]. The main purpose is to identify the group of vehicles (o_1, o_2.., o_n) that intersect the direct line of sight between two communicating vehicles o_s and o_r as it is shown in Figure 3.1. According to the International Telecommunication Union for radio communication (ITU-R) recommendations [14], the signal power loss ($L[dB]$) caused by an obstacle can be calculated using a *single knife edge* approximation which assumes a single sharp edge separates the transmitter and receiver. To make such calculation it is necessary to idealize the form of

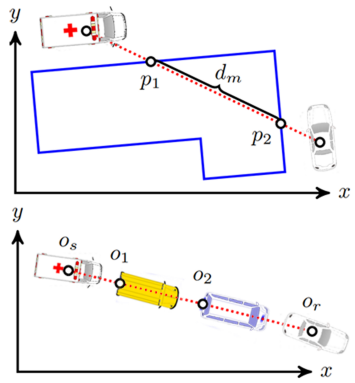


Fig. 3.1: Calculation of line of sight intersection points with building and vehicles [84]

obstacles. All the geometrical parameters are combined together in a single dimensionless parameter normally denoted by v. It is a geometrical parameter used to determinate how much of the *first Fresnel zone* is obstructed by the obstacle.

$$v = h\sqrt{\frac{2}{\lambda}(\frac{1}{d_1} + \frac{1}{d_2})} \tag{3.1}$$

where:

- h is the difference between the height of the obstacle and the height of the straight line joining sender and receiver.
- d_1 and d_2 are the distances from sender and receiver to the obstacle, respectively. We use the appropiate wavelenght (λ=0.05 m) for the standard for VANET communication which operates in the 5.89 GHz frecuency band.

In the implemented model in [14], power loss is assumed to only occur for a geometrical parameter of $v > -0,7$. In this case the loss is calculated by:

$$L[dB] = \begin{cases} 6.9 + 20log_{10}(\sqrt{(v-0.1)^2+1} + v - 0.1 \\ \text{for } v > -0,7 \\ \\ 0 \text{ ; otherwise} \end{cases} \tag{3.2}$$

This simple *single knife edge* method can be generalized to multiple obstacles.

On the other hand, one of the major problems when one wants to compare the performance of dissemination protocols is that researchers often use different metrics in assessing the performance of their protocols. In fact, they usually present the metrics which are advantageous to the proposed protocols, while other metrics are ignored. Thus, based on the results reported in

Algorithm 1 Attenuation(x,y)

```
1: for i=0 to r do
2:     [coord]=getInsersect(i)
3:     if size ([coord]) ≠ 0 then
4:         att = calcAddAtten([coord])
5:     else
6:         att = 0 dB
7:     end if
8: end for
```

the original documents, it is not possible to make a quantitative comparison among the different proposal effectively. Therefore, besides using conventional metrics, we assess the performance of protocols based on the unified metric presented in [70]. This metric is called dissemination efficiency (DE) and it is a measure that includes three separate domains (frequency, time and space) as it can be seen in Table 3.1. The DE metric is defined as:

$$DE = \frac{\text{Propagation Distance x Success Rate}}{\text{Propagation Time x Redundancy Rate}} \tag{3.3}$$

Intuitively, DE measures how far an information packet can propagate through the network per unit of time and per amount of overhead generated. The propagation distance is measured in meters, the propagation time is measured in seconds, the redundancy rate and the success rate are unit-less; therefore, DE has a unit of m/s.

Domain	Metric	Description	Favorable Value
Frecuency	Redundancy Rate	It measures the number duplicate packets per one source packet	Low
	Success Rate	It measures the proportion of vehicles that successfully receive the broadcast packets	High
Space	Propagation Distance	It measures the distance between the origin of the packet and the point where it is last received	High
Time	Propagation Time	It measures the time it takes a packet to traverse from a source to a specific point in the network	Low

Table 3.1: Metrics to calculate dissemination efficiency.

Finally, in most cases technical factors are not sufficient to globally evaluate a protocol for vehicular communications. A key component which is not very often found in the evaluation of protocols or applications traffic is the interaction of the system with human behavior, *i.e.* the driver. Although this problem can be critical for accurate and realistic assessment of performance, in this research, we have assumed that drivers act exactly as expected or as suggested by the road safety application.

3.2 Qualitative assessment

In this section, some of the protocols to disseminate messages are analysed and compared qualitatively. Table 3.2 presents a qualitative comparison of solutions for message dissemination in VANETs. The comparison is based on three sets of criteria: *forwarding strategy, scenarios and assumptions*. First, the forwarding strategy is an approach assigning the duty of relaying a packet to a specific node or nodes that satisfy some criteria. As it can be inferred it generates less contention and it is scalable for dense network condition. The main challenges faced in the relay-based approaches include selecting the relay node and ensuring reliability. Basically, the relay-based data dissemination approaches can be divided into two categories: simple forwarding and map-based forwarding exploiting GPS and digital map information. Network fragmentation may happen due to the low market penetration rate at least at the early stages of introducing the technology or due to low traffic density periods. Therefore, this issue is addressed in some of the research efforts and data dissemination approaches are proposed such that continuous network connectivity cannot be guaranteed. Next, the scenario approach categorizes protocols based on operating environments of each solution. Most of the data dissemination protocols were deployed to operate solely in highways or in urban scenarios. Finally, assumptions identify external sources of information used by each protocol for operation. In VANETs, vehicles get useful information by communicating with each other or with an RSU. It is easy to obtain the locations of a vehicle by GPS technology. However, there still are some unexpected problems such as not always being in signal coverage or the signal not being strong enough for some applications. It is necessary to develop additional localization techniques to overcome GPS limitations. Despite the vast number of proposals, only a few surveys exist on beaconing approaches. Adaptive beaconing approaches can efficiently utilize the wireless channel and provide reliable vehicular communications. In Table 3.2, we summarize the main characteristics of each analysed protocol. It can be noted that all these protocols basically use the same mechanisms for selecting nodes to forward the message: position, counter, distance, probability, waiting time, local topology and store-carry-forward. These protocols are mainly focused on reducing latency and the mitigation of broadcast storms. Nevertheless, the results are limited to simulations with unrealistic scenarios where all protocols achieve high performance. We consider that these protocols should be evaluated under more realistic scenarios to reach a fair assessment.

Protocols V2V	Forwarding strategy								Scenario		Assumptions		
	Position based	Counter based	Probabilistic based	Distance based	Local topology based	Delay based	Tall based	Store carry forward	Highway	Urban	GPS	Adaptive beaconing	Neighbours info
Slotted p-Persistence [96]	✓		✓	✓		✓					✓		
Slotted 1-Persistence [96]	✓			✓		✓					✓		
Weighted p-Persistence [96]	✓		✓	✓		✓					✓		
UV-CAST [93]	✓			✓	✓	✓		✓		✓	✓		✓
DV-CAST [90]	✓		✓	✓	✓	✓		✓	✓		✓		✓
AMD [81]	✓			✓	✓	✓		✓	✓	✓	✓		✓
NSF [74]						✓		✓		✓	✓		✓
NJL [74]	✓			✓		✓				✓	✓		✓
JSF [74]	✓	✓		✓		✓		✓		✓	✓		✓
RTAD [77]	✓	✓				✓					✓		✓
RCP [101]	✓			✓		✓				✓	✓		
APAL [89]		✓	✓			✓						✓	
NoG [59]	✓					✓						✓	✓

Table 3.2: Classification of message dissemination protocols.

3.3 Quantitative assessment

In this section, a performance assessment of dissemination protocols is carried out by means of simulations. Our goal is to study the dissemination of emergency messages under urban realistic scenarios. We first present the simulation setup used including models and scenarios. Then, we analyse the dissemination of messages applied by several selected protocols.

3.3.1 Simulation setup

To carry out the performance of the analysed dissemination schemes, we use VEINS [11]. This framework builds on the MiXiM framework physical layer model, which allows the implementation in the simulator of the building and vehicle shadowing models discussed in section 3.1. We have provided each run with a different random scenario that fulfills the requirements of the study. For each point in all figures we have calculated the average from 10 simulation runs. This let us obtain a standard error less than 5% in a 95% confidence interval. The packet error and medium access control (MAC) layer models adopted are based on the IEEE 802.11p, using a data rate of 6 Mbit/s, a transmission power of 20 mW, and a receiver sensitivity of -94 dBm. For eliminating effects caused by switching channel between the control channel (CCH) and the service channel (SCH), we changed the model to use only the CCH. In addition, all beacons use the same access category best effort (AC_BE), which results in the contention window (CW) and arbitration interframe spacing (AIFS), parameters presented in Table 3.3.

For all simulation scenarios, the data message size is 2,312 bytes, *i.e.* the maximum allowed by the IEEE 802.11p standard. This allows us to evaluate the protocols in the worst-case scenario in terms of medium occupation caused by the transmission of messages. Beacons are sent at the frequency of 1 Hz. In order to study realistic vehicle-caused radio shadowing, we used a typical mix of different vehicles (90% cars and 10% trucks). Only trucks can attenuate or even block the signal generated from cars. All vehicles are moving according to the SUMO standard Krauss driver model.

3.3.2 Scenario description

We focus on the immediate consequences of an accident. The crashed vehicle starts to generate and transmit an emergency message after the collision to inform neighbouring vehicles as quickly as possible in a distributed way. In the simulations, we used a real city area obtained from Barcelona, Spain as our urban scenario (see Figure 3.2a). This segment has an area of 1.5 x 2km^2 and

	Parameter	Value
Physics and MAC Layers IEEE 802.11p	Channel	Channel 178, 5.89 GHZ
	Bandwidth	10 MHz
	Transmission range	230m
	Transmission power	20 mW
	Sensitivity	-94 dBm
	Obstacle model	Defined in [21], [84]
	CWmin, CWmax	15,1023
	AIFSN	2
	Bit rate	6Mbit/s
Broadcast Supression mechanism	τ	5ms
	N_s	3
	tmax	500ms
	Beacon frecuency	1 Hz
	Beacon size	>=32 bytes
Scenarios	Data Message size	2312 bytes
	Number of Runs	10
	Time to live (TTL)	90s
	Vehicles' density	20 - 300 (veh/km2)

Table 3.3: Simulation parameters.

was retrieved from OpenStreetMaps [9]. A vehicle positioned approximately at the center of the network is responsible for generating a single message to be disseminated in a time to live (TTL) of 90s.

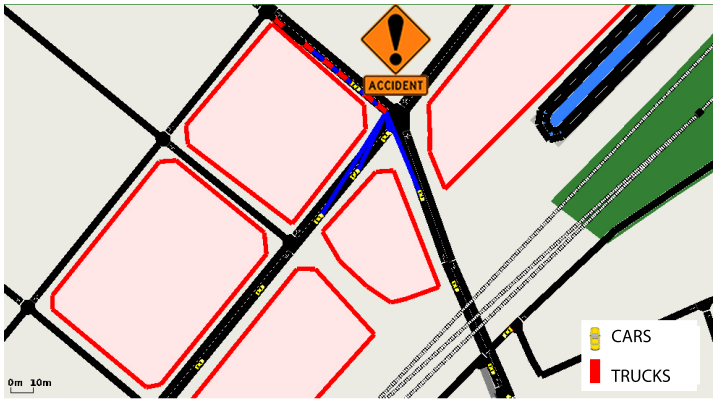
Shadowing models are used to reproduce the attenuation of a radio signal induced by obstacles, such as buildings or other vehicles blocking the direct line of sight. Figures 3.2a and 3.2b show the map section considered, where buildings represented by pink rectangles are radio obstacles. For all the experiments, the results for the three types of shading models are presented: clearances (F), shadow building (B), shadow buildings + shadow vehicles (B+V):

- Clearances (F): Assuming free-space propagation, path loss is estimated by taking the distance to the receiver and the wavelength.
- Shadow building (B): Shadowing caused by buildings. The main idea is to count the number of exterior walls of a building to approximate the impact of the radio-signal shadowing caused by exactly this building.
- Shadow buildings + shadow vehicles (B+V): The impact of radio-signal shadowing caused by buildings and other vehicles.

3.3.3 Metrics

We use four metrics to evaluate each message dissemination protocol: packet delivery ratio, average delivery ratio, total transmitted messages and dissemination efficiency.

(a) Urban scenario: a 1.5x2 km^2 region of the city of Barcelona, Spain.



(b) Traffic in urban areas with shadows on the radio communication.

Fig. 3.2: Screenshots of simulators' graphical user interfaces running network and road traffic simulations in parallel.

Packet Delivery Ratio (*PDR*): It indicates the percentage of nodes that received a single emergency message within a specified period.

Average Packet Delay (*APD*): It provides the indication of how soon the message can be delivered to the intended receiver. This is an important metric for emergency messages where messages must be disseminated as rapidly as possible.

Transmitted Messages (*TM*): It is the total number of data messages disseminated by all vehicles in the network.

Dissemination Efficiency (*DE*): It measures how far an information packet can propagate through the network per unit of time and per amount of overheads generated.

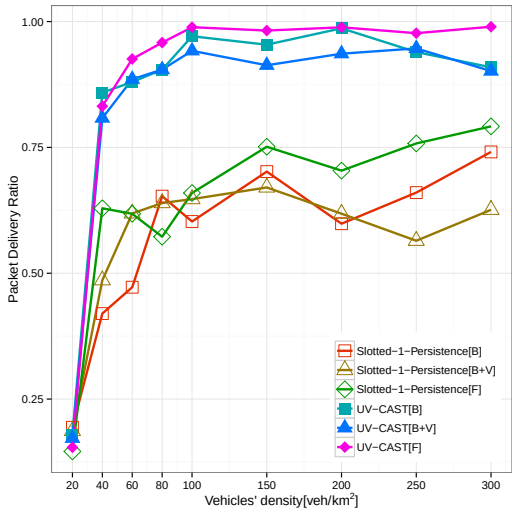
3.3.4 Simulation results

In this section, we present some representative simulation results. We select two state-of-the-art protocols for comparison, called: UV-CAST [93] and Slotted 1-Persistence [96]. Although this comparison might seem unfair because of the features of each protocol, we have prepared a testing platform to evaluate message dissemination protocols in realistic scenarios. To do so, we have implemented the code of both protocols in the VEINS simulation framework.

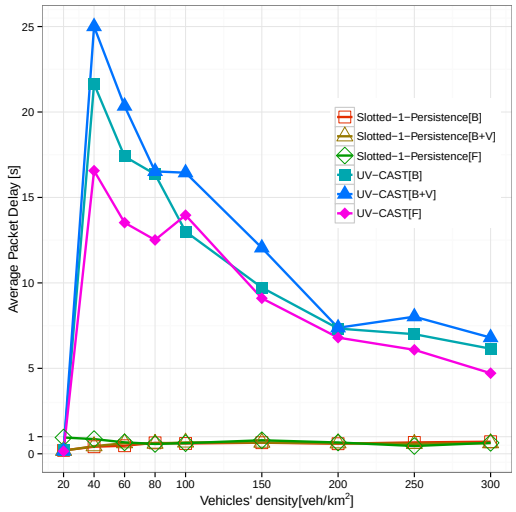
Slotted 1-Persistence is a mechanism of suppression of broadcast storms. The broadcast coverage is spatially divided into regions (slots), and a shorter waiting time is assigned to the nodes located in the farthest region. Each node uses the GPS information to calculate the waiting time to retransmit. To alleviate the broadcast storm this scheme inhibits retransmissions in some vehicles to reduce redundancy and therefore the contention and collisions. We define a number of slots N_s= 3. UV-CAST is a protocol that specifically addresses urban scenarios. It combines a suppression technique for dense networks that gives higher priority to vehicles near intersection points and mechanisms to select vehicles to store, carry, and forward packets. The vehicular density varies from 20 to 300 vehicles/km^2.

In the first set of experiments, we evaluated the performance of the packet delivery ratio. Figure 3.3a shows the packet delivery rate for three radio shadowing models. In the case of free space (F), UV-CAST achieves successful delivery rates close to 100% above 100 vehicles/km^2. The protocol uses only a subset of vehicles the task of opportunistic forwarding (store-carry-forward). Thus, uninformed vehicles that do not find a vehicle from this subset will not receive the disseminated message. It is clear the poor performance of Slotted-1-Persistence for low traffic density (3 inferior lines in Figure 3.3a). This result is expected because this protocol was designed for high-density scenarios. However, Slotted-1-Persistence only reaches delivery rates under 80%. As this protocol does not have a mechanism for opportunistic forwarding, dynamic topology networks in VANET causes temporary disconnections, interrupting the dissemination and compromising the delivery of the messages. Additionally, the results presented in Figure 3.3a corroborate the impact that buildings and high vehicles have as obstacles in the line of sight in both protocols. There is a difference on average of 3% between packet delivery rate in free space (F) and delivery rate with shadows of buildings (B). This difference achieves on average 7% if buildings and high vehicles (B+V) are considered. Although we expected a more noticeable difference, we believe that the ability of the dissemination protocols conceals a greater impact of the shadows from buildings and high vehicles.

In a second step, we investigated the performance of latency. Figure 3.3b shows the average packet delay to deliver the message for the three radio shadowing models. In the case free space (F), the lower delay (lower than 1s) for UV-CAST when the traffic is 20 vehicles/km^2 is because it fails to deliver



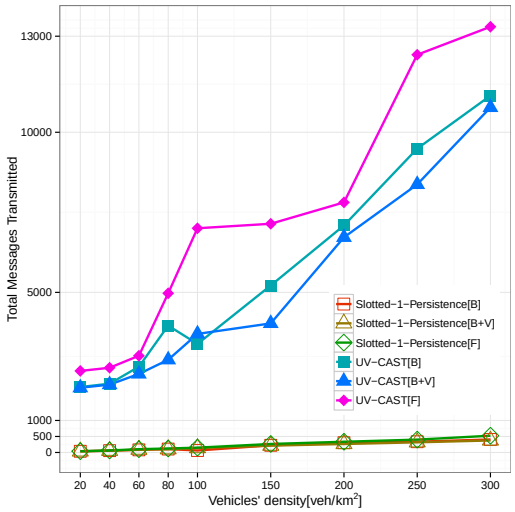
(a) Packet delivery ratio



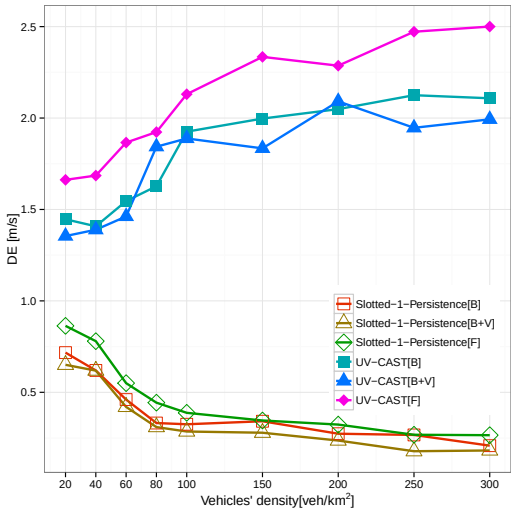
(b) Average packet delay

Fig. 3.3: Results with 95% confidence intervals for different network densities in an urban scenario.

the message to almost all vehicles of the region of interest as it was shown in Figure 3.3a. The higher delays for UVCAST under low traffic densities (*i.e.*, equal or lower than 150 vehicles/km^2) are explained by the store-carry-forward mechanism used by the protocol. As the traffic density increases,



(c) Total messages transmitted.



(d) Dissemination Efficiency.

Fig. 3.3: Results with 95% confidence intervals for different network densities in an urban scenario (cont.)

the delay decreases, since the message can be rapidly disseminated through direct relaying, thus requiring less the use of the store-carry-forward mechanism. Similarly, the results presented in Figure 3.3b confirm the impact that buildings and high vehicles have as obstacles in the line of sight in UV-

CAST protocol. There is a difference between average packet delay in free space (F) and delivery rate with shadows of buildings (B). This difference is more pronounced if buildings and high vehicles (B+V) are considered. If the scenario is densely congested, the beacon messages have shorter range, *i.e.* the number of vehicles that are able to receive beacons is affected by radio signal shadowing. Let us remember that the UV-CAST operation is based on information provided by the beacon messages, thus UV-CAST loses robustness. It is important to say that the low average packet delay (lower than 1s) of Slotted-1-Persistence is because it does not perform the tasks of store, carry and forward. Its performance is limited to direct relay through the dissemination of multi-hop, which can be done very quickly.

As a next step, we evaluate the number of messages transmitted for the three radio shadowing models in Figure 3.3c. In the case free space (F), a large number of messages transmitted by UV-CAST (3 lines at the top of the Figure 3.3c), especially at high densities. This behavior is particularly expected because UV-CAST uses beacon messages for information on traffic density. Also, because informed vehicles immediately forward the emergency message when they receive a beacon message from a neighbour node without the message. This results in redundant retransmissions, contention and many lost packets, which explains the high number of transmissions. Similar to the previous metrics, there is a difference between total messages transmitted in free space (F), shadows of buildings (B) and shadows of building and high vehicles (B+V). In those cases, the impact of the radio signal shadowing models provides opportunities due to a reduced channel load. This is evidenced by the decrease in the number of messages transmitted. The low number of messages transmitted (lower than 500) in Slotted-1-Persistenc (3 lines at the bottom at Figure 3.3c) is because the protocol does not use beacons and because it has not the mechanism of opportunistic forwarding.

Finally, in Figure 3.3d the average values for the dissemination efficiency (DE) are presented for the three radio shadowing models. As it can be seen in the case free space (F), DE values in the Slotted-1-Persistence protocol (3 lines at the bottom at Figure 3.3d) decrease in higher traffic density. Although Slotted-1-Persistence was designed for high densities, the short propagation range and its high rate of packet losses do not allow to get a better performance. In contrast, we can see that in the case of UV-CAST (3 lines at the top of the Figure 3.3d), DE values have a tendency to grow at high density. Undoubtedly opportunistic forwarding mechanism allows achieving a higher propagation distance and a higher delivery rate in comparison to Slotted-1-Persistence. Therefore, opportunistic forwarding performs better in the dissemination. This metric confirms that the dissemination is affected by the patterns of shadows (B and B+V). Consequently, we can see that dissemination efficiency is a metric that allows a clear view of the performance of a dissemination protocol.

The main limitation of many protocols is the long time delay caused by the long waiting time before each retransmission. The time delay also increases

when vehicles drive away from the desired path or when messages are kept around an intersection hoping to find a vehicle driving toward the destination.

3.4 Summary

In this chapter, a taxonomy of the main characteristics of the dissemination protocols has been presented. We have also conducted a qualitative evaluation of two relevant data dissemination mechanisms in different scenarios on a realistic evaluation platform of VANETs. We considered the effects of radio-signal shadowing caused by buildings and other vehicles. Comparative results of the quantitative assessment based on traditional evaluation metrics have been presented, and we have also included a special metric that reflects an overall performance of each protocol. Using this knowledge, we believe that an efficient data dissemination technique for VANETs can be devised on a realistic simulation platform. Future simulation will be carried out in a realistic urban scenario with obstacle modelling.

Chapter 4
A cross-layer routing strategy

At a high-level, the cross-layer design refers to a protocol design that exploits the dependency between protocol layers to achieve desirable performance improvements. In traditional routing schemes, each layer optimizes itself without considering limitations from other layers. However, with the development of new applications and services, the efficiency of these models lags behind the acceptable Quality of Service (QoS) standards. In order to meet such QoS standards, this chapter proposes a cross-layer routing paradigm for VANETs. Our approach considers the dynamic system conditions for VANETs and the routing optimisation takes place across multiple layers simultaneously. Our proposal combines the parameters from physical, MAC, and network layers to take poper routing decisions to select the best forwarding vehicles. The rest of the chapter is organized as follows: section 4.1 describes in a general way our approach. Section 4.2 presents the multimetric score to select forwarding vehicles. Finally, section 4.3 presents a summary of this chapter.

4.1 Cross-layer design approach

In our cross-layer routing strategy, we extract parameters from multiple layers in the protocol stack. Since the performance seen at the level of application depends on the parameter settings of all downstream layers, it is often desirable to jointly optimize the parameters from all downstream layers. According to authors in [87], the dynamic optimization requires constant information update across layers to ensure accuracy. Protocols often maintain a repository to store the information that is shared among layers. It is evident that implementation of the cross-layer protocols could require additional processing or storage capabilities. Unlike other ad-hoc networks, vehicles can afford to carry high-performance processing units, accommodate large memory spaces and are connected to virtually unlimited power sources.

4.2 Multimetric score to select forwarding vehicles

In the following, we present the diverse metrics considered in our research proposals for data dissemination in urban scenarios. These metrics use information from the Physical and MAC layers.

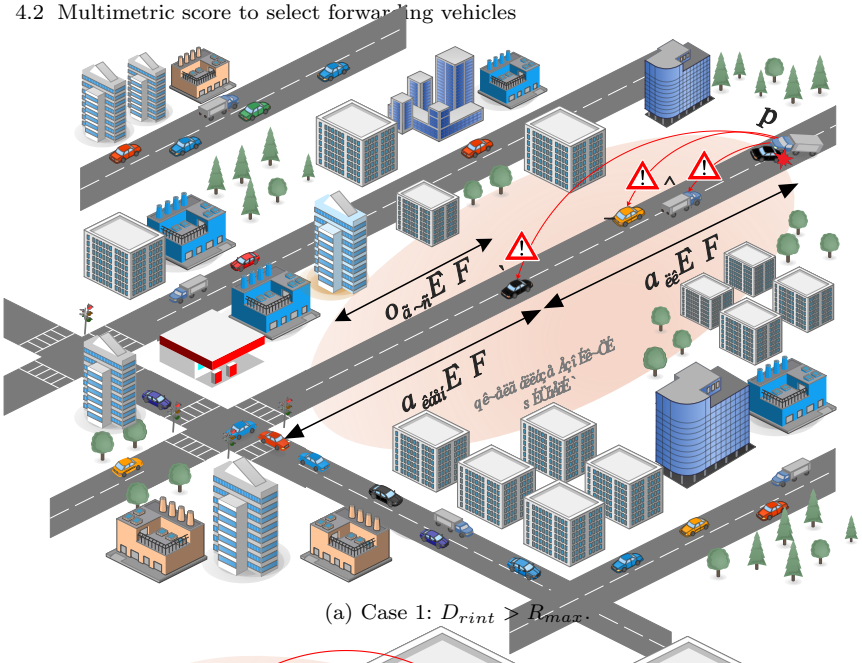
4.2.1 Distance factor (α_2, Df_i)

The distance factor is adapted to the information provided by the neighbour discovery process as well as to the information provided by the own GPS device. Thanks to the information gathered by beacon messages, the distance source-receiver D_{sr} between transmitter and receiver can be calculated. On the other hand, the information provided by GPS allows us to know the receptor-intersection distance D_{rint} to the next nearest intersection. If the receiving vehicle is not located over an intersection, the distance factor Df_{i} is calculated as the ratio between D_{sr} and the transmission range R_{max}. With this, the farthest vehicle from the sender has assigned the highest distance factor. On the other hand, if the receiving vehicle is located over an intersection, the distance factor Df_i is calculated as a decreasing function of the distance D_{rint}. This way, the lower D_{rint}, the higher its Df_i which means that the vehicle is a good candidate to broadcast the message. The distance factor is summarized in Equations (4.1a) and (4.1b).

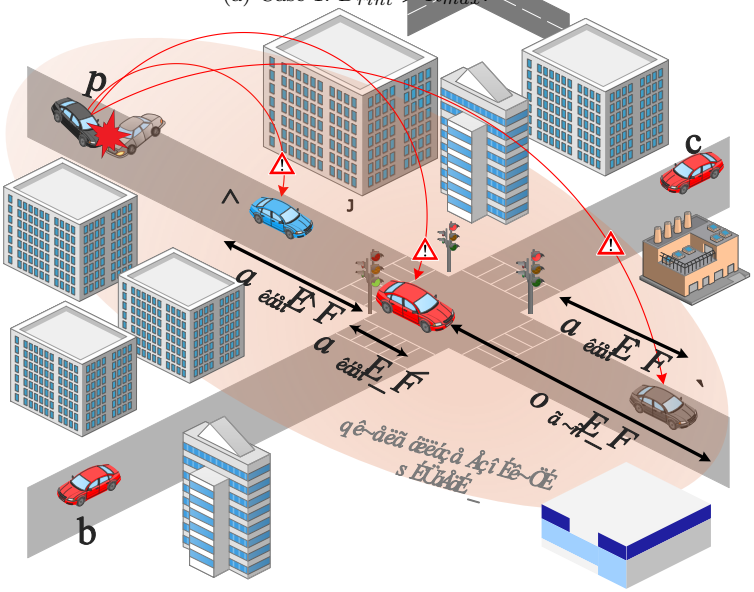
$$Df_{\mathrm{i}} = \begin{cases} \dfrac{D_{sr}}{R_{max}} & \text{,if } D_{rint} > R_{max} \quad (4.1a) \\ 1 - \dfrac{D_{rint}}{D_{rint}+1} & \text{,otherwise} \quad (4.1b) \end{cases}$$

where D_{sr} is the relative distance between source s and receptor r vehicles, $D_{\mathrm{r}int}$ is the relative distance between vehicle r and the next nearest intersection, and R_{max} is the transmission range.

As it can be seen in Figure 4.1a, vehicles A, B, and C do not have intersections within their transmission range R_{max}. In this case, the vehicles receiving the message compute the distance factor according to Equation (4.1). Thus, vehicle C which is farther from the sending vehicle S will be assigned the highest distance factor without taking into account its distance to the intersection, according to Equation (4.1)a. On the other hand, Figure 4.1b presents the scenario when the vehicles receiving the message have intersections within their transmission range. In this case, vehicles A, B, and C compute the distance factor according to Equation (4.1)b. Hence, vehicle B that is crossing the intersection is assigned the highest distance factor.



(a) Case 1: $D_{rint} > R_{max}$.



(b) Case 2: $D_{rint} \leqslant R_{max}$.

Fig. 4.1: Distance factor Df_i.

4.2.2 Link quality factor (α_2, LQf_i)

It is a function of the signal quality (sq_i), the channel quality (cq_i) and the collision probability (cp_i). The vehicle i receiving the message attains those parameters from its physical layer and MAC layer following a cross-layer design. The Link Quality factor is calculated as follows:

$$LQf_i = 0.5 \cdot sq_i + 0.5 \cdot cq_i \cdot (1 - cp_i) \tag{4.2}$$

This way we equally add the effects of the signal quality and the channel being free of collision.
The **signal quality** sq_i aims at ensuring the integrity of the received message in vehicle i, and it is calculated as follows:

$$sq_i = \begin{cases} \max(0, Sf_{\mathrm{iRSS}} \cdot (1 - \frac{1}{SNR_{\mathrm{i}}}) \cdot (1 - V_{\mathrm{i}})) & \text{, if } SNR_{\mathrm{i}} > 0 \\ Sf_{\mathrm{iRSS}} & \text{, otherwise} \end{cases} \tag{4.3}$$

where V_{i} is the ratio between the relative velocity (between the transmitter and the receiver of the warning message) and the maximum allowed velocity in the considered urban scenario. The velocity of the vehicle i is an influencing parameter in signal quality because the communication link with a vehicle moving at a very high relative speed is less stable than with a vehicle moving at the lower relative speed. Therefore, vehicles moving at high relative speed will obtain low values of sq_{i}. SNR_{i} is the ratio between the signal power and the noise intensity of the i-th receiver. Note that those vehicles which are farther from the sender will have lower SNR_{i}. Sf_{iRSS} is the received signal strength in vehicle i bounded by 1 and it is defined using the following equation:

$$Sf_{\mathrm{iRSS}} = \begin{cases} \min(1, \frac{RSS_{\mathrm{i}} - RSS_{\mathrm{th}}}{RSS_{\max} - RSS_{\mathrm{th}}}) & \text{, if } RSS_{\mathrm{i}} \geq RSS_{\mathrm{th}} \\ 0 & \text{, otherwise} \end{cases} \tag{4.4}$$

where RSS_{i} is the received signal strength, RSS_{th} is a threshold below which the received signal is considered too weak and $RSS_{\max}$ is the maximum value of the received signal strength.
The **channel quality** (cq_{i}) is defined in Equation (4.5) as an estimation of the state of the channel around the receiving vehicle i at the time of reception of the message and it is calculated using the Number of Successful Transmissions (nst) and the Number of Overall Transmissions (not) in a window time. The Number of Successful Transmissions (nst) is a statistical parameter that represents packets that were successfully processed on the MAC layer, that is to say, packets that do not suffer biterrors or collisions.

$$cq_{\mathrm{i}} = \begin{cases} \frac{nst_{\mathrm{i}}}{not_{\mathrm{i}}} & \text{, if } not_{\mathrm{i}} > 0 \\ 0 & \text{, otherwise} \end{cases} \tag{4.5}$$

The **collision probability** (cp) is defined in Equation (4.6) as an estimation of the likelihood of a collision occurrence if the message is forwarded by the receiver vehicle i. It is calculated using the channel occupancy time (cot) and a fixed window time (wt) in which the channel is observed. The channel occupancy time is computed by the MAC layer, which gives us the accumulated time that the channel was busy at the time of the query t.

$$cp_{\mathrm{i}}(t) = \frac{cot_{\mathrm{i}}(t)}{wt(t)} \tag{4.6}$$

4.2.3 Available bandwidth estimation

We have considered the ABE proposal presented in [78] as one solution to estimate the available bandwidth in the link formed by two sender-receptor vehicles. $ABE_{(\mathrm{s,r})}$ aims to provide an accurate estimation of the available bandwidth in the link formed between two neighbour nodes s and r, which can be estimated by the following equation:

$$ABE_{(\mathrm{s,r})} = (1 - K_{\mathrm{ABE}}) \cdot (1 - cp) \cdot T_{\mathrm{s}} \cdot T_{\mathrm{r}} \cdot \ C_{\mathrm{ABE}} \tag{4.7}$$

where K_{ABE} is the proportion of bandwidth used by the back-off scheme which is estimated with Equation (4.8), cp is the collision probability measured on the received $Hello$ packets and it is computed with Equation (4.6). T_s is the idle time period at the sender side and T_r is the idle time period at the receiver node, and C is the maximum medium capacity on link (s, r).

$$K_{\mathrm{ABE}} = \frac{DIFS + \overline{backoff}}{T_{\mathrm{m}}} \tag{4.8}$$

where T_m (in sec.) is the time elapsed between the emission of two consecutive frames, $DIFS$ (Distributed Coordination Function Interframe Space) is a fixed interval and $\overline{backoff}$ is the mean backoff used to transmit a single frame.

4.3 Summary

The dynamic nature of VANETs suggests using more number of routing parameters to understand and calculate a reliable routing path. In this chapter, we have detailed each one of the cross-layer metrics included in our research

proposals. The use of these metrics is a way to improve the choice of the next forwarding node. The impact of various routing metrics such as a distance factor, channel quality, link quality, signal quality, collision probability, available bandwidth estimation and node density on forwarding decision will be used in a systematic framework to make an effective forwarding decision.

Part II
Proposals developed

Chapter 5
Road Casting Protocol (RCP+)

5.1 Introduction

The use of VANET might provide advance warnings to enhance automotive safety. Furthermore, with the rapid development of standards such as Dedicated Short Range Communications (DSRC) [57], IEEE 802.11p [94], and IEEE 1609 Wireless Access in Vehicular Environments (WAVE) [16], VANETs are becoming a reality. As a result of that process, this technology has received an extensive attention in the research community and is targeted to support new services, including on-road multimedia safety security and entertainment video flows both in urban environments such as highways. Despite their technical feasibility and significant benefit-cost ratios, there are several challenges involved in developing and deploying VANETs. For instance, a high-speed mobility of vehicles in highways and the medium nature of wireless communications pose many challenges that should be solved before deploying multimedia applications. Indeed, the speed limit on the highways is usually higher than speed in streets within the city. There are also more lanes. This means, there is more traffic on highways than in cities going at faster speeds. On the other hand, one of the main challenges in video broadcasting is to design a framework able to successfully transport video frames from limited sources to the receiver ends, through a high-corruption probability channel inherent in VANETs. Video coding is a key solution to meet this challenge. The recent adoption of High-Efficiency Video Coding (HEVC) known as H.265 standard [4] provides many opportunities for new multimedia services in VANETs. The new standard achieves notable advances in compression and has a high impact on coding efficiency. HEVC intends to replace the widely used Advanced Video Coding (MPEG-4 AVC) [88] and provides an opportunity for video dissemination in critical contexts. In the light of the aforementioned challenges, this chapter proposes an adaptive mechanism to improve the resilience of video dissemination over VANETs in highways. The main contributions of this proposal can be summarized as follows:

- A delayed forwarding mechanism, so a set of forwarder vehicles are selected.
- An algorithm able to give each metric a proper weight.
- Evaluate our proposal for video warning message dissemination using real video traces to compare the performance between HEVC [4] codec and the previous H.264 [88] codec in VANETs.

The rest of the chapter is organized as follows: section 5.2 describes the features of our proposal. Afterwards, section 5.3 discusses the performance evaluation and includes the results of our analysis. Finally, section 5.4 presents a summary of this chapter.

5.2 RCP+ protocol description

This section describes the proposed mechanism called RCP+ to optimally select next forwarder vehicles based on information of the environment and an estimation of the congestion of the communication channel. The main goal of the RCP+ mechanism is to improve the quality of experience (QoE) for end-users. At the same time, it avoids unnecessary network overhead, preserving scarce wireless resources.

5.2.1 Assumptions

We assume that each vehicle is equipped with a GPS device to obtain its geographical location in current time. A preloaded digital map provides information about roads. This assumption is valid since most of the current vehicles are already equipped with this kind of systems. Besides, we assume that vehicles periodically exchange their own physical location, moving velocity and direction information enclosed in their periodic beacon messages. Finally, vehicles are assumed to be equipped with IEEE 802.11p wireless technology and computation capabilities.

5.2.2 RCP+ adaptive video streaming scheme

Figure 5.1 gives an overview of the WAVE (Wireless Access in Vehicular Environments) [15] protocol stack. In addition to the traditional IEEE 802.11 stack components, Internet protocols and WSMP (WAVE Short Message Protocol) [16], RCP+ has been located on top of UDP layer. The adaptive video stream scheme RCP+ includes three main modules: neighbour discovery, relay selection, and video quality strategy.

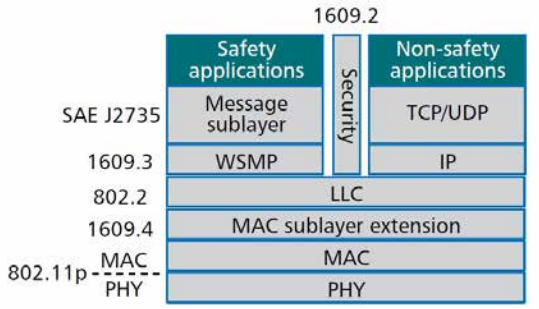


Fig. 5.1: The WAVE Stack.

5.2.2.1 Neighbour discovery

The neighbour discovery mechanism estimates the local topology by monitoring periodic beacon updates received from one-hop neighbours. Each vehicle periodically announces its status to all its one-hop neighbours by broadcasting a beacon packet. These packets carry the current location of the node which is acquired from the GPS. The periodic broadcasting of beacon packets is a default operation provided in the IEEE 802.11p protocol for service announcements. Moreover, each vehicle maintains a neighbour table. It records the status of its one-hop neighbours by listening to beacon messages within its coverage range. The recent beacon time field records the time when a recent beacon packet from a neighbour is received. If the elapsed time has a duration twice the length of one beacon interval, that neighbour is supposed to be moving away and it is removed from the neighbours' table.

5.2.2.2 Relay selection

Relaying is an approach assigning the duty of forwarding a message to specific node or nodes that satisfy some criteria. This challenge can be resolved if a random waiting time is assigned to each vehicle located within the relaying area. The vehicle with the shortest waiting time then retransmits the message. Vehicles that receive a safety message should not rebroadcast it immediately; the responsibility of broadcasting should be assigned to the relaying node. After the waiting time expiration, the next forwarder vehicle rebroadcasts the safety message, and any of its neighbours that hears this duplicate rebroadcast, with regard to the recently received safety message, will cancel its message-rebroadcast process.

5.2.2.3 Multimetric score to select forwarder vehicles

In the following, we present the diverse metrics considered to compute a multimetric score to assist the selection of the forwarder vehicles.

The protocol developed by Zemouri [101] introduces the selection of the next forwarders which is performed in a decentralised manner, as each receiver of a safety message calculates a probability, which will determine its Backoff period (*i.e.*, waiting time before retransmitting the received message) according to the following equation:

$$WT = CW \cdot (1 - p) + \delta \tag{5.1}$$

Where WT is the Backoff value, CW is the contention window multiplied by the time slot, p is the calculated probability, and δ is a random value in microseconds, smaller than one time slot. The vehicle with the shortest waiting time will forward the message first. If a vehicle overhears the same message before the end of its own waiting time, that vehicle will consider it as an acknowledgement for the last message it received and will omit the re-transmission process. Note that the vehicle having the highest probability will be assigned the shortest Backoff period. Inspired by this proposal, we have adapted the calculation of probability as a function that combines several parameters obtained from our simulation framework and thus from the considered VANET real scenario.

Unlike the work developed by Zemouri [101] and based on our previous work [55], we have developed an algorithm to compute the weights of the Distance factor (D) and the Link Quality factor (LQ) (both described below) as a function of the variation of the values of the normalized metrics with respect to the average of those values. This gives proper weights to each metric. We obtain the re-transmission probability as a weighted sum of the Distance factor (D) and the Link Quality factor (LQ). It is calculated as follows:

$$p = LQ \cdot \mathrm{W_{P_1}} + D \cdot \mathrm{W_{P_2}} \tag{5.2}$$

Where LQ is the Link Quality factor, D is the Distance factor and $\mathrm{W_{P_1}}, \mathrm{W_{P_2}}$ are the computed weights. LQ and D are factors described in chapter 4, Eq. 4.2 and Eq. 4.1 respectively

Algorithm to update the weights of the metrics. We proposed in [55] an algorithm to compute the weights of the metrics as a function of the variation of the values of the normalized metrics with respect to the average of those values. For the calculation of the weights in Eq. (5.2), let us denote R as the variation made in each $\mathrm{T_{beacon}}$ seconds (each i iteration) for each metric such as:

$$R = \begin{cases} R_1 = \left| \frac{LQ_{\mathrm{i}} - A_{\mathrm{LQ}}}{LQ_{\mathrm{i}}} \right| \\ \\ R_2 = \left| \frac{D_{\mathrm{i}} - A_{\mathrm{D}}}{D_{\mathrm{i}}} \right| \end{cases} \tag{5.3}$$

where LQ_{i} and D_{i} are the current value for each metric in each $\mathrm{T}_{\mathrm{beacon}}$ seconds, A_{LQ} and A_{D} are the average value for each metric. All values entries are maintained based on their age using a timer T, which can be considered as an *age threshold*: below the threshold T, the information is considered to be up-to-date, whereas any value of the metrics set older than T are discarded. After that, we have a vector $R = [R_1; R_2]$. Suppose that the maximum value found in vector R is $[R_{1\max}; R_{2\max}]$. Now, we bound vector R to be between 0 and 1 and this new vector is named S.

$$S = \begin{cases} S_1 = \frac{R_1}{R_{1\max}} \\ S_2 = \frac{R_2}{R_{2\max}} \end{cases} \tag{5.4}$$

Therefore, the new normalized vector weights for the metrics is $\mathrm{W_P}$.

$$\mathrm{W_P} = \begin{cases} \mathrm{W_{P_1}} = \frac{S_1}{S_1 + S_2} \\ \mathrm{W_{P_2}} = \frac{S_2}{S_1 + S_2} \end{cases} \tag{5.5}$$

5.2.2.4 Video quality strategy

The latest versions of JM [88] and HM [4] reference software models were used for encoding video sequences with H.264/AVC and H.265/HEVC. As a strategy for maintaining high-quality video, we evaluate two coding parameters: the Constant Rate Factor (CRF) and the encoding mode. First, CRF is the quality setting for the encoder. The range of the quantizer scale is 0-51: where 0 is lossless, 28 is the default, and 51 is worst possible. A lower value is a higher quality (at the expenses of higher file sizes) and a subjectively sane range is 18-28.

$$\underbrace{0}_{\text{best, lossless}} \leftarrow 18 \leftarrow 23 \rightarrow 28 \rightarrow \underbrace{51}_{\text{worst}} \tag{5.6}$$

CRF is a way of compressing video dynamically, adapting the compression ratio to the motion characteristics of the video. We use this parameter to encode our test video because our objective is to retain good visual quality and do not care about the exact bitrate or filesize of the encoded file. Second, we have used two different encoding modes: All Intra (AI) and Low-Delay-P (LP). In AI mode, every frame of the video sequence is encoded as an *I frame i.e.* it is coded without any motion estimation/compensation. As reported in the HEVC standard [23], AI mode is a fast coding process because no time

Vehicle Type	**Maximum Speed** $[m/s]$	**Lengh** $[m]$	**Height** $[m]$	**Probability** %
Slow Car	25	5	2	5
Car	33	4	2	69
Fast Car	39	4	3	1
Bus	25	12	3.4	15
Truck	25	12	4	10

Table 5.1: Vehicle types and associated probability in highway.

Capacity	**Detail**
5 Vehicles/km/lane	Represents a free-flow operation. Vehicles are practically free in their ability to maneuver within the traffic stream.
10 Vehicles/km/lane	Represents reasonably free-flow operation. The ability to maneuver within the traffic stream is slightly restricted.
15 Vehicles/km/lane	Represents a traffic flow with speeds near or at free-flow speed of the freeway. Ability to maneuver with the traffic stream is noticeably restricted.
20 Vehicles/km/lane	Represents speeds that begin to decline with increased density. Ability to maneuver with the traffic stream is noticeably limited.
25 Vehicles/km/lane	Represents operation at its capacity. Vehicles are closely spaced with the traffic stream and there are virtually no useable gaps to maneuver.

Table 5.2: Values for highway capacity.

is wasted in motion estimation; however, this mode gets lower compression rates because P-frames and B-frames can usually obtain better compression rates than I-frames at the same quality level. Applications that require a fast encoding process fit perfectly in this coding mode. Besides, we have also used Low-Delay-P (LP) encoding mode. In this case the first frame is an intra-frame while the others are encoded as generalized P frames. This makes this mode more vulnerable to packet losses since it needs to wait to receive an entire GoP before decoding the video frames. This structure is conceived for interactive real-time communications because Low-Delay coding structure usually provides an improved coding efficiency.

	Parameter	Value
Physics and Mac Layers IEEE 802.11p	Channel; Bandwidth	178, 5.89 GHZ ; 10 MHz
	Transmission range	230m
	Transmission power	20 mW
	Obstacle model	Defined in [21], [85]
	Beacon [CWmin, CWmax], AIFSN	[15,1023], 6
	Data [CWmin, CWmax], AIFSN	[7,15], 3
	Bit rate	6Mbit/s
RCP+	RSS_{th}, RSS_{max}	$-89dBm$, $-20dBm$
	Time slot	$13\mu s$
	Time window	$10sec$
	δ (Waiting Time)	$[1, 11]\mu s$
	Beacon frecuency, Beacon size	1 Hz, >=32 bytes
RCP	ω (Distance Factor)	1.5
	ω_P (Weight for the send probability)	0.5
	ω_Q (Weight for the link quality)	0.5
Video	Video Sequence, Duration	*Highway* [12], 00:01:20.00
	Constant Rate Factor (CRF)	28
	Video resolution	352x288
	Codec	H.265/HEVC, yuv420p, 25 fps
		H.264/AVC, yuv420p, 25 fps
	Encoding Modes	All Intra (AI)
		Low-Delay P (LP)
	File size	636 KB (H.265 LP CRF=28)
		6139 KB (H.265 AI CRF=28)
		4519 KB (H.264 AI CRF=28)
		1063 KB (H.264 LP CRF=28)
Scenarios	Number of Runs	10
	Time to live (TTL)	90s

Table 5.3: Simulation parameters.

5.3 Performance evaluation

In this section a performance assessment of some dissemination protocols is carried out by means of simulations. We first present the simulation setup used including models and scenarios. Then, we assess our proposal with pre-compressed sequences of video.

5.3.1 Simulation setup

To carry out the performance of the analysed dissemination schemes, we have provided each run with a different random scenario that fulfils the requirements of the study. For each point in all figures, we have calculated the average from 10 simulation runs. This let us obtain a standard error less than 5% in a 95% confidence interval. The packet error and Medium Access Control

(MAC) layer models adopted are based on the IEEE 802.11p, using a data rate of 6 Mbit/s, a transmission power of 20 mW, and a receiver sensitivity of -89 dBm. In addition, all beacon messages use the same Access Category (AC_BE), which results in the Contention Window (CW) and AIFSN parameters. Table 5.3 contains a summary of the simulation parameters common to all simulation scenarios.

Also, beacon messages are sent at the frequency of 1 Hz for all simulation scenarios. This is usually the highest frequency expected to be used for the transmission of beacon messages which gives the worst-case scenario in terms of freshness of the one-hop neighbourhood information. We used a typical mix of different vehicles according to the distribution presented in Table 5.1. All vehicles are moving according to the SUMO standard Krauss driver model. For the evaluation of our proposal, we considered different capabilities highways detailed in [51] and presented in Table 5.2.

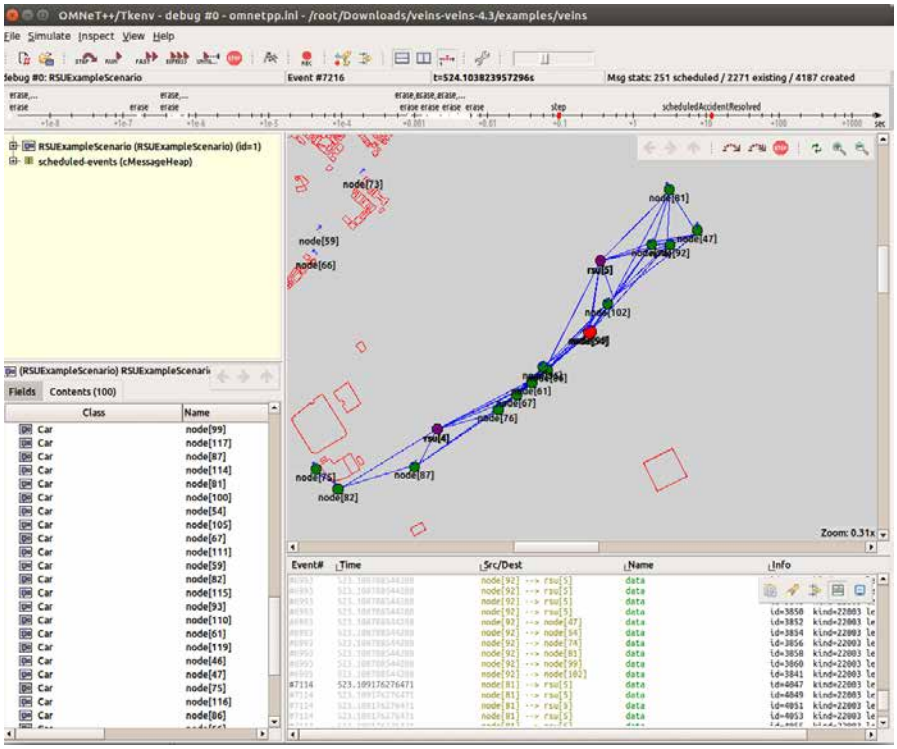


Fig. 5.2: Vehicular network scenario in OMNeT++ (red rectangles = buildings; red circle = crashed vehicle; green circles = warned vehicles; purple circles = RSUs): 9 km region of a primary highway C-32 in Barcelona, Spain.

Finally, we have prepared pre-compressed sequences of video and produced trace files with the information needed for the simulation, that is, the size

of every video frame. We have also included the frame sequence number in order to be able to compare the received and decompressed videos with the original sequences. For our evaluation, we used the well-known *Highway* video stream, which is publicly available at [12]. It is the CIF (Common Intermediate Format) version which contains 2000 frames and it was encoded with H.264/AVC [88] and H.265/HEVC [4]. As described in detail in Eq. 5.6, Constant Rate Factor (CRF)=28 was selected and used to control quality level of AVC and HEVC encoded. Table 5.3 presents a summary of the videos injected into the network. The video traces were built with the following structure: frame sequence number n, cumulative display time T_n, frame type (I, P, or B), frame size X_n (in bit).

5.3.2 Scenario description

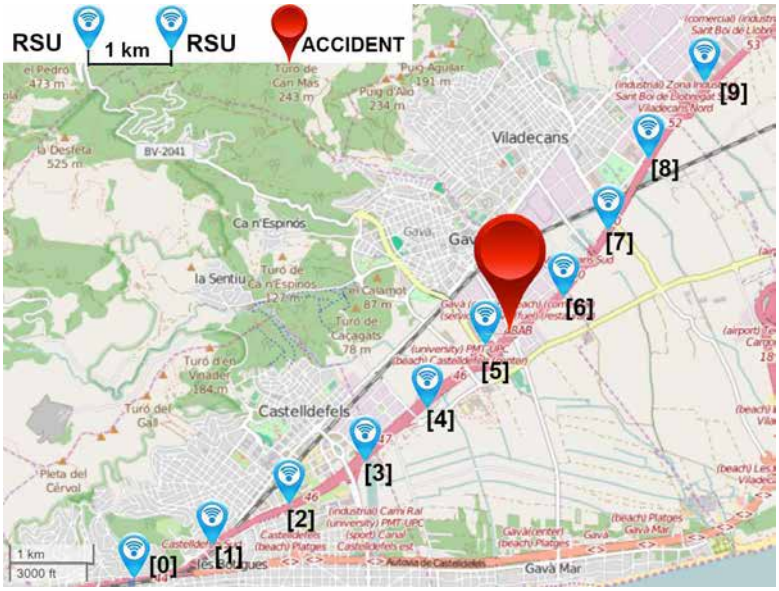


Fig. 5.3: Road Side Units (RSUs) distribution on the highway C-32 in Barcelona, Spain.

We simulate a 9 km highway with two lanes per road direction. Lanes are 10 m wide with a 4 m space between the directions. A set of 10 RSUs has been strategically located along the road every kilometer as it is shown in Figure 5.2. RSUs are traffic sinks used to measure the quality of the received video. That is, RSUs only will write a similar trace file with the frames they receive correctly.

We focus on the immediate consequences of an accident in kilometer 5.2 of a primary highway in Barcelona, Spain. The crashed vehicle starts to generate and transmit an SOS alert in order to inform the vehicles in the network about the incident and to the appropriate emergency centers (*e.g.* 112 or 911). The information includes a short video information of the last 80 seconds before the crash. Shadowing models are used to reproduce the attenuation of a radio signal induced by obstacles, such as buildings or other structures blocking the direct line of sight. Figure 5.2 shows the map section considered in OMNet++, where buildings represented by red rectangles are radio obstacles.

5.3.3 Performance measures

In this chapter, we use two performance metrics to evaluate the quality of video transmitted over VANETs: Frame Delivery Ratio and Peak Signal-to-Noise Ratio.

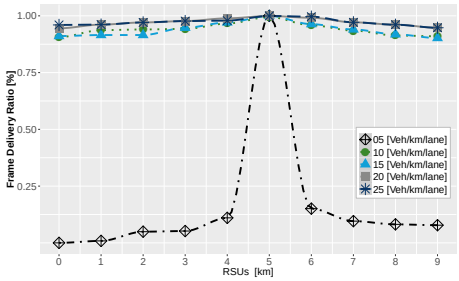
Frame Delivery Ratio: It is defined as a ratio between the number of frames delivered and the total number of frames received during a time interval T.

PSNR Peak Signal-to-Noise Ratio: It is an objective metric used to assess the application-level QoS of video transmissions. PSNR measures the error between the reconstructed image and the original one, frame by frame.

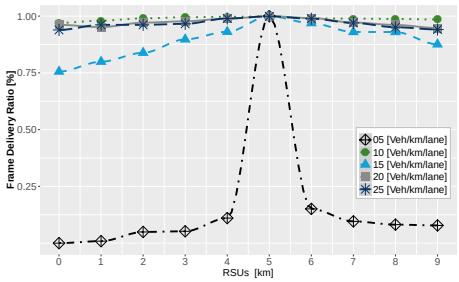
5.3.4 Simulation results

In this section, we present some representative simulation results. Our goal is to study the capability dissemination of RCP+ under realistic highway scenarios. To do so, we have implemented the code of RCP+. As described in section 5.2.2.4, our proposed mechanism is evaluated with pre-compressed sequences of video using H.265/HEVC and H.264/AVC.

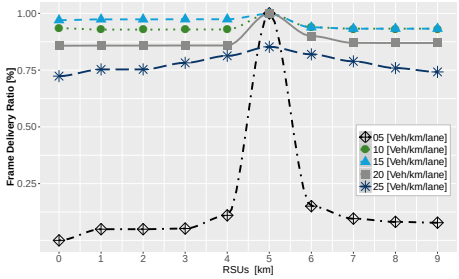
In the first set of experiments, we evaluated the performance of the frame delivery ratio with two H.265/HEVC video traces (LP CRF=28 and AI CRF=28) in RCP+ and RCP [101]. Figures 5.4a and 5.4b shows the frame delivery rate for different vehicles density with RCP+ and RCP using LP CRF=28 video trace. In Figure 5.4a, low density (5 vehicles/km/lane) directly affects the ability of the algorithm to disseminate. In fact, only RSU_5 located 200 m from the accident, received the complete trace. In the RSU_6 located 4.8 km from the accident, RCP+ reaches an average maximum rate of 15%. In the other RSUs our proposal does not exceed 10% of received frames. This result is expected because dynamic topology networks and low density causes temporary disconnections, interrupting the dissemination and compromising the delivery of the frames. In the other densities (10, 15, 20, 25



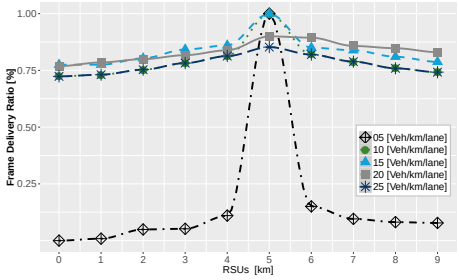
(a) RCP+ with video stream LP CRF=28.



(b) RCP with video stream LP CRF=28.



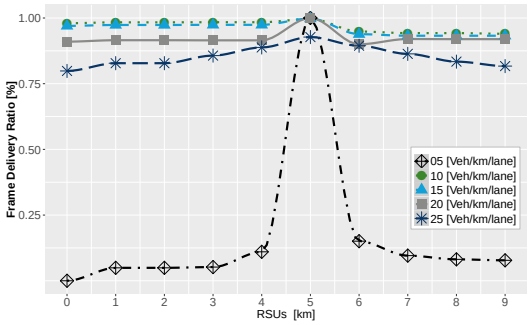
(c) RCP+ with video stream AI CRF=28.



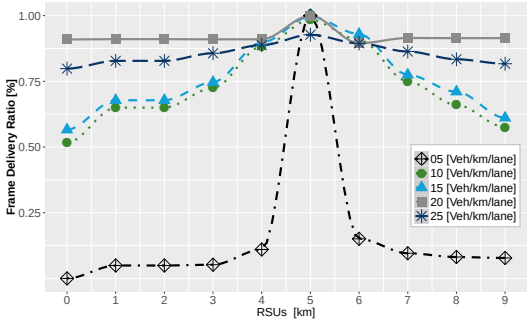
(d) RCP with video stream AI CRF=28.

Fig. 5.4: Received Frames with 95% confidence intervals for different network densities in a highway scenario using H.265/HEVC.

vehicles/km/lane), RCP+ is able to deliver more than a 85% of the frames in all RSUs. It is important to remember that RCP+ computes the weights of the Distance factor (D) and the Link Quality factor (LQ) as a function of the variation of the values of the normalized metrics with respect to the average of those values. This allows an optimal performance in middle and high vehicle densities. In Figure. 5.4b, the advantages of our proposal is notorious in 15 vehicles/km/lane. In the other vehicle densities, the performance of RCP+ is similar to RCP mainly because the channel is already congested and our adaptive algorithm almost does not affect the performance of the protocol.



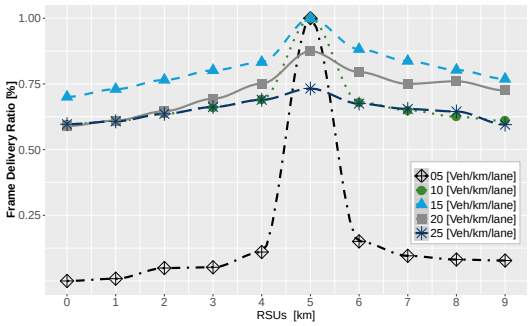
(a) RCP+ with video stream LP CRF=28.



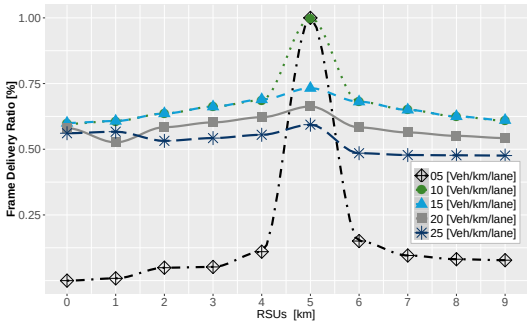
(b) RCP with video stream LP CRF=28.

Fig. 5.5: Received Frames with 95% confidence intervals for different network densities in a highway scenario using H.264/AVC

On the other hand, Figures 5.4c and 5.4d show the frame delivery rate for different vehicles density with RCP+ and RCP using AI CRF=28 video trace. In Figure 5.4c, low density (5 vehicles/km/lane) directly affects the ability of the algorithm to disseminate the warning video stream. In fact, only RSU_5 located 200 m from the accident, received the complete trace. In the RSU_6 located 4.8 km from the accident, RCP+ reaches an average



(c) RCP+ with video stream AI CRF=28.

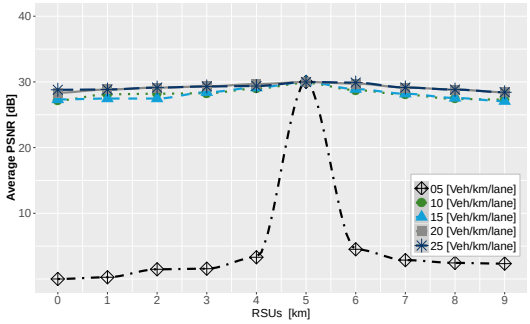


(d) RCP with video stream AI CRF=28.

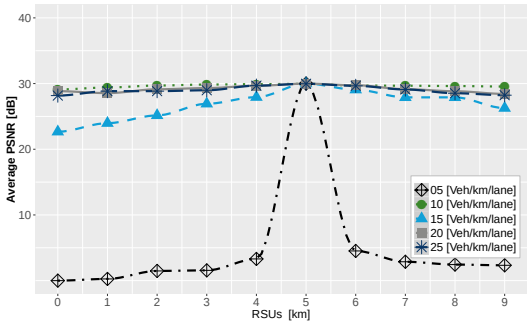
Fig. 5.5: Received Frames with 95% confidence intervals for different network densities in a highway scenario using H.264/AVC (cont.)

maximum rate of 15%. In the other RSUs our proposal does not exceed 10% of received frames. In the other densities (10, 15, 20, 25 vehicles/km/lane), RCP+ is able to deliver more than 70% of the frames in the far RSUs. In this case, the high vehicular densities (20 and 25 vehicles/km/lane) reach peak rates between 95% and 80%, respectively. Only when traffic density is 10 and 15 vehicles/km/lane, the frame delivery ratio reaches 99%. As RCP has fixed values for the weights of the Distance factor (D) and the Link Quality factor (LQ), RCP can not adapt to the changing traffic density. In addition, All Intra mode gets lower compression rates because P-frames and B-frames can usually obtain better compression rates than I-frames at the same quality level. With these observations, we can interpret the performance of RCP in Figure 5.4d. In this case, RCP is able to deliver more than a 70% of the frames in the far RSUs for 10, 15, 20, 25 vehicles/km/lane. Only RSU_5 located 200 m from the accident reaches an average maximum rate of 95% for 5 and 10 vehicles/km/lane.

As a next step, we evaluated the performance of the frame delivery ratio with two H.264/AVC video traces (LP CRF=28 and AI CRF=28) in RCP+



(a) RCP+ with video stream LP CRF=28.

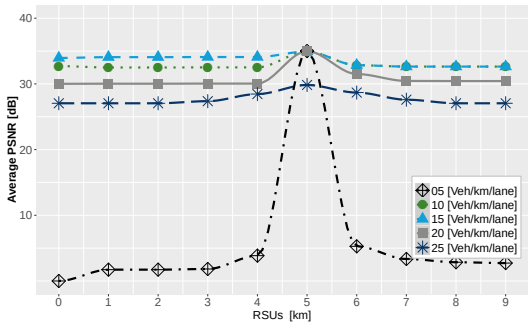


(b) RCP with video stream LP CRF=28.

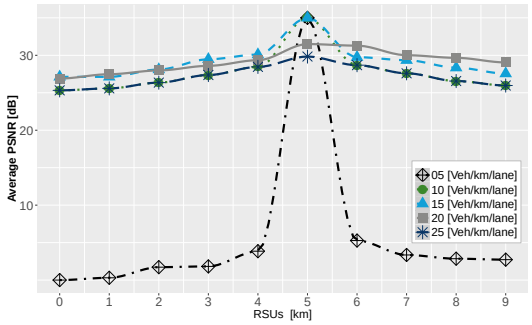
Fig. 5.6: Average PSNR with 95% confidence intervals for different network densities in a highway scenario using H.265/HEVC

and RCP. A similar behavior can be seen in Figure 5.5. Figures 5.5a and 5.5b show the frame delivery rate for different vehicles density with RCP+ and RCP using LP CRF=28 video trace. In Figure 5.5a, low density (5 Vehicles/km/lane) directly affects the ability of the algorithm to disseminate. In fact, only the RSU_5 located 200 meters from the accident, received the complete trace. In the RSU_6 located 4.8 km from the accident, RCP+ reaches an average maximum rate of 12%. In the other RSUs our proposal does not exceed 10% of received frames. In the other densities (10,15,20,25 Vehicles/km/lane), RCP+ is able to deliver more than a 75% of the frames in all RSUs. If we compare the results of the frame rate received for H.265/HEVC and H.264/AVC, we can conclude that while the H.265 codec is able to maintain frame loss at low levels, the H.264 codec suffers a high frame loss. This is evident in Figures 5.5b and 5.5d where frame delivery rates show losses up to 50%.

Finally, we evaluate the PSNR (Peak Signal to Noise Ratio) of the received video frames. We assume that in case an individual frame was lost, the decoder would display instead of the last successfully received frame. So



(c) RCP+ with video stream AI CRF=28.

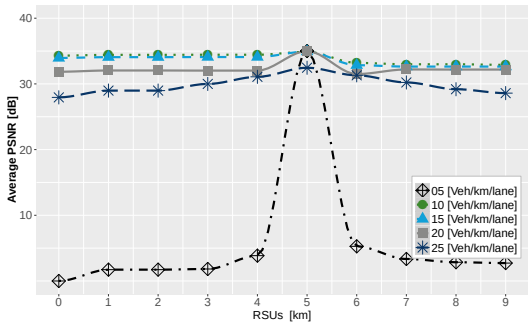


(d) RCP with video stream AI CRF=28.

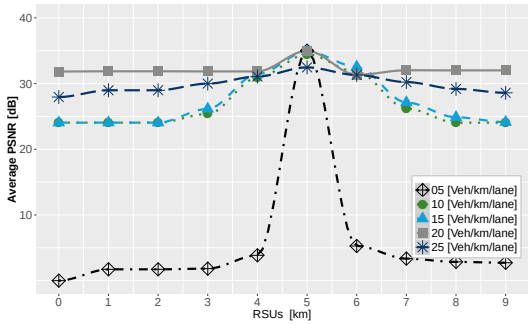
Fig. 5.6: Average PSNR with 95% confidence intervals for different network densities in a highway scenario using H.265/HEVC (cont.)

if a frame is dropped, we need to compare the source frame to the previous streamed frame. This way, instead of a grey area for the missing frame we will get an approximation to the lost data. Next, we decoded each frame into its YUV[1] channels. The PSNR of the channels needs to be calculated independently. We just use the Y channel, as it is the most important. In Figures 5.6 and 5.7 we show an analysis of the video quality by means of the PSNR of the reconstructed video sequences received at the RSUs. In Figure 5.6a, we can see that the video quality is inside a range of 30-35 dB for 10, 15, 20, 25 vehicles/km/lane. When RSUs are far the accident, quality drops to values around 10 dB in low vehicular density (5 vehicles/km/lane). This is caused by keeping on the screen the last received frame which produces a freezing effect. This happens because burst losses appear instead of isolated losses. Although PSNR values do not increase much with our simple error method to improve video quality results, the subjective evaluation shows an improve-

[1] YUV files contain bitmap image data stored in the YUV format, which splits color across Y, U, and V values. It stores the brightness (luminance) as the Y value, and the color (chrominance) as U and V values.



(a) RCP+ with video stream LP CRF=28.



(b) RCP with video stream LP CRF=28.

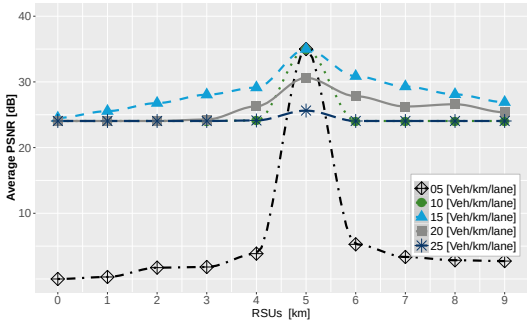
Fig. 5.7: Average PSNR with 95% confidence intervals for different network densities in a highway scenario using H264/AVC

ment. This was verified during the simulations observing the output of the received video streams.

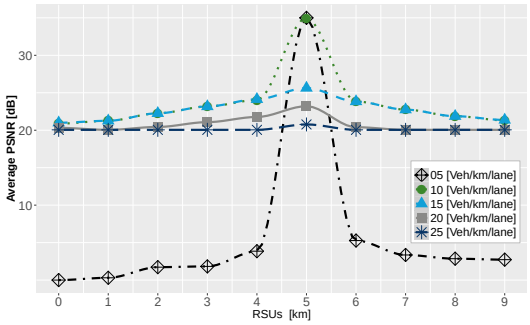
In short, our performance evaluation has highlighted that H.265 outperforms H.264 in terms of both frame loss and PSNR quality. The results show that a video with a moderate CRF and appropriate coding structures low-delay-P (LP) (Figures 5.4a and 5.6a) can be received in such a high motion scenario with acceptable quality.

5.4 Summary

In this chapter, we have proposed RCP+, a rebroadcasters selection mechanism for video streaming over VANET. RCP+ selects a subset of vehicles in the networks to rebroadcast the content, based on their strategic location in the network and their capacity to evaluate the congestion of the communication channel. Also, we have designed a proposal to update the weight



(c) RCP+ with video stream AI CRF=28.



(d) RCP with video stream AI CRF=28.

Fig. 5.7: Average PSNR with 95% confidence intervals for different network densities in a highway scenario using H264/AVC (cont.)

values for metrics in RCP+ to provide video-streaming services. In addition, our proposed mechanism was evaluate with H.265/HEVC and H.264/AVC. H.265 achieves significantly greater efficiency than H.264. Simulation results have shown that our solution can provide a good video quality in different scenarios. Furthermore, we show that our proposal reduces the frame loss and enhances the PSNR of the received video. As future work, we will focus on a more precise selection for the relaying vehicles, with considerations of buffer management. We will seek an efficient forwarding mechanism to guarantee enhance video QoE (Quality of Experience) according with VANET safety applications' requirements.

Chapter 6
Game-theoretical proposals for VANET dissemination

6.1 Introduction

In this chapter, we propose an Adaptive Distributed Dissemination (ADD) protocol to perform data dissemination in VANETs. ADD is designed to operate without any roadside infrastructure in urban scenarios under diverse road traffic conditions. To achieve this objective, ADD employs a decentralized stochastic solution for the broadcast data dissemination problem through two game-theoretical mechanisms. Game theory can be used to design a mechanism to predict behavior in situations where a state is the result of a series of interactions between different nodes (*players*), who act according to their preferences regarding future performance and existing incentives. In first place, the Asymmetric Volunteers Dilemma Game modeled by Diekmann [27] is evaluated as a mechanism to quench the broadcast storm problem. The probability that a node forwards a broadcast message is calculated using the number of candidate vehicles to forward the message, *i.e.*, the number of vehicles that are listening to the transmission. The cost/benefit relation to forward the message by the vehicle, is obtained from metrics like distance and link quality. Next, the Forwarding Game modeled by Naserian [61] is evaluated as another mechanism to mitigate the broadcast storm problem. In this case, the strategy of the players is to select a forwarding probability that maximizes their pay off using a utility function. The utility function is designed as a function of the player's availability and the forwarding probability of other players. Availability of a player is a normalized factor based on metrics like distance from the source of the flooding packet (*e.g.,* an accidented vehicle) and estimated bandwidth of the link formed between the node currently holding the packet and each candidate node within its transmission range. Finally, our proposal employs a mechanism of Store-carry-forward (SCF) to mitigate the intermittently connected network problem presented on streets or roads that have low-density traffic conditions in which the number of vehicles is not enough to disseminate data messages using multi-hop communication.

Our contributions in this chapter can be summarized as follows:

- Review of two mathematical models of game-theoretical.
- Adapt two game-theoretical models to VANETs.
- Propose an Adaptive Distributed Dissemination (ADD) protocol to perform data dissemination through two game-theoretical mechanisms.
- Compare our proposal against others protocols with different traffic densities in terms of Packet Delivery Ratio (PLR), Average Packet Delay (APD), Total Packet Loss Ratio (PLR) and Propagation distance.
- Evaluate our proposal for video warning message dissemination in terms of Frame Delivery Ratio (FDR) and Average PSNR.

The remainder of this chapter is organized as follows: section 6.2 explains the game theoretical formulation. section 6.3 details the game formulation used in vehicular networks. section 6.4 presents the ADD protocol. Afterwards, section 6.5 discusses the performance evaluation and includes results of our analysis. We conclude in section 6.6 with a summary of this chapter.

6.2 Game-theoretical approaches for dissemination in VANETs

According to on [52], the essence of game theory is the mathematical study of interactions between independent decision-makers (called *players*) who can have common interests or conflicting. What the other players do has an impact on each decision-maker, whose benefit or utility not only depends on its decisions but also on the others' decisions. The problem in interactive situations is that the optimal decision (strategy) is unclear because no player completely controls the final outcome. This means that the problem must be defined before it can be solved. Game theory is a means of proposing, designing interaction models, studying the conditions under which some outcomes can be reached, and designing good strategies [53]. In this section, we summarize two game-theoretical models proposed to mitigate the broadcast storm problem. The two models consider vehicles as intelligent entities capable of observing a structured environment and deciding whether or not to forward packets. In the following we present two approaches for smart dissemination in urban VANETs based on two well-known games: the Asymmetric Volunteers Dilemma Game [26, 27] and the Forwarding Game [60, 61].

6.2.1 First game-theoretical algorithm designed for dissemination in VANETs: Asymmetric volunteer's dilemma

The Volunteers Dilemma Game modeled by Diekmann [26] is a game composed of N players in which each individual prefers to avoid the cost of volunteering and exploit the benefit of the collective goods produced by others, although someone must volunteer. Defection is the dominant strategy from the perspective of individual rationality. Nevertheless, it becomes collectively irrational if all players in the group choose to free ride. If there is no volunteer in the group, all lose. Everyone can be better off by playing the dominated strategy which explains the existence of a dilemma. The basic game model is defined as:

$$G = \{N, S, K, U\},\ N \geqslant 2, \tag{6.1}$$

where N is the number of players, $S = \{Cooperation, Defection\}$ is the strategy set that dictates player responses to stimuli in the external environment, $K > 0$ is the cost of volunteering (Cooperation), and U is the benefit earned when at least one player volunteers.

Variable	Definition
β_i	Probability of defection of player i
K_i	Cost of volunteering for player i
U_i	Benefit earned by player i when at least one player volunteers
β_j	Average defection probability of all the other players j ($j \neq i$)
β_i^N	Probability that nobody volunteers
i=1,2,3...,N	i is a generic player, being N the number of players

Table 6.1: Definitions of the variables presented in the asymmetric volunteer's dilemma.

In this type of game, there are N asymmetric equilibria in pure strategies, *i.e.* cooperation (C) and defection (D), in which exactly one player, the volunteer, contributes [26]. They are usually attainable with coordination amongst players. With N players, there is a equilibrium point that is symmetric if mixed strategies are introduced. Letting β_i, be the probability of player i's D-choice (not volunteering) the expected utility is:

$$E_i = \overbrace{\beta_i \cdot U_i \cdot \left(1 - \prod_{j \neq i}^{N} \beta_j\right)}^{\textbf{Defect (D)}} + \underbrace{(1 - \beta_i) \cdot (U - K)}_{\textbf{Collaborate (C)}} \tag{6.2}$$

The mixed-strategy equilibrium can be found by taking the derivative with respect to β_i and letting $\frac{dE_i}{d\beta_i} = 0$, which gives:

$$\beta_{eq} = \left(\frac{K}{U}\right)^{\frac{1}{N-1}} \tag{6.3}$$

A key assumption is strict symmetry in terms of the costs of volunteering (K) and benefit (U) of all players. So, this version of the game is referred to as symmetric volunteer's dilemma. Conversely, Diekmann presented an analysis of an asymmetric volunteer's dilemma game [27]. In that version of the game, the author introduced an unequal distribution of cost of volunteering K_i and benefit U_i earned when at least one player i volunteers in a group of size N players. If we let strategy D_i be played with probability β_i, the expected utility of player i can be expressed as follows:

$$E_i = \overbrace{\beta_i \cdot U_i \cdot \left(1 - \prod_{j \neq i}^{N} \beta_j\right)}^{\textbf{Defect (D)}} + \underbrace{(1 - \beta_i) \cdot (U_i - K_i)}_{\textbf{Collaborate (C)}} \tag{6.4}$$

where β_i is the player i's probability of defection, U_i is the benefit earned by that player when at least one player volunteers, β_j is the average defection probability of all the other players ($j \neq i$), and K_i is the cost of volunteering for that player i.

The best response function for player i can be obtained by maximizing Equation (6.4), we get the solution of the best response for player i:

$$\beta_i^* = \frac{U_i}{K_i} \cdot \left(\prod_{j=1}^{N} \frac{K_j}{U_j}\right)^{\frac{1}{N-1}} \tag{6.5}$$

Based on Equation (6.5)[1], the Nash-equilibrium strategy implies that node i's defection probability will increase with decreasing the value of K_i or increasing the value of U_i. All variables presented in this game are defined in Table 6.1.

The asymmetric volunteer's dilemma game would be played in a VANET whenever a vehicle receives a broadcast message that must be forwarded. Each receiving vehicle computes its β_i in equilibrium using Equation (6.5). Thus, each vehicle could choose in a decentralized way its best strategy. Afterwards, in section 6.3 we adapt the asymmetric volunteer's dilemma game to VANETs.

[1] In Appendix A, we extend the development of β_i^*.

6.2.2 Second game-theoretical algorithm designed for dissemination in VANETs: Forwarding game

Unlike the volunteer's dilemma, in the Forwarder Game modeled by Naserian [61] the outcome is the probability that each node forwards the message. Upon receiving the flooding packet, the neighbours of a source node i choose the forwarding probability as their strategy according to the following game G.

$$G = \{N, S_i, U_i\},\ N \geqslant 2,\ i \in N \tag{6.6}$$

where N is the number of players of the game, S_i is defined as the probability that node i forwards the received message ($0 < S_i \leq 1$), and U_i is the utility earned when at least one node forwards the received message.

Variable	Definition
S_i	Probability that node i forwards the received flooding packet
U_i	Utility of node i
a_i	Availability of node i
S_i	Average forwarding probability of the neighbouring nodes of i
Q_i	Neighbour action reflection
k, m, n	Constant values. Our results showed that k=4, m=2, n=3 provide optimum results based on our simulations.
i=1,2,3...,N	i is a generic node, being N the number of nodes

Table 6.2: Definitions of the variables presented in the forwarding game.

As our main goal is to mitigate the broadcast storm problem and therefore improve the overall performance of the network by eliminating redundant broadcast, we used the utility function U_i modeled by Naserian [61] and defined as:

$$U_i(S_i, a_i, Q_i) = \frac{a_i \cdot S_i}{Q_i} \cdot exp\left(\frac{-S_i^2}{2 \cdot k \cdot a_i^n \cdot Q_i^m}\right) \tag{6.7}$$

where k, m and n are constant values, a_i is the availability of node i, and Q_i is the neighbour action reflection.

We identify the availability of a node a_i and the strategy of its neighbouring nodes S_i as main metrics that allow node i to select a strategy S_i that maximizes its utility U_i. First, we design the availability a_i of a node i as a multimetric parameter that measures the amount of resources available for that node. This estimated value is a normalized average ($0 < a_i \leq 1$) of some relevant parameters in our network such as available bandwidth and node's position. Next, a node i can estimate its neighbours' participation from the

information provided by beacon messages. This estimated parameter is called *neighbour action reflection*, denoted by Q_i and defined as:

$$Q_i = 1 - S\_\text{-}i \tag{6.8}$$

Q_i generates a balance between the probability of participation of node i and the average forwarding probability of the neighbouring nodes of i.

Setting the derivative of Equation (6.7) equal to zero, we get an expression that allows us to calculate the maximum utility of node i as a function of parameters a_i and Q_i:

$$S_i^* = \sqrt{k \cdot a_i^n \cdot Q_i^m} \leftarrow \textit{Strategy that maximizes the utility function of node } i \tag{6.9}$$

In the forwarding game, a node i with N neighbours can estimate the average forwarding probability S_i of the other nodes as:

$$S\_\text{-}i^* = \sum_{\substack{j=1 \\ j \neq i}}^{N} \frac{S_j}{N-1} \tag{6.10}$$

Equilibrium is a term used in game theory to describe a point where each player's strategy is optimal given the strategies of all other players. In this sense, every node can find its best strategy to play the game replacing Equations (6.8) and (6.10) in Equation (6.9), so we have:

$$S_i{}^* = \sqrt{k \cdot a_i^n} \cdot \left(1 - \sum_{\substack{j=1 \\ j \neq i}}^{N} \frac{S_j}{N-1} \right)^{\frac{m}{2}} \tag{6.11}$$

We design Equation (6.11) with $k = 4$, $n = 3$ and $m = 2$ since these are optimal values. Also, we rename the availability factor $\alpha_i = \sqrt{4 \cdot a_i^3}$. Finally, we obtain an expression for the best forwarding probability of node i:

$$S_i{}^* = \alpha_i \cdot \left(1 - \sum_{\substack{j=1 \\ j \neq i}}^{N} \frac{S_j}{N-1} \right) \tag{6.12}$$

Equation (6.12) consists of N linear equations for each player i. Thus, every node can solve the system of equations and find its best strategy to play the game. We assume that each node i knows the value of its availability factor α_i and number of neighbouring nodes of node i, N_i. In section 6.3 we will see

how nodes compute their α_i in the designed game to improve dissemination in VANETs.

$$\begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ \vdots \\ S_N \end{bmatrix} \begin{bmatrix} 1 & \frac{\alpha_1}{N-1} & \frac{\alpha_1}{N-1} & \cdots & \frac{\alpha_1}{N-1} & \alpha_1 \\ \frac{\alpha_2}{N-1} & 1 & \frac{\alpha_2}{N-1} & \cdots & \frac{\alpha_2}{N-1} & \alpha_2 \\ \frac{\alpha_3}{N-1} & \frac{\alpha_3}{N-1} & 1 & \cdots & \frac{\alpha_3}{N-1} & \alpha_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \frac{\alpha_N}{N-1} & \frac{\alpha_N}{N-1} & \frac{\alpha_N}{N-1} & \cdots & 1 & \alpha_N \end{bmatrix} \tag{6.13}$$

Once the results of the system of equations have been found, each node i can calculate its best forwarding probability S_i[2]. All variables presented in this game are defined in Table 6.2. In section 6.3.2 we will see how to use the designed game in VANETs, and specifically we will design the availability parameter a_i in the forwarding node selection process.

6.3 Adapting both game-theoretical models to VANETs

As we have seen in the previous section, the purpose of Game Theory is to model interactions between players, to define different types of possible outcome, to predict the solution of a game under given information and behavior assumptions, and to design strategies to reach the outcomes. When an emergency message is received by a vehicle, the message should be re-broadcasted by that node. Nonetheless, in the shared wireless medium, unnecessary broadcasts degrade the performance of the network, which is known as broadcast storm problem. In our approach, neighbours of the source node play a game-theoretical algorithm upon receiving the emergency message, and they choose a forwarding probability as their strategy. The outcome of the game is the probability that each node forwards the emergency message.

6.3.1 Design of the utility function for the asymmetric volunteer's dilemma

Using the framework of the volunteer's dilemma (VoDi) defined in section 6.2.1, we now formulate the VoDi to model warning messages dissemination in VANETs. We consider the special case of an asymmetric volunteers dilemma with increasing benefit earned by vehicle i when at least one player volunteers (U_i) and strictly constant costs ($K_i = constant$) , *i.e*,

[2] In Appendix B, we extend the development of $S_i{}^*$.

$U_1 > U_2 > ... > U_N$ where $U_i > K_i > 0$. The costs K_i have been fixed to 1. This is not a limitation of the analysis. Quite the opposite, it is a grade of freedom of the game that could be used to extend the model based on the benefits earned by vehicle i when at least one player volunteers.

Efficient delivery of messages in a VANET depends critically on the set of intermediate nodes which act as forwarding nodes. The behavior of the vehicle that received the message affects positively or negatively the behavior of other vehicles, depending on whether there was a choice of forwarding the message or not. We define several core strategies combined as an integral scheme to enhance the performance and the reliability of the warning message broadcast. Our proposal of utility function includes information about its local neighbourhood and significant cross-layer information. Thus, the utility function for node i is given by:

$$U_i(Df_i, LQf_i) = 10^{(10-(\alpha_1 \cdot Df_i + \alpha_2 \cdot LQf_i))} \tag{6.14}$$

which is composed by two parameters related to information provided by vehicle i: the position of the vehicle in the network (Df_i) and an estimation of the congestion of the communication channel (LQf_i). ADD calculates the utility U_i, which is later used to compute its β_i in equilibrium. Higher values of Df_i and LQf_i represent a better position of the vehicle and better channel conditions, respectively (in the range $[0, 1]$). Powers of base ten to make the relationship sensitive enough to environmental conditions. The weights $\alpha_1 = 6$ and $\alpha_2 = 4$ have been obtained through extensive simulations and under different traffic conditions, showing best results with those values. Nevertheless, we plan to design a dynamic scheme to update the weights of the multimetric score to calculate the utility function U_i for node i.

Once the cost function K_i has been designed for an urban scenario, each vehicle is able to calculate its β_i^* in equilibrium according Equation (6.5). Thus, the asymmetric volunteer's dilemma game is played whenever vehicles receive a broadcast message and they choose in a decentralized way its best strategy.

6.3.2 Design of the availability function in the forwarding game

We have designed the availability function of a vehicle as a parameter a_i ($0 < a_i \leq 1$) that measures the amount of available resources in the node i that make more efficient the process of disseminating emergency messages. This estimated value is a normalized average of two parameters: estimated available bandwidth and position of the node in the network.

Due to a possible large number of vehicles sharing the wireless medium, it is unclear whether the channel capacity is sufficient to support the data

generated by hello messages and at the same time leaving enough available bandwidth for supporting other applications. For the specific case of emergency video dissemination, the overall capacity of the channel can affect the effectiveness of emergency dissemination schemes if the density of potential forwarders is high. Definitely, available bandwidth estimation is a key component for quality of service (QoS) in VANETs. We have considered the ABE proposal presented in section 4.2.3 to estimate the available bandwidth in the link formed by two sender-receptor vehicles.

On the other hand, we have taken into account the position of the receiver node in the network to design a measure of the amount of available resources a_i for vehicle i. As mentioned previously, vehicles located in intersections typically have better network connectivity than non-intersection vehicles. Also, vehicles whose location is farthest from the source are potential forwarders in the process of message dissemination. In addition, the position of the vehicles in the road-map has a large impact on the efficiency of dissemination due to the effect of buildings. With all these considerations, the position of the node is evaluated similarly to the distance factor Df_{i} presented in Equation (4.1).

To compute the availability a_i, first, we divide ABE by the link capacity C_{ABE}, obtaining a normalized available bandwidth metric. A high value of ABE means a high available bandwidth in the link formed by both vehicles s and r. Next, we also consider the distance factor Df_{i} as a function of the distance between the sender and the potential next forwarder i, and the next nearest intersection D_{rint}. Equation (6.15) presents the availability function a_i of the potential forwarder.

$$a_i = \frac{ABE_{i(s,r)}}{C_{ABE}} \cdot \gamma + Df_i \cdot (1 - \gamma) \tag{6.15}$$

where $\gamma = 0.5$ is a weight to average both metrics.

Each vehicle has an utility function U_i that is a function of its strategy S_i^* and its availability a_i. Since the forwarding decision is made locally every vehicle can calculate its S_i^* in equilibrium according to Equation (6.12). Thus, the forwarding game is played whenever vehicles receive a broadcast message and they choose in a decentralized way their best strategy to broadcast the message or not.

Figure 6.1 shows the variables present in the Forwarding Game where each vehicle must select a strategy that maximizes its utility. Below we detail the Forwarding Game for the black vehicle i. First, when vehicle i receives an emergency message, it should compute the parameters: availability a_i and neighbour action reflection Q_i. While the availability of vehicle i depends exclusively on information of itself, Q_i is estimated based on the information of the strategy of its neighbours (purple vehicles A, B and C), *i.e.*, S_i allows us to estimate the parameter Q_i. Note that red vehicles D and E are outside the transmission coverage of vehicle i. Finally, vehicle i selects its best strategy S_i to obtain a maximum utility U_i.

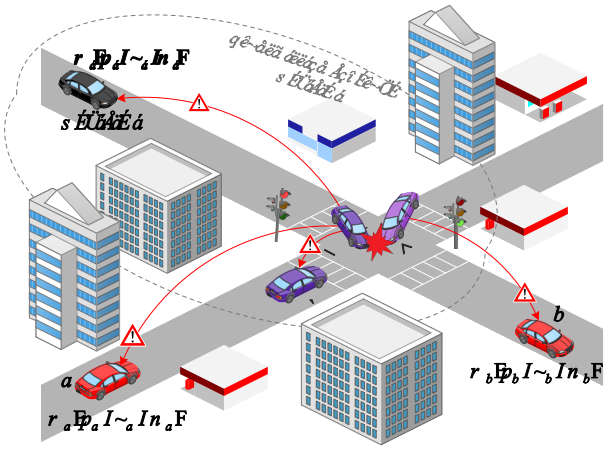


Fig. 6.1: Forwarding Game in an urban scenario.

6.4 Adaptive distributed dissemination protocol description

This section describes the proposed protocol called Adaptive Distributed Dissemination (ADD). The main goal of the ADD mechanism is disseminate warning messages to all vehicles inside the region of interest (ROI) independently of the road traffic condition. Therefore, our proposal must be able to tackle the broadcast storm and intermittently connected network problems.

We assume that each vehicle is equipped with a GPS device to obtain its geographical location in current time. A preloaded digital map provides information about roads and intersections. Besides, we assume that vehicles periodically exchange their physical location, moving velocity and moving direction enclosed in their periodic beacon messages. Finally, vehicles are assumed to be equipped with IEEE 802.11p wireless technology and computation capabilities.

6.4.1 Adaptive distributed dissemination (ADD) scheme

ADD is a data dissemination protocol based on a periodic beacon-based approach, so-called Basic Safety Message (BSM) [100]. ADD is located on top of UDP (User Datagram Protocol) and WSMP (WAVE Short Message Protocol) [16]. The WSMP protocol is meant to handle safety messages, whereas non-safety messages can be sent with either WSMP or UDP. ADD includes

five main modules: neighbour discovery, relaying node selection, store-carry-cooperative forward, adaptive beaconing and video quality strategy, which are described in the following.

6.4.1.1 Neighbour discovery

The neighbour discovery mechanism in ADD keeps the knowledge of the local topology by monitoring periodic beacon updates received from one-hop neighbours. Each vehicle periodically announces its status to all its one-hop neighbours by broadcasting a beacon packet. These packets carry the current location of the node which is acquired from the GPS, moving velocity and moving direction. In addition, each beacon contains the IDs of the warning messages that have been received and are being carried by the vehicle. Note that incorporating the IDs of the received data messages into the beacons works as an implicit acknowledgment mechanism. Therefore, when a vehicle receives a beacon from a neighbour, it is able to verify if it has any warning message that has not been received by this neighbour and then forwards it accordingly. Each vehicle sets up and dynamically updates a neighbours table that contains identification, mobility information of all one-hop surrounding vehicles and IDs of received warning messages.

6.4.1.2 Relaying node selection in ADD

Relaying is the task of assigning the duty of forwarding a message to a specific node or nodes that satisfy some criteria. Our approach ADD is able to respond to environmental changes, adapting its operation mode to face those frequent topology changes inherent in VANETs. Two types of relaying node selection are presented based on two game-theoretical schemes. The games are played whenever a vehicle receives a broadcast message that must be forwarded. Algorithms 2 and 3 show the *Volunteer's Dilemma* relaying scheme and the forward game relaying scheme, respectively.

The first game-theoretical forwarding scheme uses the *Volunteer's Dilemma* (see section 6.2.1) to select the relaying node. According to Algorithm 2, the Relaying node selection module executes the procedure $receiveWarningMessage(*WarningMessage)$. If a warning message with identifier $warningMsgId$ was previously received (line 2), the message is accounted and discarded (line 3). Also, if the vehicle receives a duplicate warning message while it is scheduled to rebroadcast $warningMsg$, then it cancels the rebroadcast (lines 12-13), thus avoiding a possible redundant retransmission. Otherwise, if a warning message is new, a vehicle will insert the identifier $warningMsgId$ into subsequent beacons, until warning message expires (line 8). After that, the vehicle computes the probability of defection β_i^* using Equation (6.5), as a function of the benefit earned by

that player when at least one player volunteers (U_i), the average defection probability of all the other players (β_j), the cost of volunteering for that player i (K_i) and the average cost of volunteering of all the other players j (line 9). Once calculated β_i^*, the $receiveWarningMessage()$ procedure provides a random number $rnd()$ to be compared with the probability to volunteer (*i.e.*, to forward the packet) $1 - \beta_i^*$ (line 11). If $rnd() < (1 - \beta_i^*)$ then vehicle i is selected as a forwarding node and rebroadcasts this warning message (lines 12-13). Otherwise, if the vehicle does not forward the message, a timeout WT is assigned to the node (line 16). Note that in Equation (6.16), the vehicle farthest from the transmitting node will have assigned the shortest WT period. After the waiting time expiration, the forwarder vehicle rebroadcasts the message only if the node has not received a copy of the message (lines 17-18) and stores data packet in the main buffer (line 19).

The second game-theoretical forwarding scheme designed uses the *Forwarding Game*, explained in section 3, to select the relay node or nodes. The proposed mechanism is further described in Algorithm 3. The general scheme of this game is similar to the *Volunteer's Dilemma*. The main difference is

Algorithm 2 Asymmetric Volunteer's Dilemma Operation

Require: Neighbour Table, Warning Message ($warningMsg$)
Ensure: Select forwarder node
1: **procedure** RECEIVEWARNINGMESSAGE(*Warning Message)
2: **if** WarningMsgTable.getId=warningMsgId **then**
3: Discard packet
4: **if** rebroadcast timer for $warningMsg$ is scheduled **then**
5: Cancel rebroadcast timer for $warningMsg$
6: **end if**
7: **else**
// Embedding IDs of received warning messages into beacons
8: Add $warningMsgId$ in subsequent beacons
// Best response for vehicle i, see Equation (6.5)
9: $\beta_i \leftarrow \frac{U_i}{K_i} \cdot \left(\prod_{j=1}^{N} \frac{K_j}{U_j}\right)^{\frac{1}{N-1}}$
10: $rnd \leftarrow uniform(0,1)$
11: **if** $rnd < (1 - \beta_i)$ **then**
12: Node selected for forwarding
13: Forward packet
14: Storage in temporary buffer
15: **else**
16: Wait for a Backoff
17: **if** packet was not forwarded by another vehicle **then**
18: Forward packet
19: Storage in main buffer
20: **end if**
21: **end if**
22: **end if**
23: **end procedure**

that the forwarding probability of a source node i is now calculated as a function of the availability of node i (line 9). Any of its neighbours that hears a duplicate rebroadcast, with regard to the recently received message, will cancel its message-rebroadcast process.

According to both schemes, each forwarder candidate adjusts its own waiting time WT that is inversely proportional to the distance from itself to the previous forwarder vehicle, as it is shown in Equation 6.16.

$$WT = 0.005 + (SLOT\_TIME \cdot (R_{max} - D_{tc})) \tag{6.16}$$

where $SLOT\_TIME$ represents a time slot, R_{max} represents the maximum transmission range, and D_{tc} is the distance between the transmitter and the forwarding potential candidate vehicle. Since forwarding candidates are neighbours $D_{tc} \leqslant R_{max}$, a vehicle in the edge of the coverage radius will wait a $WTmin$, while a vehicle close to the sending one will have to wait $WTmax$. This gives priority to the most distant vehicle in the coverage area to broadcast the message.

Algorithm 3 Forwarding Game Operation

Require: Neighbour Table, Warning Message ($warningMsg$)
Ensure: Select forwarder node
1: **procedure** RECEIVEWARNINGMESSAGE(*Warning Message)
2: **if** WarningMsgTable.getId=warningMsgId **then**
3: Discard packet
4: **if** rebroadcast timer for wm is scheduled **then**
5: Cancel rebroadcast timer for Warning Message wm
6: **end if**
7: **else**
// Embedding IDs of received warning messages into beacons
8: Add $warningMsgId$ in subsequent beacons
// Best response for vehicle i, see Equation (6.12)
9: $S_i^* \leftarrow \sqrt{k \cdot a_i^n} \cdot \left(1 - \sum_{\substack{j=1 \\ j \neq i}}^{N} \frac{S_j}{N-1}\right)$
10: $rnd \leftarrow uniform(0, 1)$
11: **if** $rnd < S_i^*$ **then**
12: Node selected for forwarding
13: Forward packet
14: Storage in temporary buffer
15: **else**
16: Wait for a Backoff
17: **if** packet was not forwarded by another vehicle **then**
18: Forward packet
19: Storage in main buffer
20: **end if**
21: **end if**
22: **end if**
23: **end procedure**

$$WT_2 = 0.005 + (SLOT\_TIME \cdot D_{tc}) \tag{6.17}$$

6.4.2 Store-Carry-Cooperative Forward

The store-carry-forward (SCF) based approach is a conventional data forwarding mechanism in vehicular ad-hoc networks proposed in several works. The main idea is that vehicles keep the copies of messages and replicates whenever there is a contact opportunity. Taking advantage of vehicle mobility, relay vehicles are expected to have contact with new neighbours and deliver the message. This mechanism is robust to intermittent network connectivity and can guarantee data delivery.

In our proposal, a vehicle presents two types of data buffers to store message: main buffer and temporary buffer.

- *Temporary buffer*: It stores copies of message which are being broadcasted but waiting for duplicated to ensure the successful reception. After the vehicle overhears the duplicated packets from the forwarding vehicle, the corresponding message copy will be deleted from the temporary buffer. Otherwise, the vehicle will recover the message from the secondary buffer and store it in the main buffer after timeout δ_t.
- *Main buffer*: It stores messages when a vehicle cannot find neighbours within its transmission range.

When the network is partitioned (sparse road traffic), vehicles use their mobility capabilities to carry the stored messages to different parts of the ROI. Furthermore, vehicles must be able to determine if a new neighbour has already received a warning message or not. For this, beacons are used as an implicit acknowledgement mechanism. Algorithm 4 shows how our proposed solution delivers warning messages even when the network is intermittently connected. When a vehicle receives a beacon message b_j from a neighbour j, it verifies whether there is a warning message that has not been acknowledge by j in b_j (lines 1-6). For that, the vehicle searches into its main buffer and compares their IDs with the IDs contained in the beacon message b_j. If the vehicle finds any message $warningMsg$ that has not been acknowledged, then it calculates a waiting delay WT_2 to rebroadcast $warningMsg$. This delay will depend on the Equation (6.17). In this case, vehicles closer to the uninformed neighbour receives a lower waiting time than vehicles farther away. Then, the vehicle schedules to rebroadcast $warningMsg$ with delay WT_2(lines 2-4). As in the relaying node selection algorithms, if the vehicle receives a duplicate message, it cancels the rebroadcast (lines 7-11), thus avoiding a possible redundant retransmission. However, when the waiting delay WT_2 expires and the vehicle has not received any duplicate, then it rebroadcasts $warningMsg$ (lines 12-14).

Algorithm 4 Store-Carry-Cooperative Forward Operation

Require: Beacon Message (b), Main buffer,
Ensure: Hold received data messages and replicates whenever find non-informed neighbours
// Check if there is a warning message that has not been acknowledge by neighbour j in Beacon b.
function CompareMainBuffer_IDsMsgsBeacon(IDsMsgsBeacon,MainBuffer)
  if message $warningMsg$ is not acknowledged in b **then**
// Calculate a waiting delay WT_2 to rebroadcast $warningMsg$. See Equation (6.17)
    WT_2 →Waiting Delay
    Schedule rebroadcast timer for found message $warningMsg$
  end if
end function
// A warning message $warningMsg$ is received from neighbour j.
if $warningMsgId$ is duplicated **then**
  if rebroadcast timer for $warningMsg$ is scheduled **then**
    Cancel rebroadcast timer for $warningMsg$
  end if
end if
// Rebroadcast timer expires
function rebroadcastMessage(*Warning Message)
  Rebroadcast message $warningMsg$
end function

6.4.2.1 Adaptive beaconing

In this section we summarize the adaptive traffic beacon (ATB) protocol, that we have included in our ADD game-theoretical dissemination algorithms. Beaconing is the basic supporting process that enables message dissemination; however, this requires a significant amount of bandwidth. The higher the beaconing frequency, the better the accuracy of neighbouring information, but the higher the bandwidth consumption. This means that if the beacon rate was fixed, channel load could increase too much, specially in scenarios with high vehicle density. To tackle this problem, we have implemented the ATB protocol proposed in [86] that adapts the beacon rate continuously to the current environment circunstances. We compute the beacon interval ΔI_i according to Equation (6.18):

$$\Delta I_i = I_{min} + (I_{max} - I_{min}) \cdot I_i \tag{6.18}$$

where I_{min} and I_{max} represent the minimum and the maximum beacon interval, respectively. The interval parameter I_i (in the range [0, 1]) is calculated according to:

$$I_i = \left((1 - W_I) \cdot P_i^2 + W_I \cdot C_i^2\right) \tag{6.19}$$

where P_i is the beacon message priority and C_i represents the current channel condition. The relative impact of those two parameters is configured using an interval weighting factor W_I. Smaller values of P_i and C_i represent a higher priority in the channel access category and a better channel conditions, respectively.

In the following, we briefly introduce the different metrics that the ATB algorithm uses to assess channel conditions and beacon message priority for a given vehicle i.

$$P_i = \overbrace{\frac{A_i + D_{e_i} + D_{r_i}}{3}}^{\textbf{Priority Beacon}} \tag{6.20}$$

$$A_i = \min\left\{\left(\frac{\textit{beacon message age}}{I_{max}}\right)^2; 1\right\} \tag{6.20a}$$

$$D_{e_i} = \min\left\{\left(\frac{\textit{dist. to event}/\textit{speed}_i}{I_{max}}\right)^2; 1\right\} \tag{6.20b}$$

$$D_{r_i} = \max\left\{0; 1 - \sqrt{\frac{\textit{dist. to junction}/\textit{speed}_i}{I_{max}}}\right\} \tag{6.20c}$$

$$C_i = \overbrace{\frac{N_i + W_c \cdot \frac{S_i + K_i}{2}}{1 + W_c}}^{\textbf{Channel conditions}} \tag{6.21}$$

$$N_i = \min\left\{\left(\frac{\#neighbours_i}{\#neighbours_{max}}\right)^2; 1\right\} \tag{6.21a}$$

$$S_i = \max\left\{0; \left(\frac{SNR_i}{SNR_{max}}\right)^2\right\} \tag{6.21b}$$

$$K_i = 1 - \frac{1}{1 + \#colisions_i} \tag{6.21c}$$

According to the U.S. Department of Transportation [67], intersections are potential points of conflict in any roadway system. Therefore, there is a need for heightened caution and attention when vehicles approach intersections. For a final situation-adaptive beaconing scheme, we propose to include the distance to the next intersection as a factor to increase the beacon rate. In this way, when vehicles approach intersections, those vehicles temporarily increase their beacon rate, as it is presented in Equation 6.20c. A detailed analysis of all the parameters discussed here can be found in [84].

6.4.2.2 Video quality module in ADD

Disseminating video over a VANET is not an easy task because transmission of video should fulfill timing constraints inherent in the delivery and playback of video content. Besides, supporting video transmission is an attractive feature for a wide variety of services such as: traffic management, infotainment, road emergencies and scientific application. For instance, disseminating a video showing vehicles stuck in a traffic jam could be more effective than receiving a text message for a driver to change the current route. On the other hand, the benefits of smart cities also provide infotainment applications for citizens. In the future, information dissemination base stations could be deployed in shopping mall, museums, theaters and stadiums to send advertisements offering smart services to passing drivers using VANETs.

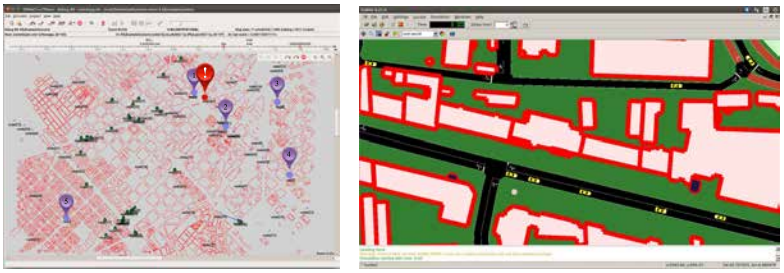
A key component to efficiently transport video with its stringent playout deadlines and bursty traffic characteristics, is using the most–efficient current encoding format. According to our previous studies [42] [41], H.265 allows us to transport higher quality videos with better resolution at the same bit rates of previous generation codecs, reducing the overall cost of video delivery while improving on the quality of experience for users. The latest versions of HM (**H**EVC Test **M**odel) [4] reference software model was used for encoding video sequences with H.265/HEVC. We use two coding parameters: the Constant Rate Factor (CRF) and the encoding mode as a strategy for maintaining high quality video. The video traces were built with the following structure: frame sequence number n, cumulative display time T_n, frame type (I, P, or B) and frame size X_n (in bits).

6.5 Performance evaluation

We evaluate ADD by means of several simulations to show its feasibility in a realistic urban scenario. We compare its performance with other similar approaches. In the following, we describe the experiments and discuss the results.

Vehicle Type	**Maximum Speed [m/s]**	**Lengh [m]**	**Height [m]**	**Probability %**
Slow Car	14	5	2	5
Car	25	4	2	69
Fast Car	33	4	3	1
Bus	17	12	3.4	25

Table 6.3: Vehicle types and associated probability in urban scenarios. SUMO parameters.



(a) OMNet++ (b) SUMO

Fig. 6.2: Screenshots of OMNet++ and SUMO simulators' graphical user interfaces running network and road traffic simulations, respectively. Vehicular network scenario in OMNeT++: 2.5 x 2.5 km^2 urban region in Berlin, Germany (red rectangles = buildings; red circle = crashed vehicle; green circles = warned vehicles; purple circles = RSUs)

6.5.1 Framework

We have employed OMNeT++ [8] to perform the simulations and SUMO [10] to generate the vehicular movement traces. OMNeT++ provides a baseline to develop different type of projects which implement models for several network protocols. Two of these projects, INET [5] and VEINS [11], have been put together to provide a vehicular network simulator. SUMO reports to OMNeT++ with the mobility model with vehicles and their current positions at each simulation step using Traci interface. For a more realistic mobility behavior, we defined a scenario including different type of vehicles (car, bus and truck) with an associated probability of occurrence and maximum speed presented in Table 6.3. All vehicles are moving according to the SUMO standard Krauss driver model. Besides, seeking to dispose a scenario prepared as much realistic as possible, we use real maps extracted from OpenStreetMap [9]. Specifically, we used a map of Berlin, Germany.

6.5.2 Simulation setup

To carry out the performance of our proposal and compare the results with the other analyzed dissemination schemes, we have prepared each run with a different random scenario that fulfils the requirements of the study. For each point in all figures, we have calculated the average from 10 simulation runs, each with a different seed. This let us obtain a standard error less than 5% in a 95% confidence interval. The Medium Access Control (MAC) layer is used in the IEEE 802.11p, using a data rate of 6 Mbit/s, a transmission power

	Parameter	Value
Physics and MAC Layers IEEE 802.11p	Bandwidth	10 MHz
	Channel Frecuency	5.89 GHZ
	Transmission range	∼300 m. Defined in [20]
	Transmission power	10 mW
	Sensitivity	-89 dBm
	Obstacle model	Defined in [21], [84]
	AC_{BE} [CWmin, CWmax], AIFSN	[15,1023], 6
	AC_{VI} [CWmin, CWmax], AIFSN	[7,15], 3
	Bit rate	6 Mbps
ADD	RSS_{th}, RSS_{max}	$-89\ dBm$, $-20\ dBm$
	Time slot	$13\ \mu s$
	Time window	$10\ sec$
	δ (Waiting Time)	$[1, 11]\ \mu s$
	Beacon frecuency	Defined in [85]
	Beacon size	$>= 32\ B$
	Data size	$2312\ B$
	Video file size	$5399\ KB$
	Video Codec	H.265/HEVC, yuv420p, 25 fps Low-Delay P (LP)
	Constant Rate Factor (CRF)	28
	Duration	1min 20sec
	Video resolution	640x360
Adaptive Beaconing	I_{min}	$30\ ms$
	I_{max}	$10\ s$
	W_I	0.35
	W_C	0.5
NJL NSF	Warning message size	$256\ B$
	Beacon Message size	$512\ B$
	Warning messages priority	AC_3
	Beacon priority	AC_1
	Beacon frecuency	1 Hz (1 beacon per second)
RCP+	RSS_{th}, RSS_{max}	$-89\ dBm$, $-20\ dBm$
	Time slot	$13\ \mu s$
	Time window	$10\ sec$
	δ (Waiting Time)	$[1, 11]\ \mu s$
Flooding-Distance	$MaxTime$	$500ms$
	Counter C	1 $(80, 100, 200, 300\ veh./\text{km}^2)$
		2 $(60\ veh./\text{km}^2)$
		3 $(20, 40\ veh./\text{km}^2)$
Scenarios	Number of Runs	10
	Time to live (TTL)	30s (text), 120s (video)
	Vehicles' density	$20, 40, 60, 80, 100, 200, 300\ veh./\text{km}^2$
	Area of interest to warn vehicles	2.5 x 2.5 km^2

Table 6.4: Simulation parameters.

of 10 mW, and a receiver sensitivity of -89 dBm. Beacon messages use the Access Category AC_BE, whereas data traffic uses AC_VI. Internally, ADD calculates the so-called interval parameter I, which is later used to adapt the beacon interval in all simulation scenarios. Table 6.4 contains a summary of the simulation parameters common to all the simulation scenarios evaluated.

6.5.3 Scenario description

We focus on the immediate consequences of an accident on a city road. The crashed vehicle starts to generate and transmit an SOS alert after the collision to warn neighbouring vehicles and to alert the appropriate emergency centers (*e.g.*, 112 or 911) as quickly as possible in a distributed way. In a first scenario, we have evaluated the performance of the dissemination of a text message. A vehicle positioned approximately at the center of the network is responsible for generating a single warning message to be disseminated in a time to live (TTL) of 30s. Additionally, a second scenario is evaluated when the crashed vehicle starts to generate and transmit a short video information of the last 40 seconds before the crash and the 40 seconds after the accident in a TTL of 120s. We have prepared pre-compressed sequences of video and produced trace files with the information needed for the simulation, that is, we prepare the video frames and encapsulate them in packets. We have also included the frame sequence number in order to be able to compare the received decompressed video with the original video sequence. For our evaluation, we have used an *Urban* video stream, which is publicly available at [12]. It is the CIF (Common Intermediate Format) version which contains 2400 frames encoded with H.265/HEVC [4]. Constant Rate Factor (CRF)=28 was selected and used to control quality level of the HEVC encoded sequence. A set of 4 RSUs have been strategically located at 20m, 300m, 600m, 1200m and 1500m from-scene, and the distance between the RSUs and the road is 3m. Notice that those RSUs are used just as traffic sinks to receive the video warning messages, in order to be able to measure the quality of the received video at several fixed distances from the incident. Figure 6.2a shows the map section considered, where buildings represented by pink rectangles are radio obstacles. This segment has an area of 2.5 x 2.5 km^2 and was retrieved from OpenStreetMaps [9]. Shadowing models are used to reproduce the attenuation of a radio signal induced by obstacles, such as buildings or other vehicles blocking the direct line of sight.

6.5.4 Performance measures

In this chapter, we use four metrics to evaluate our two message dissemination protocols:

- *Packet Delivery Ratio* (PDR): It indicates the percentage of vehicles that received a single emergency message within a specified period of time T. We set $T = 30s$ in our evaluations.
- *Average Packet Delay* (APD): It provides the average time from creating a message until it is finally received by the destination node.
- *Broadcast Overhead* (BO): It is measured as the number of global duplicate packets in a defined area.
- *Number of collision packets* (NCP): It is measured as the amount of packet collisions into the network topology during the data dissemination.

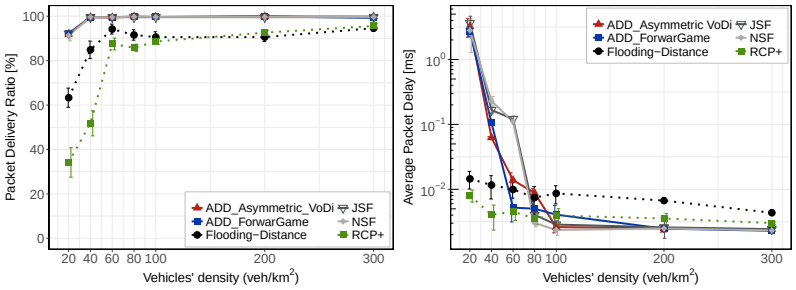
Additionally, we use two performance metrics to evaluate the quality of the video received:

- *Frame Delivery Ratio* (FDR): It is defined as the ratio between the number of frames delivered and the total number of frames received during a time interval $T = 120s$.
- *Peak Signal-to-Noise Ratio* (PSNR): It is an objective metric used to assess the application-level QoS of video transmissions. PSNR measures the error between the reconstructed image and the original one, frame by frame.

6.5.5 Simulation results for text message dissemination

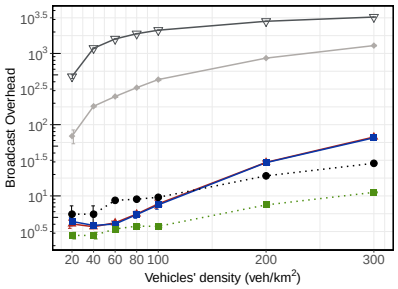
In this section, we present some representative simulation results after a performance evaluation of our ADDs proposals compared to other approaches. Our goal is to study the capability dissemination of our proposal ADD under realistic urban scenarios. To do so, we have implemented the code of ADD with both the Volunteer's Dilemma and the Forwarding Game as selection mechanisms of the next forwarding vehicle or vehicles. The purpose of the performance evaluation was to compare ADD with three well-known state-of-the-art protocols: Junction Store and Forward (JSF) [75], Neighbour Store and Forward (NSF) [74], RCP+ [41] and a simple flooding approach (Distance-Flooding) [91], in light of a realistic simulation environment.

- *Junction Store and Forward* (JSF) [75]: JSF is a protocol designed to exploit the road topology by considering that vehicles rebroadcasts the message every time they arrive at a new junction until the message timer expires. According to the JSF protocol, vehicles can store warning messages until a better communicating situation arises. This scheme requires

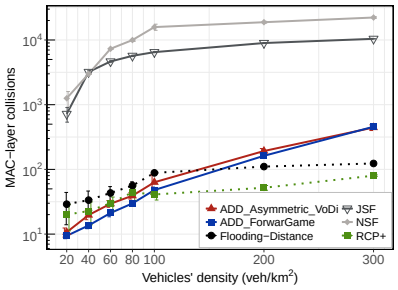


(a) Packet Delivery Ratio (PDR)

(b) Average Packet Delay (APD)



(c) Broadcast Overhead (BO)



(d) Number of collisions per received packet (NCP).

Fig. 6.3: Results with 95% confidence intervals for 10 repetitions per point with independent seeds. Text dissemination case. Different vehicles' densities in a 2.5 x 2.5 km^2 urban region in Berlin, Germany.

each vehicle to maintain a neighbours' table, which is updated taking advantage of the beacons exchanged by the vehicles. In adition, vehicles are assumed to use the information provided by the GPS to decide if a vehicle is near an intersection.

- *Neighbour Store and Forward* (NSF) [74]: NSF protocol was designed to tackle low density conditions. The behaviour of NSF is the following: after receiving a warning message, the vehicle waits until it finds a new neighbour to rebroadcast the message, that is, until it receives a beacon from another vehicle which is not contained in the neighbours' table.
- *Road Casting Protocol* (RCP+) [41]: It is an efficient delay-based forwarding mechanism. It selects a set of forwarders with regard to the distances between the sender, the forwarder and the intersections; as well as the link quality estimated by means of channel quality, signal quality, and collision probability.
- *Flooding-Distance* [91]: This scheme relies on the concept of every vehicle having an internal counter of the number of times that a certain packet is received. The parameters employed by this algorithm are: the number of copies (C) that a node should hear a message to

stop rebroadcasting that message, the maximum time ($MaxTime$) to rebroadcast and the shortest value between the distances to the original sending node ($OriginalDistance$) and the re-broadcaster node ($RebroadcasterDistance$). All optimal values for the urban scenarios are presented in Table 6.4.

Figure 6.3 shows the results for an urban scenario when varying the network density from 20 to 300 $veh./\text{km}^2$. First, we evaluate the global effectiveness of our solutions. We consider that the dissemination protocol is effective if it is able to deliver the information about the emergency event to all vehicles before the time period expires. The time of the packet delivery for various VANET applications is defined in [46]. Figure 6.3a shows the packet delivery ratio of all aforementioned protocols. ADD, JSF and NSF achieve near 100% in delivery ratio for densities higher than 40 $veh./\text{km}^2$. Notice that ADD-Forwarding Game and ADD-Volunteer's Dilemma have a high performance for high traffic scenarios. This result was expected since both protocols were designed to mitigate the broadcast storm problem. In contrast, RCP+ and Distance-Flooding present lower delivery ratio, even in high densities. In a low traffic scenario (20 $veh./\text{km}^2$), ADD, JSF and NSF schemes deliver the message about 90% of the vehicles. On the other hand, RCP+ and Distance-Flooding present lower delivery ratio. This is fundamentally because at the moment that an emergency message is generated, there may happen that no vehicle is in neighbourhood to receive and disseminate the message to other vehicles on the road. Nevertheless, both ADD, NSF and JSF protocols present an improvement of near 45% in very low densities in terms of PDR, compared to RCP+ and Distance-Flooding schemes. This is explained by the fact that these protocols lack an SCF forwarding. Thus, nodes cannot replicate the packet copies when the message has never been forwarded.

Moreover, the end-to-end delay shown in Figure 6.3b is the average delay it takes to disseminate a data packet from the source to all vehicles within the area of interest. In terms of end-to-end delay, SCF mechanism of ADD, JSF and NSF protocols incur longer delay for some messages compared to RCP+ and Distance-Flooding schemes when varying the network density from 20 to 60 $veh./\text{km}^2$. This is explained by the fact that in low densities, ADD, JSF and NSF protocols have to frequently resort to using their SCF mechanisms. Thus, their performance in terms of end-to-end delay and delivery ratio becomes dependent on the movement of nodes. The increase in end-to-end delay in ADD-Forwarding Game and ADD-Volunteer's Dilemma are due to the scheduling, the waiting time of 5 ms required before contending with other nodes for re-transmission at each hop and mainly to the Store-Carry-Cooperative Forward (SCCF) module. As the traffic density increases from 80 to 300 $veh./\text{km}^2$, all protocols show the lowest delay since they do not have to resort to using their SCF mechanisms. Besides, we see how all schemes are far below the 100 milliseconds delay limit requirement defined in [23] for safety messages dissemination. This shows that ADD is able to

quickly disseminate messages whenever there exists end-to-end connectivity to one of the fixed vehicles responsible for gathering data messages.

Finally, the overhead and collision metrics allow us to assess the efficiency of our porposal. Because a high number of transmissions could lead to overload the network unnecessarily, RCP+, Distance-Flooding, ADD-Forwarding Game and ADD-Volunteer's Dilemma protocols were designed to minimize the number of message transmissions in the network. As shown in Figure 6.3c, both ADD approaches, RCP+ and Distance-Flooding strongly decrease the number of messages exchanged, providing better results than JSF and NSF. Note that the lack of the SCF module in the RCP+ and Flooding-Distance schemes produces a low overhead. With our dissemination mechanisms, the number of messages decreases after a few seconds because when informed vehicles receive a beacon from an uniformed vehicle, they use SCCF mechanism to coordinate the rebroadcast of the message, thus avoiding redundant retransmissions. On the contrary, nodes with JSF or NSF will try to replicate the packet to all the neighbouring nodes it encountered. Therefore, massive packet replications will impose a serious overhead. This overhead is not significant at low densities, although it could become a problem in scenarios with high vehicle densities. In general, JSF and NSF schemes efficiently disseminate messages in both dense and sparse vehicular networks. More specifically, they achieve a high delivery ratio with a low propagation delay in case of text dissemination, although both introduce excessive load in the network. Alternatively, ADD is a cross-layer dissemination protocol capable to alleviate load by means of optimizing the packet forwarding mechanism. We also examined the performance of the wireless channel by measuring the number of collisions per received packet, which are depicted in Figure 6.3d on a log-scale. Adaptive beaconing always leads to a moderated number of collisions. However, the number of collisions caused by a static beaconing exponentially increases with the number of nodes in the network. In section 6.5.6, we evaluate the performance of the adaptive beaconing module.

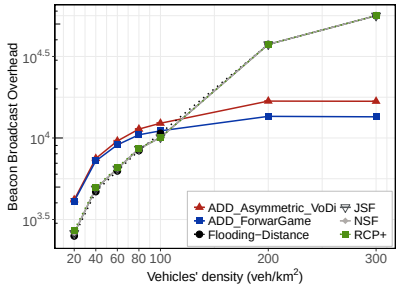


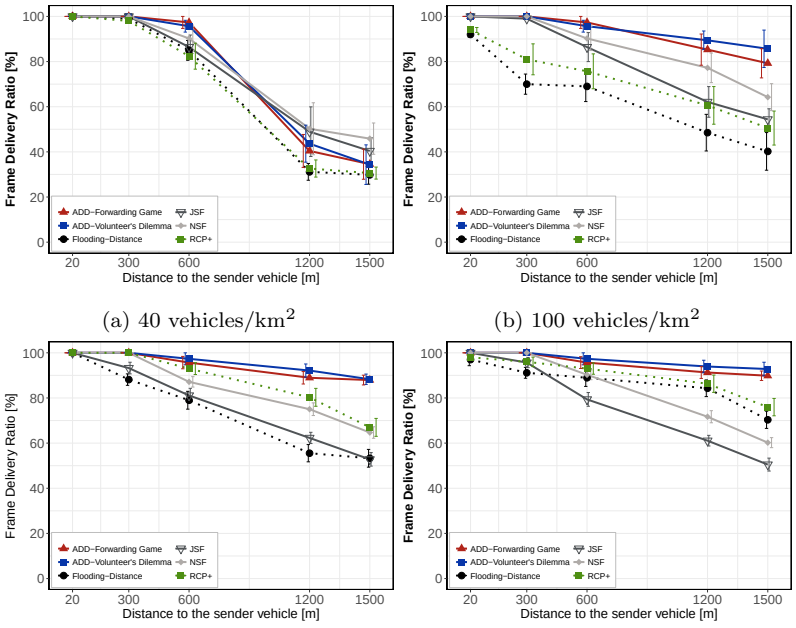
Fig. 6.4: Beacon Overhead

6.5.6 Simulation results for adaptive beaconing

Exchanging vehicle information via beacon messages is an important feature for all schemes. All these protocols need beacon messages to discover neighbours and share local information. However, due to the beaconing periodic transmission, a substantially high load may be caused in the wireless channel. Our ADD proposals include an adaptive beaconing module, whereas RCP+, Distance-Flooding, JSF and NSF use a static beaconing scheme. ADD's limits are configured accordingly to $I_{min} = 30ms$ and $I_{max} = 10s$ while the beaconing period of JSF and NSF is set to a traditional $1s$. Figure 6.4 depicts the effects of adapting the beacon rate in our proposal. According to the beacon overhead obtained, Distance-Flooding scheme, RCP+, JSF and NSF protocols introduce a lower overhead in the network for low to medium vehicles' density, from 20 to 80 $veh./\text{km}^2$. Both ADD schemes perform better under high vehicular density scenarios (in the interval between 100 and 300 $veh./\text{km}^2$). Concluding, adaptive beaconing can reduce significantly the number of beacons. Nonetheless, it is important to take into account that beacon sizes depend on the type and purpose of protocols. While beacons in Distance-Flooding, RCP+, JSF and NSF are considered as small packets periodically broadcast, the size of the beacon in ADD vary depending on the amount of data carried. In fact, beacons used by ADD contains a list of packet identifiers and this beacon could be notably large when there are a lot of packets being sent in the network. This could lead to an unpredictable behavior in the network and it could cause a scalability problem. To avoid this problem, in [59] authors proposed an efficient beacon solution that uses a Bloom filter. For that reason, we also plan to design a specific Bloom filter to represent the data inside of beacons as pointed out in section 6.6.

6.5.7 Simulation results for video warning message dissemination

In this section, we present some representative simulation results for video content dissemination. Our goal is to study the dissemination capability of ADD under urban realistic scenarios. As seen previously, a video sequence is composed of I, P, and B-frames. We have evaluated the performance of the Frame Delivery Ratio (FDR), that is, the rate in which video frames are successfully delivered to each destination. Figure. 6.5a shows the FDR for light vehicle density 40 $veh./\text{km}^2$. A low density of vehicles directly affects the ability of the protocols to disseminate through the VANET. In fact, only RSU_1 ($20m$) and RSU_2 ($300m$) from the accident, received the complete trace. At RSU_3 located 600 m from the accident, ADD reaches an FDR of 97% and 95% with forwarding game and volunteer's dilemma, respectively. In



(a) 40 vehicles/km^2 (b) 100 vehicles/km^2

(c) 200 vehicles/km^2 (d) 300 vehicles/km^2

Fig. 6.5: Frame delivery ratio (FDR) with 95% confidence intervals for 10 repetitions per point with independent seeds. Video dissemination case. Different vehicles' densities in a 2.5 x 2.5 km^2 urban region in Berlin, Germany.

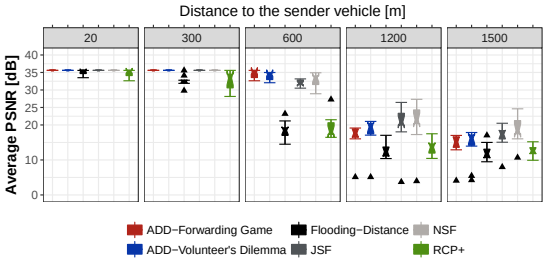
the NSF, JSF, Flooding-Distance and RCP+ schemes we obtain an FDR of 90%, 86%, 84% and 82% respectively. At the RSUs located at 1200 and 1500 m. all the protocols keep an FDR below 50% of received frames. This result is expected, because at the moment that a video packet is generated, there are cases where no vehicle is in neighbourhood to receive and disseminate the video packet to other vehicles around. Also, it is known that an urban scenario suffers more difficulties in the packet loss due to the existence of buildings. This causes temporary disconnections, interrupts the dissemination and compromises the delivery of the frames.

Figure 6.5b shows the FDR for 100 *veh.*/km^2. A moderated density of vehicles improves the FDR. This is evident in RSU$_3$ (600m), RSU$_4$ (1200m) and RSU$_5$ (1500m) where the FDR increases with respect to Figure 6.5a for all the tested schemes. For instance, at RSU$_3$ located 600 m from the accident, ADD reaches an average maximum rate of 97% and 95% with forwarding game and volunteer's dilemma, respectively, while in the JSF, NSF, Flooding-Distance and RCP+ schemes, we obtain an FDR of 86%, 90%, 69% and 75% respectively. At the RSUs located at 1500 m., JSF, NSF, Flooding-Distance and RCP+ schemes keep an FDR below 64% of received frames. Conversely, ADD reaches an average maximum rate of 79% and 85% with

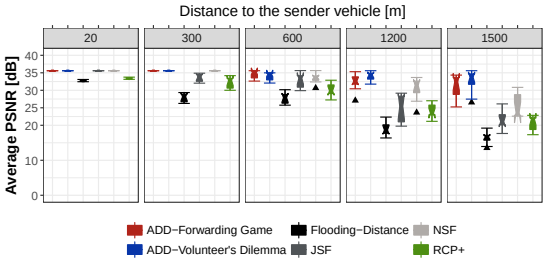
forwarding game and volunteer's dilemma, respectively. Here we can notice how the game-theoretical schemes allow us to achieve a better performance in comparison to the other schemes. Figure. 6.5c shows the frame delivery rate for a heavy vehicles' density (200 $veh./\text{km}^2$). In all RSUs, ADD-Forwarding Game and ADD-Volunteers' Dilemma schemes reach levels above 88% of received frames. We can see that most schemes are able to provide more than 78% of the FDR at a distance of $600m.$ from the accident. We can also notice that ADD is able to improve the FDR between $1200m.$ and $1500m.$. This is due to the reduced number of collisions produced when ADD is used. Figure. 6.5d shows the FDR for high vehicles density (300 $veh./\text{km}^2$). A traffic jam situation directly affects the ability of JSF and NSF schemes to disseminate video messages, since in this scenario, the number of collisions increases exponentially as it can be seen in the Figure 6.3d. This retrains the progress of the packets and consequently, the information will reach closer vehicles only. This can be seen at $\text{RSU}_4(1200m)$ and $\text{RSU}_5(1500m)$ where the FDR does not exceed 60% of received frames despite a high connectivity in the network. It is important to highlight that JSF and NSF protocols were designed for the effective dissemination of text messages at low vehicles' densities [76]. However, these same characteristics that make them successful disseminators in low densities end up affecting their performance in high densities. While JSF resends video messages in an unlimited number of junctions, NSF resends video messages each time it finds a new neighbour. We can also notice that RCP+ and Distance-Flooding are able to improve the packet delivery ratio. This is due to the reduced number of collisions produced when these schemes are used. In all RSUs, ADD-Forwarding Game and ADD-Volunteers' Dilemma schemes are able to deliver more than a 90% of the frames at a distance as far as $1500m.$ With our dissemination mechanisms, the selection of potential forwarders is controlled by a game-theoretical algorithm (see section 6.2). When the network is partitioned due to low vehicles' density, the SCCF module coordinates the selective forwarding only when informed vehicles receive a beacon from an uniformed vehicle (see Algorithm 14, lines 1- 6), thus avoiding redundant retransmissions.

As a next step, we have evaluated the quality of a received video in terms of the Peak Signal to Noise Ratio (PSNR). We assume that in case an individual video frame was lost, the decoder would replace that lost frame by the last successfully received frame (of same type) instead. So if a frame is dropped, we need to compare the source frame to the previous received frame of the same type. Next, we decoded each frame into its YUV[3] channels. The PSNR of the channels needs to be calculated independently. We just use the Y (luminance) channel, since the human eye is far more sensitive to the presence of noise and distortions in brightness rather than the presence of errors and distortions in the color [97]. According to a classification presented in [17],

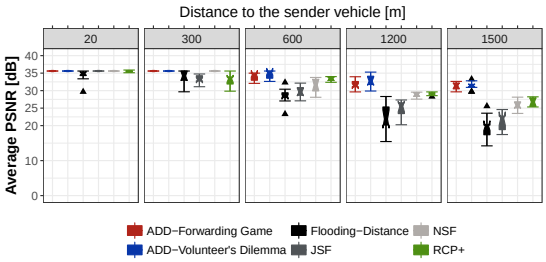
[3] YUV files contain bitmap image data stored in the YUV format, which splits color across Y, U, and V values. It stores the brightness (luminance) as the Y value, and the color (chrominance) as U and V values.



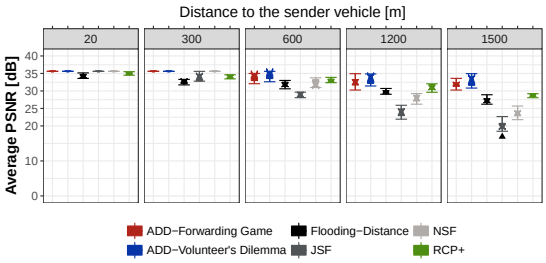
(a) 40 vehicles/km^2



(b) 100 vehicles/km^2



(c) 200 vehicles/km^2



(d) 300 vehicles/km^2

Fig. 6.6: PSNR for video dissemination with 95% confidence intervals for 10 repetitions per point with independent seeds. Different network densities in a 2.5 x 2.5 km^2 urban region in Berlin, Germany.

PSNR values higher than 37 dB, guarantee an excellent video quality on the receiver side. If this value varies between 31 dB and 37 dB, the received video quality will be good. When PSNR values vary between 25 dB and 31 dB we have a fair video quality on the receiver side. If PSNR is lower than 25 dB it provides poor video quality to users. Figure 6.6 shows the average PSNR of the reconstructed video at the receivers' vehicles in RSUs located at 20, 300, 600, 1200 and 1500 m for different traffic densities. These results show how distance and traffic congestion affect video performance at each RSU. Figure. 6.6a shows the average PSNR for low vehicles density ($40 veh./\text{km}^2$). Low vehicles' density directly affects the ability of the protocols to disseminate messages. We can see that the average PSNR in the game-theoretical schemes are all higher than 35dB (good video quality) in RSUs locate at 20 and 300 m. In the RSUs located at 1200 and 1500 m. all the protocols keep a PSNR below 25 dB. This poor quality is caused by temporary disconnections which provoke long loss bursts. As traffic density increases (see Figures 6.6b, 6.6c and 6.6d), we see how the quality of the received video presents a growing trend in all the protocols.

(a) ADD-Forwarding Game (b) ADD-Volunteer's Dilemma

(c) NSF (d) JSF

Fig. 6.7: Comparison sample for the different simulated protocols at frame 72 in RSU_4 located at 1200 m with 100 vehicles/km^2.

As it is illustrated in Figure 6.6d, ADD-Forwarding Game and ADD-Volunteer's Dilemma provide good to excellent video quality ($PSNR > 31$) in all RSUs. On the other hand, RCP+, Distance-Flooding, JSF and NSF schemes provide fair to good video quality ($25 < PSNR < 37$) in RSUs locate at 20, 300, 600 m. In RSU_4 located at 1200 m and RSU_5 located at 1500 m, the average PSNR in JSF and NSF schemes provide poor video qual-

ity ($PSNR < 25$ dB). Despite the good performance of both JSF and NSF schemes in the dissemination of text messages, when we send video messages we observe a poor performance. The reason is that those schemes, which were not specially designed for video dissemination, generate excessive redundant transmissions, which may lead to a broadcast storm problem. In those situations, the network suffers from the increasing administrative load, especially as the number of vehicle nodes increases. Likewise, RCP+ and Distance-Flooding provide fair video quality ($25 < PSNR < 30$). This performance mainly occurs because the video stream suffers from loss bursts associated with the protocol's difficulty to maintain the dissemination and thus compromising the delivery of the video packets. Another interesting observation is that the calculated confidence intervals are quite large which indicates that results vary significantly. The reason for this is that although all video packets are treated in the same way they contain the information of different frames (I and P frames). This information has a different impact on the overall video quality. We randomly selected one sample frame from the transmitted video, aiming to give the reader an idea of the user's point-of-view, as illustrated in Figure 6.7. The frame # 72 is the moment when a person is thrown out of the vehicle. The transmitted sequences using ADD have low distortion compared to the same frame sent using JSF and NSF. This is mainly because ADD-Forwarding Game and ADD-Volunteer's Dilemma schemes do not only relay on the distance factor information, but also consider the position of the vehicle in the network (distance between receiver to next junction, distance between transmitter and receiver), an estimation of the link quality (signal quality, channel quality and collision probability), and an estimation of the available bandwidth. All these factors taken into account improve the video dissemination performance.

In general, video dissemination is a demanding task for any kind of network because of high bandwidth utilization and strict delay requirements. Furthermore, VANETs provide one of the most difficult environments to achieve a good video transmission quality. Results show that ADD is clearly able to perform well in all the investigated scenarios. The comparison shows that ADD-Forwarding Game and ADD-Volunteer's Dilemma are effective and efficient in video dissemination without incurring a high load into the network. In addition with the proposed ADD scheme, real-time video in VANET environments is feasible even in long distances ($1500m.$), if the density of vehicles on the road is moderated or jam ($100 - 300$ $veh./\text{km}^2$). On the other hand, when the vehicular density is low, video transmission is difficult in urban scenarios without a backhaul communication infrastructure. A combination of both protection of packets at network level and error resilience techniques at application level could be welcome to guarantee a high video quality.

6.6 Summary

In this chapter, we have modeled a cooperative game where vehicles have the choice to participate in the data dissemination process or not. First, we have evaluated the use of the asymmetric volunteer's dilemma game as a mechanism for mitigating the broadcast storm in VANETs. An optimized utility function based on distance and link quality was proposed for enhancing data dissemination. Additionally, we have developed a forwarding game where each vehicle has a utility that is a function of its own strategy (its forwarding probability), availability and of the strategy of its neighbours. In this game, an optimized availability function based on distance and an estimated bandwidth was proposed. The availability component of the utility function was designed to improve the network performance by eliminating redundant broadcasts. Both Volunteer's Dilemma and Forward Game have been evaluated in terms of packet delivery ratio, average packet delay, broadcast overhead, and number of collision packets. Also, we focus on a beaconing module that captures both beacon message priority and channel conditions to adapt to highly dynamic environments that change from fully connected to disconnected states. This adaptivity is achieved by nodes continuously sensing their surroundings in order to quickly and dynamically react to changes. In general, ADD selects a minimum set of vehicles to broadcast and also estimates when the broadcast should take place. This way, ADD protocol tries to reduce the load sent to the link layer by decreasing the amount of redundant re-transmissions. Moreover, given that network partitioning is very common in VANETs, independently of the traffic density, received messages are kept in a local buffer to be later forwarded to uninformed vehicles. Simulation results show that the proposed schemes can reduce broadcast overhead and collision packets while still offering acceptable end-to-end delay for most multihop VANET applications. The models developed here provide efficient mechanisms for mitigating the broadcast storm and insights into how vehicular networks can be a platform to develop cooperative communication systems. Future work includes to design a dynamic scheme to update the weights of the multimetric score to calculate the utility function U_i for node i (see Equation (6.14)) so that the algorithm is self-configured and adapts to the changing environment. We will use machine learning techniques to attain this goal. In addition, we plan to extend the model to analyze the behavior of the nodes based on the benefits earned by player i when at least one player volunteers, as an awards strategy for enhancing cooperation. Finally, we will introduce a scalable proactive content discovery scheme, hierarchical bloom-filter routing, to tackle mobility, large population, and rich content challenges of VANETs.

Chapter 7
Performance comparison of encoders in video dissemination

7.1 Introduction

A key component to efficiently disseminate video over VANETs with its stringent playout deadlines and bursty traffic characteristics is using the most–efficient available encoding format. The current video codec standard H.264/AVC provides a better compression efficiency compared to other standards such as H.262/MPEG-2 or VP8. The goal behind the H.264 standard was to provide high-quality video at lower bit rates. However, the emerging of a more efficient next generation video coding standard is a high demand at the moment. Two main contenders for the position of the next state of the art video standard are H.265/HEVC [4] and Google VP9 [13]. H.265/HEVC is the latest video coding standard, which achieves an increase of about 50% in coding efficiency compared to its predecessor H.264/AVC [32]. On the other hand, VP9 is an efficient open source video codec developed as part of the WebM Project by Google to get a royalty-free compression standard with efficiency superior to AVC [82]. In this chapter, we aim to evaluate the efficiency of the video compression standards H.265/HEVC, H.264/AVC and VP9. Our interest is centered on using a video dissemination mechanism in an urban scenario where vehicles' traffic is relatively dense and the communications are more exposed to interferences and radio obstacles. The rest of the chapter is organized as follows: section 7.2 describes the features of selected encoders. section 7.3 discusses the main approach aimed towards an effective solution for video dissemination over VANETs. The performance comparison of encoders and simulation results are discussed and presented in section 7.4. Finally, we conclude in section 7.5 with a summary of this chapter.

7.2 Selected encoder implementations: H.265/HEVC, VP9, and H.264/AVC

In this section, a brief overview of the selected representative encoders is presented.

7.2.0.1 VP9 Encoder.

Google started an Open Source project to develop royalty-free video codecs for the web entitled the WebM Project. The codec developed in the WebM project called is VP9 and is currently being served extensively by Google Chrome and YouTube. To evaluate VP9 compression efficiency, we use the open source libvpx encoder in its version 1.6.0 [13]. It has a two-pass run option which results in the improved rate-distortion performance and which is also used in our work.

7.2.0.2 H.264/AVC Encoder.

The latest version of JM reference software model (JM 19) was used for encoding video sequences with AVC [3]. The H.264/AVC standard has proven to be very fast, reliable, and efficient. Similarly as VP9, H.264/AVC has a two-step run option. At the first pass, a file with the detailed statistic data about every input frame is generated. At the second step, this information is used to improve the encoder rate-distortion performance.

7.2.0.3 H.265/HEVC Encoder.

For evaluating H.265/HEVC-based encoding [4], we selected the latest reference model 16 (HM 16.9) in its simplified model to estimate the compression efficiency of the H.265/HEVC standard. To get constant QP (Quantization Parameter) on each frame we modified *Qpoffset* values of the GOP (Group of Pictures) structure in the configuration file.

The configuration parameters for HEVC, AVC and VP9 were set so that similarity was ensured between the three codecs to avoid any penalization. More details about the configurations can be found in Table 7.1.

Table 7.1: Selected parameters and settings for the AVC, HEVC, and VP9 codecs.

Codec	Version	Parameters
HEVC	HM 16.9	**TAppEncoderStatic** -c encoder_lowdelay_P_main10.cfg (Default main low-delay profile with P frames) -c Traffic.cfg -b encoded sequence.bin -o decoded sequence.yuv -q <QP>
AVC	JM 19	**lencod** -f encoder.cfg -p FrameRate=<FR> -p QPISlice=<QP> -p QPPSlice=<QP> -p QPBSlice=<QP> -p Bitrate= -p SourceWidth=<W> -p SourceHeight=<H>
VP9	v1.6.0-326	**vpxenc** --codec=vp9 --profile=0 --fps=<FR> --static−thresh=0 --drop-frame=0 --good --auto-alt-ref=1 --kf-min-dist=8 --kf-max-dist=8 --cq-level=<QP> --max-intra-rate=8 --target-bitrate= --static-thresh=4 -w <W> -h <H> --limit=500 <inFile>.yuv −o <outFile>.webm

7.2.1 Dataset

The comparison was carried out on the video sequences listed in Table 7.3. Four video sequences were downloaded from [1] and were used in the simulations, with different spatial, temporal characteristics and frame rates.

Each video file was encoded with all three evaluated codecs. Since fixed QP[1] configuration was used to control the quality of AVC, HEVC, and VP9 compressed bitstreams, the sequences were encoded at various QP values trying to cover the full quality scale for each content.

We aim to compare maximum video compression efficiency provided by the latest standards. We selected Low-Delay-P (LP) coding configuration to reflect the real-time application scenario for all encoders. In this mode the first frame is an intra-frame while the others are encoded as generalized P frames. This makes this mode more vulnerable to packet losses since it needs to wait to receive an entire GoP before decoding the video frames. To mitigate large dependencies between frames and trying to achieve a better packet loss resilience, the GOP size was set to 8 pictures and the Intra Period was set to 25 and 30 pictures for 25 and 30 fps contents, respectively. Table 7.2 reports the final sets of targeted (R1'-R4') and actual (R1 - R4) bit rates, with corresponding QPs, for each codec.

[1] The Quantization Parameter (QP) regulates how much spatial detail is saved. When QP is very small, almost all that detail is retained. As QP is increased, some of that detail is aggregated so that the bit rate drops, but at the price of some increase in distortion and some loss of quality.

Table 7.2: Target R_i' and actual R_i bit rates (kbps) including the corresponding QP values for each codec.

Sequence	**Codec**	R1'	**R1**	**QP**	R2'	**R2**	**QP**	R3'	**R3**	QP	R4'	R4	**QP**
Highway	AVC	375	384	30	750	747	24	1500	1574	15	2500	2515	11
	HEVC	375	336	27	750	776	24	1500	1450	21	2500	2717	18
	VP9	375	390	28	750	749	25	1500	1486	22	2500	2833	19
Hall monitor	AVC	375	385	32	750	779	25	1500	1590	17	2500	2877	13
	HEVC	375	363	28	750	675	25	1500	1319	22	2500	2452	19
	VP9	375	416	30	750	787	26	1500	1640	22	2500	2370	20
City	AVC	256	242	58	512	520	33	1024	1010	23	2048	2087	12
	HEVC	256	235	35	512	508	29	1024	1392	24	2048	2041	19
	VP9	256	253	37	512	535	31	1024	1126	25	2048	2195	20
Bus	AVC	256	251	54	512	539	43	1024	1006	34	2048	2038	22
	HEVC	256	248	40	512	514	34	1024	997	29	2048	2089	23
	VP9	256	267	41	512	512	36	1024	1080	30	2048	2192	24

7.3 Video dissemination in VANETs

The realization of a reliable transmission of video over VANETs is extremely challenging mainly due to the network's dynamic topology and stringent requirements of the video streaming service. The high velocity and limited communication range of the vehicles incur frequent link disconnection and even network partition. To evaluate the efficiency of the video compression standards over VANETs, we use a smart dissemination protocol known as RCP+ that we proposed in chapter 5. The proposed mechanism is built on top of IEEE 1609.3 by adding a layer to select next forwarder vehicles based on the information of the environment and an estimation of the congestion of the communication channel. RCP+ ensures a large dissemination in the network to rebroadcast the video content.

Table 7.3: Test video sequences have a resolution of 352x288 pixels

Sequence	**Frame rate**	**Number of frames**
Highway	25 fps	2000
Hall monitor	30 fps	300
City	30 fps	300
Bus	25 fps	150

Table 7.4: Simulation parameters.

	Parameter	Value
Physic and MAC Layers IEEE 802.11p	Channel; Bandwidth	178, 5.89 GHZ ; 10 MHz
	Transmission range	230m
	Transmission power	20 mW
	Obstacle model	Defined in [21], [84]
	Beacon [CW_{min}, CW_{max}], AIFSN	[15,1023], 6
	Data [CW_{min}, CW_{max}], AIFSN	[7,15], 3
	Bit rate	6Mbit/s
RCP+	RSS_{th}, RSS_{max}	$-89dBm$, $-20dBm$
	Time slot	$13\mu s$
	Time window	$10sec$
	δ (Waiting Time)	$[1, 11]\mu s$
	Beacon frecuency, Beacon size	1 Hz, >=32 bytes
Scenarios	Number of Runs per point	10
	Time to live (TTL)	90s

7.3.1 Scenario description

We focus the situation on the immediate consequences of a traffic accident. The crashed vehicle starts to generate and transmit a real–time SOS message to alert the vehicles in the network about the incident and to the appropriate emergency centers (*e.g.* 112 or 911). The emergency message includes a short video of a few seconds before the crash. We consider a real street environment imported from OpenStreetMap [9]. Under the street model, vehicles are generated and their moving patterns are controlled by SUMO [10]. Shadowing models are used to reproduce the attenuation of a radio signal induced by obstacles, such as buildings or other structures blocking the direct line of sight. A set of 4 RSUs (Road Side Units) have been strategically located at 20m, 300m, 600m, and 1200m from the accident scene. The distance between the RSUs and the road is 3m. RSUs are traffic sinks used to measure the quality of the received video at different distances from the accident.

7.4 Performance evaluation

This section provides simulation results on the coding performance of the three video coding standards under evaluation. We first present the simulation setup used, including models and scenarios. Then, we present the comparison of the compression efficiency between HEVC, VP9 and AVC by means of objective and subjective evaluations in the considered VANET video streaming scenario.

7.4.1 Simulation setup

To carry out the performance comparison, each run uses a different random scenario that fulfills the requirements of the study. For each point in all figures we have calculated the average from 10 simulation runs. This let us obtain a standard error less than 5% in a 95% confidence interval. The packet error and Medium Access Control (MAC) layer models adopted are based on the IEEE 802.11p, using a data rate of 6 Mbit/s, a transmission power of 20 mW, and a receiver sensitivity of -89 dBm. In addition, all hello messages use the same Access Category (AC_BE), thus with the same values of Contention Window (CW) and Arbitration Inter-Frame Spacing (AIFSN). Table 7.4 contains a summary of the simulation parameters common to all simulation scenarios.

We assume that each vehicle is equipped with a GPS device to obtain its geographical location in current time. A preloaded digital map provides information about roads. We assume that vehicles periodically exchange their own physical location, moving velocity and direction information enclosed in their periodic hello messages. They are sent at the frequency of 1 Hz. Finally, vehicles are assumed to be equipped with IEEE 802.11p wireless technology and computation capabilities.

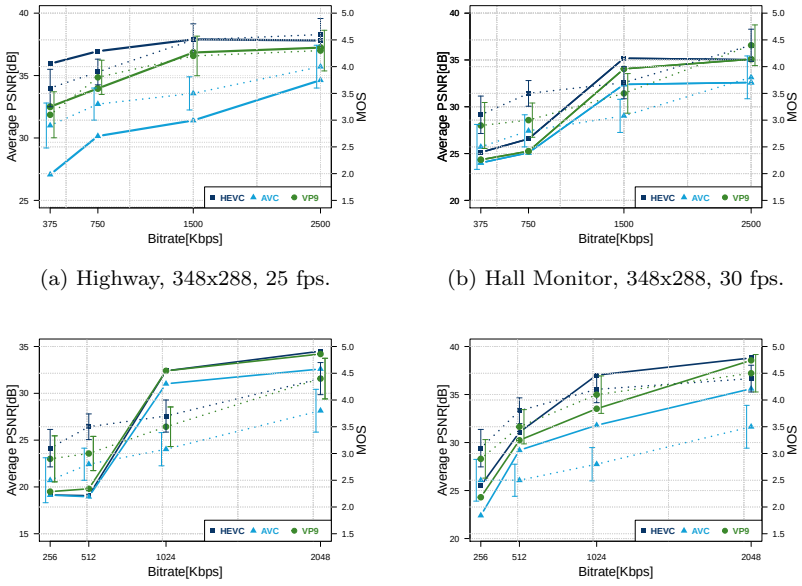
7.4.2 Performance measures

We use three performance metrics to evaluate the quality of video transmitted over VANETs:

Frame Delivery Ratio: It is defined as the ratio between the number of frames delivered and the total number of frames received during a time interval of T seconds.

PSNR(*Peak Signal-to-Noise Ratio*): It is an objective metric used to assess the application-level QoS of video transmissions. PSNR measures the error between the reconstructed image and the original one, frame by frame. We assume that in case an individual frame was lost, the decoder would display the last successfully received frame of the same type. So if a frame is dropped, we need to compare the source frame to the previous streamed frame.

MOS(*Mean Opinion Score*): It is a subjective metric used to provide a numerical indication of the perceived quality from the users's point of view of the received video. In a MOS assessment test, video sequences are presented in a predefined order to a group of subjects, who are asked to rate their visual quality on a rating scale. The MOS score is expressed in the range from 1 to 5, where 5 is the highest perceived quality and 1 is the lowest perceived quality.



(a) Highway, 348x288, 25 fps.

(b) Hall Monitor, 348x288, 30 fps.

(c) City, 348x288, 30 fps.

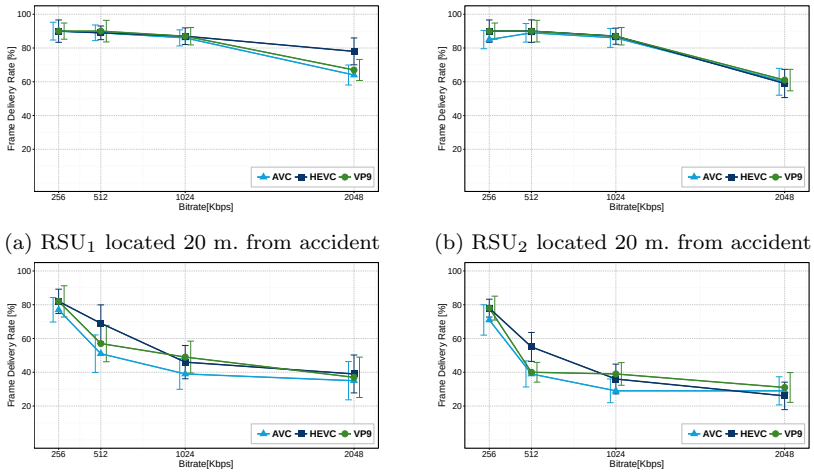
(d) Bus, 348x288, 25 fps.

Fig. 7.1: PSNR (solid line) curves and subjective MOS (dashed line) values, for each bit rate and each video content. 95% confidence intervals are shown.

7.4.3 Results and discussion

In a first set of experiments, we used the Bjϕntegaard model to calculate the coding efficiency between different codecs. This metric allows us to compute the average gain in PSNR or the average per cent saving in bitrate between two rate-distortion curves. Also, we used another model based on subjective quality scores [36]. This model computes the average MOS difference and average bit rate difference between two sets of subjective results corresponding to two different codecs. This model reports the average bit rate difference, ΔR, for a similar perceived visual quality. Table 7.5 provides the results in terms of BD-Rate[2] and Δ R results. Results based on the Bjϕntegaard model show that the average bit rate reduction of HEVC relative to AVC and VP9 is 49.73% and 27.12%, respectively. Also, the average bit rate reduction of VP9 relative to AVC is 38.85%. On the other hand, results based on the subjective ratings indicate an average bit rate saving of 44.11% and 30.35% for HEVC when compared to AVC and VP9, respectively. Furthermore, the bit

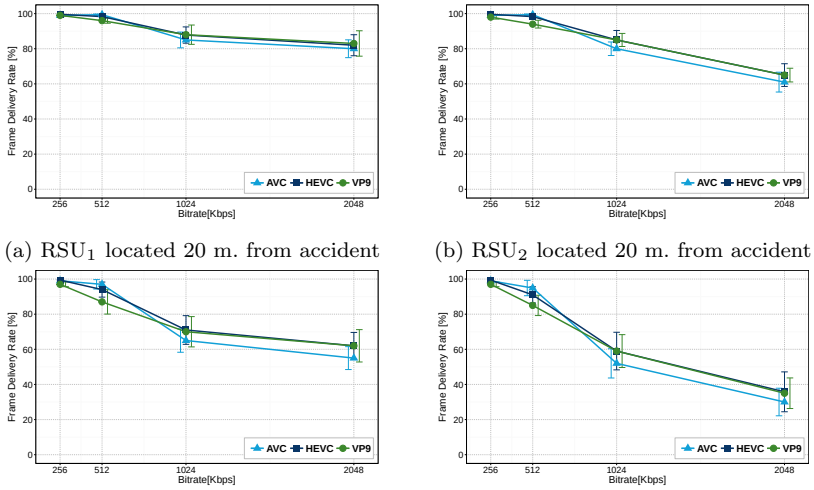
[2] Bjϕntegaard Delta-Rate (BD-Rate) is the average bit rate difference in percentage for the same PSNR.



(a) RSU_1 located 20 m. from accident (b) RSU_2 located 20 m. from accident

(c) RSU_3 located 20 m. from accident. (d) RSU_3 located 20 m. from accident.

Fig. 7.2: Urban medium-density scenario: 60 vehicles/km^2. Frame delivery rates with 95% confidence intervals for the CITY.



(a) RSU_1 located 20 m. from accident (b) RSU_2 located 20 m. from accident

(c) RSU_3 located 20 m. from accident. (d) RSU_3 located 20 m. from accident.

Fig. 7.3: Urban high-density scenario: 120 vehicles/km^2. Frame delivery rates with 95% confidence intervals for the CITY.

rate reduction achieved by VP9 relative to AVC is 35.35%. As it can be seen, HEVC encoder provides better results than all the other codecs avaluated.

As a next step, we carry out a comparative assessment for the Low-Delay-P (LP) configuration of H.265/HEVC, VP9, and H.264/AVC encoders. Fig-

ure 7.1 shows the Rate-Distortion curves based on PSNR measurements and subjective ratings based on MOS measurements for all sequences. Based on PSNR measurements, HEVC outperforms VP9 by 0.5 to 3.5 dB, while VP9 provides a gain ranging from 0.5 to 8.45 dB when compared to AVC. For all video contents and bit rates, objective measurements show that HEVC outperforms both VP9 and AVC coding algorithms. The subjective results show similar trend to objective measurements: HEVC provides the best visual quality for a similar bit rate and outperforms AVC in most cases. Also, VP9 achieves better visual quality than AVC. However, in some cases (in particular, at high bit rates), HEVC and VP9 have similar ratings and there is no sufficient statistical evidence indicating differences in performance between these codecs at these bit rates.

Finally, we compare the effectiveness of the RCP+ scheme in terms of frame delivery rate for each codec. In the urban scenario, we define three densities: 30, 60 and 120 vehicles/km^2. These densities can be considered as Low, Medium, and High densities of vehicles. These network densities cover a range from low (normal or night time) to high vehicular traffic density (rush hour). A vehicle operating in a sparse traffic density is said to be in a totally disconnected neighbourhood if it has no vehicle neighbour within its transmission range. In this case, simulation results (not shown here due to space limits) indicate that only the RSU_1 and RSU_2 located 20 and 300 meters from the accident, received the complete trace. This makes it difficult to evaluate the codec in this scenario. On the other hand, the performance of our mechanism in Medium and High densities are presented in Figures 7.2 and 7.3, respectively. As it is clearly seen, the HEVC encoder provides gains in terms of Frame Delivery Ratio compared to both VP9 and AVC encoders. Also, as the distance from the accident increases for the RSU, the delivery ratio decreases since probability of collisions or network failure increases. This result is expected, because the urban scenario shows more aggressiveness in the packet loss due to the existence of buildings. Besides, dynamic topology networks in VANET causes temporary disconnections, interrupting the video message dissemination and compromising the delivery of the video frames.

Table 7.5: Comparison of the three evaluated coding algorithms in terms of bit rate reduction for similar PSNR and MOS. Negative values indicate actual bit rate reduction.

Sequence	**HEVC vs AVC**		**VP9 vs AVC**		**HEVC vs VP9**	
	BD-Rate	ΔR	BD-Rate	ΔR	BD-Rate	ΔR
highway	-47.41%	-40.11%	-32.48%	-36.58%	-41.19%	-42.79%
hall monitor	-32.60%	-23.70%	-27.38%	-20.08%	-9.57%	-12.80%
city	-51.11%	-47.01%	-42.89%	-34.29%	-21.66%	-26.16%
bus	-67.82%	-65.62%	-52.64%	–50.44%	-36.05%	-39.25%
Average	**-49.73%**	**-44.11%**	**-38.85%**	**-35.35%**	**-27.12%**	**-30.25%**

7.5 Summary

In this chapter, we have studied compression efficiency of the current video compression standard and candidates for the next generation video coding standard over VANETs in an urban traffic scenario. The high bandwidth required for video dissemination can be tackled through the use of recent encoders that allow doubling the efficiency coding, reducing almost half the bit rate for similar levels quality. The results have shown the superior compression efficiency of H.265/HEVC coding standard over H.264/AVC and VP9 encoders. The possible drawback of using H.265/HEVC is a higher computational complexity.

Chapter 8
Privacy issues in VANETs

8.1 Introduction

A VANET could potentially consist of millions of on-road vehicles and RSUs. Such size makes it very challenging to guarantee user-related privacy information, such as the driver's name, the car's license plate, the current car's position, model, and traveling route. Unfortunately, existing studies on communication security and privacy preservation cannot work effectively in VANETs, since they do not take the typical characteristics of vehicular networks into consideration. Privacy in VANETs have recently been studied for many researchers, although most of them do not present information about implementation or evaluation of algorithms working in a realistic environment. In this chapter, we evaluate three location privacy mechanisms as a first step to understand the importance of privacy in VANETs. The rest of the chapter is organized as follows: section 8.2 describes the concept of privacy and presents recommendations to guarantee the vehicle's location privacy. Afterwards, section 8.3 discusses the performance evaluation and includes the results of our analysis. Finally, section 8.4 presents a summary of this chapter.

8.2 Privacy

Most safety applications for VANETs broadcast messages to all neighbours and do not contain secrets to be processed by a specific destination. In VANETs, vehicles periodically broadcast their local data base to neighbouring vehicles. These messages typically contain plaintext information, such as a vehicle's position and speed, which could be used by potential adversaries to determine which messages were generated from the same vehicle in order to be able to track that vehicle. Privacy in VANETs should guarantee

and preserve that the vehicle is anonymous and untraceable. Furthermore, privacy in VANETs should also safeguard the driver's private information during sharing of information with other nodes or vehicles in the network. However, any attacker could also perform traffic analysis to identify a vehicle's unique communication pattern and use those patterns to identify or track the vehicle. To tackle this problem, we have considered the following recommendations:

1. Use randomized pseudonyms.
2. Provide vehicles with the ability to change pseudonyms/certificates simultaneously with further identifiable properties.

If a vehicle uses different pseudonyms along the road, the impossibility of linking pseudonyms can guarantee the vehicle's location privacy. However, if a vehicle changes its pseudonym in a not proper moment, changing the pseudonyms does not serve to protect the privacy of the location, since an adversary could link a new pseudonym with the previous one. Therefore, it is imperative for us to evaluate the location privacy achieved by frequent and changing pseudonyms in a realistic setting. For this, we have unified an extensible framework called PREXT [28] that simulates pseudonymous change schemes to provide privacy in VANETs.

8.2.1 Framework to simulate privacy schemes

Based on [28], we have evaluated a framework that simulates pseudonym change schemes in VANETs. Below we describe each evaluated privacy scheme:

- Periodical pseudonym change (PPC): Each vehicle changes its pseudonyms at fixed [18] or random times.
- Random silent period (RSP): Each vehicle changes its pseudonym after a fixed time and keeps silent for a uniformly random period (*e.g.*, from 3 to 13 s).
- Slow pseudonym change (SPC): Each vehicle checks its current speed and broadcasts beacon messages when its speed is higher than a fixed threshold. If a vehicle does not send beacon messages for a fixed time, it changes its pseudonym.

These privacy schemes allow each vehicle to decide locally when to change a pseudonym and how long that vehicle should be silent based on parameters presented in Table 8.1. Furthermore, to evaluate the efficiency of the mechanisms described above, the framework simulates an adversary whose goal is to track vehicles by collecting beacon messages, as we can see in Figure 8.1. This adversary is used in measuring the gained privacy in terms of several popular privacy metrics such as traceability and pseudonym usage statistics.

We have evaluated the privacy mechanisms assuming the worst scenario, *i.e.*, this adversary has deployed receivers covering the entire road network. Each receiver has an eavesdropper functionality, *i.e.*, they listen to the wireless medium and report the received messages to a central entity called Vehicle Tracker. The central entity collects beacon messages from different eavesdroppers. This vehicle tracking may run the nearest neighbour probabilistic data association (NNPDA) tracking algorithm to reconstruct vehicle traces. The employed tracking algorithm was proposed in [29]. It has shown promising effectiveness in tracking anonymous beacon messages under different densities of vehicles.

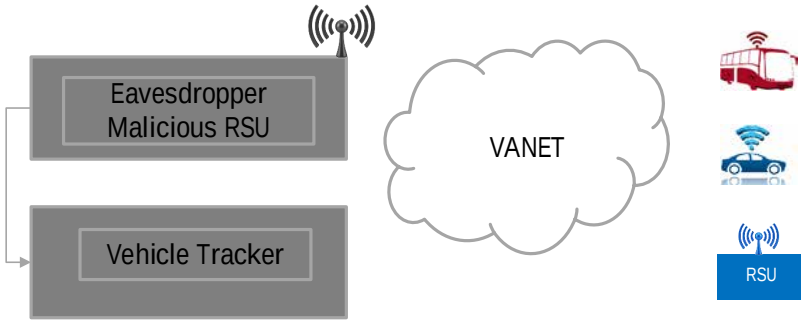


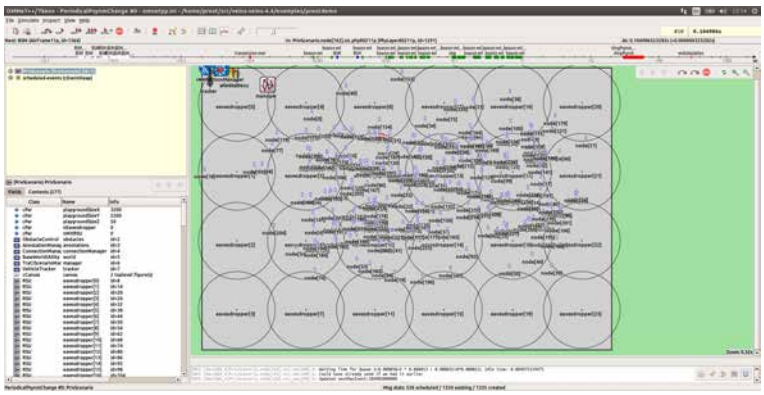
Fig. 8.1: Privacy framework for VANETs

8.3 Performance evaluation

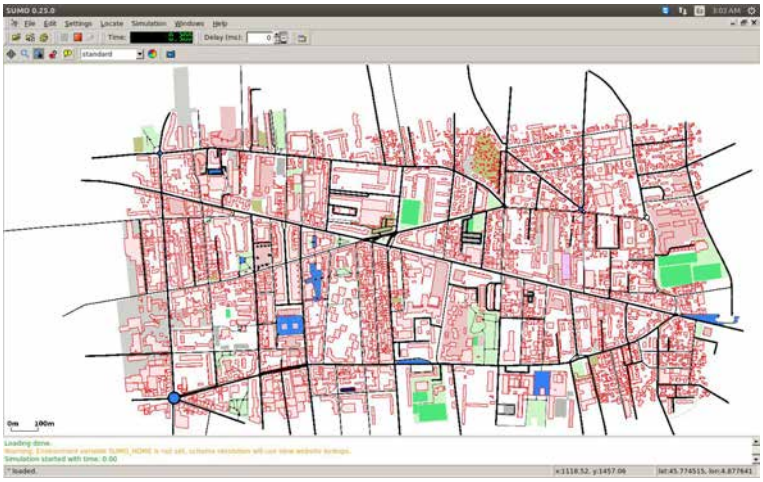
We have evaluated our privacy framework for VANETs showing its efficiency and the performance of the analysed privacy schemes. In the following, we describe the experiments and discuss the results.

8.3.1 Scenario description

The privacy of users is evaluated through simulations in an urban traffic scenario. Each vehicle is equipped with a reliable positioning device (*e.g.*, a global positioning system or GPS) and establishes mutual perceptions by periodically exchanging single-hop status information broadcasts, which include *pseudonym, geographical location, speed, and driving direction.* This type of



(a) OMNet++ [8].



(b) SUMO [10].

Fig. 8.2: Screenshots of OMNet++ and SUMO simulators' graphical user interfaces running network and road traffic simulations, respectively. Vehicular network scenario in OMNeT++: 2.5 x 2.5 km^2 urban region in Berlin, Germany (black circles= full coverage of the adversary for the road network, red rectangles = buildings).

periodic status information exchange is referred to as *beacon messages*. Figure 8.2 shows the map section considered, where buildings represented by pink rectangles are radio obstacles. This segment has an area of 2.5 x 2.5 km^2 and was retrieved from OpenStreetMaps [9]. Shadowing models are used to reproduce the attenuation of a radio signal induced by obstacles, such as buildings or other vehicles blocking the direct line of sight. A global adversary installs 24 malicious receivers (represented by black circles) over the road network which in turn report eavesdropped messages to a central vehicle tracker.

	Parameter	Value
Physics and MAC Layers IEEE 802.11p	Bandwidth	10 MHz
	Frecuency band	5.89 GHZ
	Transmission range	∼500 m
	Transmission power	10 mW
	Sensitivity	-89 dBm
	Obstacle model	Defined in [21], [84]
	AC_{BE} [CWmin, CWmax], AIFSN	[15,1023], 6
	AC_{VI} [CWmin, CWmax], AIFSN	[7,15], 3
	Bit rate	6 Mbit/s
Tracker	Eavesdropper range	$300m$
	Eavesdropper overlap	$30m$
	Track interval	1 sec
Privacy	Periodical pseudonym change (PPC)	Pseudonym lifetime=60 s
	Random silent period (RSP)	Pseudonym lifetime=60 s
	Slow pseudonym change (SPC)	Speed threshold = 8 m/s
		Silent threshold = 5 s
Messages	Beacon frecuency	1 Hz
	Beacon size	>= 32 $bytes$
	Data size	2312 $bytes$
Scenarios	Number of runs	10
	Simulation time	300s
	Vehicles' density	$20, 60, 100$ $veh./km^2$
	Area of interest to warn vehicles	2.5 x 2.5 km^2

Table 8.1: Simulation parameters.

8.3.2 Simulation setup

To carry out the performance of our framework and compare the results with the analyzed privacy schemes, we have prepared each run with a different random scenario that fulfills the requirements of the study. For each point in all figures we have calculated the average from 10 simulation runs, each with a different seed. This let us obtain a standard error less than 5% in a 95% confidence interval. The medium access control (MAC) layer is the used in the IEEE 802.11p, with a data rate of 6 Mbit/s, a transmission power of 20 mW, and a receiver sensitivity of -89 dBm. Beacon messages use the access category AC_BE, whereas data traffic uses AC_VI. Beacon messages are sent at the frequency of 1 Hz in all simulation scenarios. This is usually the highest frequency expected to be used for the transmission of beacon messages which gives the worst-case scenario in terms of freshness of the one-hop neighbourhood information. Table 8.1 contains a summary of the simulation parameters common to all the simulation scenarios evaluated.

8.3.3 Performance measures

In this chapter, we use five metrics to evaluate privacy in our VANET scenario:

- *Vehicle Tracker-Traceability*: It expresses the correctness of an adversary to reconstruct vehicle traces from beacon messages.
- *Vehicle Tracker-N_Traceability*: It expresses the correctness of an adversary to reconstruct vehicle traces from beacon messages. It eliminates vehicles that never changed their pseudonym.
- *VehicleTracker-nTracesChngPsynms*: It provides the total number of vehicles encountered by the tracker that changed their pseudonyms at least once.
- *Vehicle Tracker-nTraces*: It is the total number of vehicles encountered by the tracker.
- *Eavesdropper-nPseudonyms*: It provides the total number of distinct pseudonyms encountered by the eavesdropper.

8.3.4 Privacy schemes comparison

In this section, three different privacy schemes are evaluated in terms of the traceability [28]:

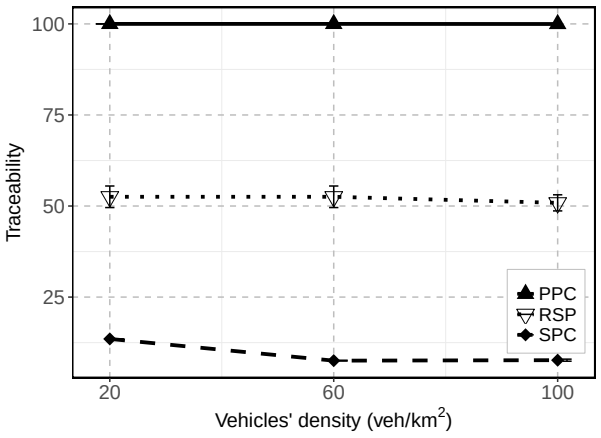
- Periodical pseudonym change (PPC) [69].
- Random silent period (RSP) [92, 38].
- Slow pseudonym change (SPC) [25].

To evaluate the efficiency of the privacy schemes, the framework simulates an adversary whose goal is to track vehicles by collecting beacon messages. The *traceability* metric measures how effective an adversary can track a vehicle continuously for more than 90% of its trace. This continuous monitoring is necessary to practically violate the driver's privacy because traces de-anonymization needs complete trajectories with allowable errors around endpoints. *Normalized traceability* considers the effectiveness of the privacy scheme when a vehicle changes its pseudonym at least once. Traceability and normalized traceability of privacy schemes are shown in Figures 8.3a and 8.3b, respectively.

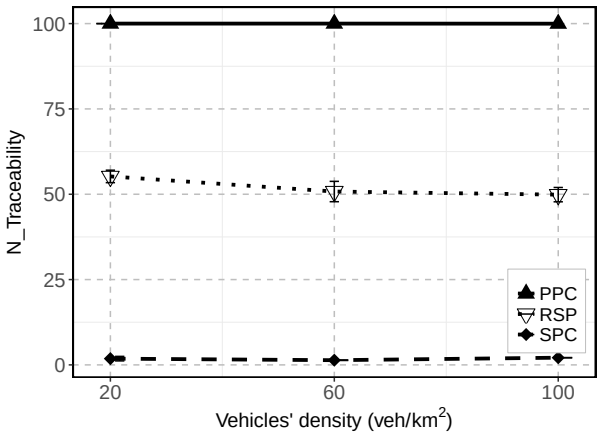
These are the main conclusions obtained after analysing the performance evaluation of the three aforementioned privacy schemes for VANETs in Figure 8.3a:

- PPC scheme cannot reduce traceability (up to 98% regardless the vehicles's density) because it does not employ any discontinuity in the spatiotemporal information broadcast in beacon messages.

- RSP scheme reduces traceability up to 52% due to the silent periods used before a pseudonym change.
- SPC scheme reduces traceability significantly up to 12%. However, SPC could make vehicles silent for almost 45% of their lifetime on average. This silence reduces the targeted traffic awareness and may negatively impact the functionality of applications.



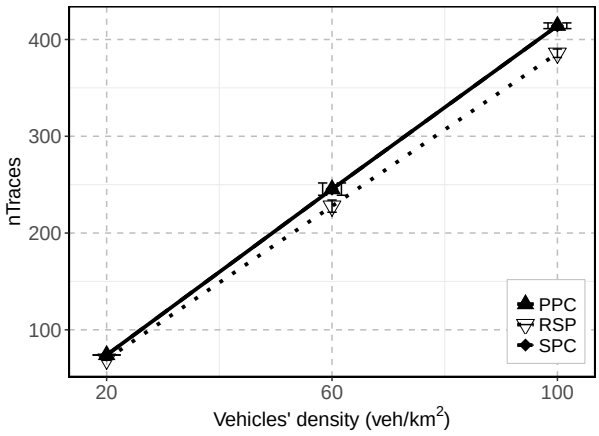
(a) Traceability



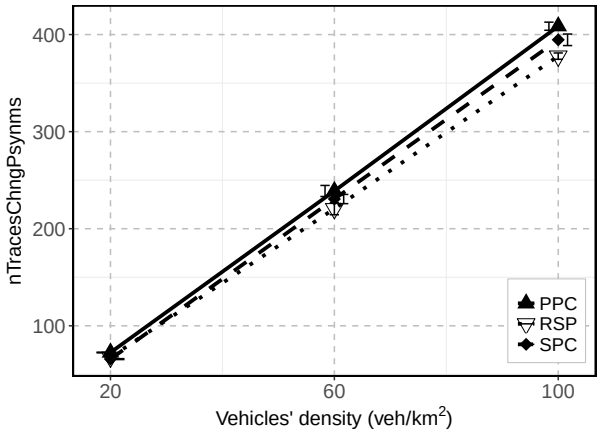
(b) N_traceability

Fig. 8.3: Results with 95% confidence intervals for 10 repetitions per point with independent seeds. Different network densities in a 2.5 x 2.5 km^2 urban region in Berlin, Germany.

Figure 8.4a presents the total number of vehicles encountered by the tracker. The total number of vehicles encountered by the tracker that changed their pseudonyms at least once is presented in Figure 8.4b.



(a) Vehicle Tracker-nTraces: Total number of vehicles encountered by the tracker.



(b) Vehicle Tracker-nTracesChngPsynms: Total number of vehicles encountered by the tracker and changed their pseudonyms at least once.

Fig. 8.4: Results with 95% confidence intervals for 10 repetitions per point with independent seeds. Different network densities in a 2.5 x 2.5 km^2 urban region in Berlin, Germany.

Periodical pseudonym change (PPC) Random silent period (RSP) Slow pseudonym change (SPC)

Table 8.2: Comparison of the three evaluated privacy schemes in terms of total number of distinct pseudonyms encountered by each eavesdropper for different vehicles' densities.

Malicious RSU	**20** *veh.*/**km**^{2}			**60** *veh.*/**km**^{2}			**100** *veh.*/**km**^{2}		
	PPC	RSP	SPC	PPC	RSP	SPC	PPC	RSP	SPC
Eavesdropper[0]	1	1	1	3.8	3.3	3.8	8.6	7.6	8.2
Eavesdropper[1]	4.3	3.7	2	20.8	16.3	19.2	32.4	26	29.2
Eavesdropper[2]	0	0	0	4.6	4.2	4.4	5.6	4.8	5.4
Eavesdropper[3]	0	0	0	0	0	0	0	0	0
Eavesdropper[4]	21.3	16.2	19.7	89.5	72.6	93.9	154.4	124.4	152.6
Eavesdropper[5]	62.1	51.4	60	212.2	176.6	229.9	374.8	301.2	355
Eavesdropper[6]	39.5	29.3	41	129.1	109.1	138.3	206.8	172	229.6
Eavesdropper[7]	5	3.3	3.9	20	17.1	21.2	31	25.4	32
Eavesdropper[8]	45.3	39.4	40.1	175.8	144.1	151.1	263.4	218.2	235.8
Eavesdropper[9]	207.9	171.1	163.5	618.3	502.2	485.6	991.8	812.6	725.2
Eavesdropper[10]	85.9	69.7	83.3	269.4	228.4	265.2	414.6	341.2	394.8
Eavesdropper[11]	3.5	2.5	3.1	14.2	13.8	13.3	22.2	19.6	19.6
Eavesdropper[12]	80.2	69.8	62.8	229.1	182.4	158.5	328.6	271	251.6
Eavesdropper[13]	228.9	188.5	163.8	722.6	571.3	464.6	1078.2	879.6	699.4
Eavesdropper[14]	90.8	75.3	81.2	324.7	265.3	266	525.2	431	414.4
Eavesdropper[15]	4	3.3	4	10.2	9.3	9.3	16	14.2	14
Eavesdropper[16]	66.9	55	45.2	251.7	201	170.9	467.2	375.8	274.4
Eavesdropper[17]	151.1	126.9	124	539.2	432	433.3	1009	820.4	732
Eavesdropper[18]	65.1	57	55.7	217.9	176.4	202.5	388.4	324.2	367.6
Eavesdropper[19]	1.5	1	1	11	9.2	10.5	13.8	12.2	13
Eavesdropper[20]	26.4	22	18	58.4	51.7	56.9	105.8	87.2	107.2
Eavesdropper[21]	52	46.2	42.8	155.6	131	157.3	390	321.8	287.6
Eavesdropper[22]	33.8	30.2	29.6	102.9	83.9	98.2	186.2	158.8	175.6
Eavesdropper[23]	1.5	1	1	3.1	2.5	3	5	5.4	5

We have evaluated the privacy mechanisms assuming the worst scenario, *i.e.*, an adversary has deployed 24 receivers (malicious RSUs) covering the entire road network, as shown in Figure 8.2. Each receiver has an eavesdropper functionality. Table 8.2 shows the comparison of the three evaluated privacy schemes in terms of total number of distinct pseudonyms encountered by each eavesdropper for different vehicles' densities. Note how the PPC privacy scheme almost always presents the highest values in comparison with the other schemes. This supports the conclusion that the PPC privacy scheme is more vulnerable than other schemes. In addition, the eavesdroppers 0,1,3,77,11,15,19, and 23 present poor results. This is due specifically to their location in the network as it can be seen in Figure 8.2a.

8.4 Summary

Broadcast transmissions from a vehicle operated by a private citizen should not leak information that can be used to identify that vehicle to unauthorized recipients. In this chapter, we have addressed the problem of privacy location in VANETs. First, we have considered general security requirements, and mapped those to specific VANET communications in chapter 2.4. In order to assess privacy-preserving techniques, we have included in our architecture a privacy framework based on temporary pseudonyms. Due to the changing of pseudonyms, vehicles cannot be able to link with their last pseudonym sessions, hereby location of the vehicle is hard to be determined. In particular, efficient pseudonym changing schemes for location privacy protection in VANETs were evaluated. However, the evaluated pseudonym mechanisms have some limitations. It might still be possible to fully track vehicles between pseudonym changes (see PPC privacy scheme in Figure 8.3a). Increasing the frequency of changes can help, but it also increases the incurred overhead. Hence, there is a need for new and improved privacy protecting mechanisms that provide stronger guarantees. In future work, we will use the proposed framework to develop a hybrid privacy protocol that uses the appropriate privacy scheme according to the vehicle context.

Part III
Research results and future guidelines

Chapter 9
Conclusions, publications and future work

In this thesis we have studied existing protocols for smart dissemination of emergence messages in vehicular ad-hoc networks. Also, we have developed three novel protocols for dissemination of emergence messages to improve the overall performance in both highway and urban scenarios. Moreover, we have studied existing schemes for location privacy in VANETs. In order to accurately evaluate previously proposed protocols, as well as our own proposals, we have provided a simulation framework to simulate realistic vehicular scenarios. In this chapter, we summarise the research and the findings reported in this thesis. We highlight the major contributions and conclude the chapter by suggesting possible directions for future work along the line of research.

9.1 Conclusions

Throughout this thesis, four main contributions have been made:

- A delay-based multihop broadcast protocol called Road Casting Protocol (RCP+), which is described in chapter 5 [42, 41, 43].
- Two probabilistic-based multihop broadcast protocols called Adaptive Distributed Dissemination-Forwarding Game (ADD-Forwarding Game) and Adaptive Distributed Dissemination-Volunteer's Dilemma (ADD-Volunteer's Dilemma) which are described in chapter 6 [44].
- A platform to evaluate the proposed dissemination protocols, which is described in chapter 3 [40].
- A framework to evaluate the efficiency of the privacy schemes in different scenarios, which is described in chapter 8.

The first contibution has been the implementation of RCP+ [42, 41, 43] where different waiting delays are assigned to the receivers before granting them the access to the channel to rebroadcast their messages. Each vehicle computes its delay based on their strategic location in the network and

their capacity to evaluate the congestion of the communication channel. In addition, RCP+ was evaluated with H.265/HEVC, VP9 and H.264/AVC as video codecs to disseminate an emergency video message about an incident or other traffic situation. To easily compare the outcomes of the different approaches, we have set two main metrics: Frame Delivery Ratio (FDR), and Peak Signal-to-Noise Ratio (PSNR). Simulation results have shown that our proposal can provide a good video quality in different scenarios. Furthermore, we show that our proposal reduces the frame loss and enhances the PSNR of the received video.

The second main contribution has been the proposal of two game-theoretical models to perform data dissemination [44]. In first place, the Asymmetric Volunteers Dilemma Game has been evaluated as a mechanism to quench the broadcast storm problem. This game is played whenever vehicles receive a broadcast message and they choose in a decentralized way their best strategy. The propability of broadcasting the message or not, is obtained from cross-layer information like distance and link quality. Next, the Forwarding Game has been evaluated as another mechanism to mitigate the broadcast storm problem. In this case, the forwarding probability is a factor based on traslayed metrics like distance and estimated bandwidth. Furthermore, ADD employs a mechanism Store-Carry-Forward (SCF) to mitigate the intermittently connected network problem presented on streets and roads that have low-density traffic conditions in which the number of vehicles is not enough to disseminate data messages using multi-hop communication. Both Volunteer's Dilemma and Forward Game have been evaluated in terms of packet delivery ratio (PDR), average packet delay (APD), broadcast overhead (BO), and number of collision packets (NCP). In addition, ADD was evaluated with H.265/HEVC as video codec to disseminate an emergency video message about a road accident. Simulation results show that the proposed schemes can reduce broadcast overhead and collision packets while still offering acceptable end-to-end delay for most multihop VANET applications

The third contribution has been the implementation of a simulation framework able to simulate and evaluate previously proposed protocols and our novel contributions. For this, we have studied different available tools for conducting simulations of vehicular networks (network and traffic simulation tools) in order to select the most suitable one for accurately simulating vehicular environments. Also, the simulation scenarios used throughout this research relied on real maps extracted from online maps and shadowing effects caused by buildings as well as by vehicles.

Finally, the last contribution has been the evaluation of a privacy framework for VANETs. We have addressed the problem of privacy location in VANETs. In order to assess privacy-preserving techniques, we have evaluated a privacy framework based on temporary pseudonyms. In particular, efficient pseudonym changing schemes for location privacy protection were evaluated. However, the evaluated pseudonym mechanisms have some limi-

tations. It might still be possible to fully track vehicles between pseudonym changes.

In conclusion, this thesis has contributed to the literature by providing new insights into the process of disseminating data in VANETs. The solutions presented throughout the chapters have the potential to deliver data related to a wide range of events such as accidents, traffic jams, and points of interest, thereby increasing safety, efficiency and comfort to road users. Infrastructure-less solutions may prove to be particularly useful at an early stage of deployment, since they are by design robust against intermittent connectivity.

9.2 Publications

The research work related to this thesis has resulted in nine publications; among them we have one journal article listed in the Journal Citation Report, one book chapter, three international conference papers and four articles in national conferences. We now proceed by presenting the publications list.

9.2.1 Journals

- [44] **Cristhian Iza-Paredes**, Ahmad Mohamad Mezher, Mónica Aguilar Igartua, Jordi Forné, "Game-Theoretical Design of an Adaptive Distributed Dissemination Protocol for VANETs", Sensors, ISSN: 1424-8220, Vol. 18, No. 1, January 2018, (IF 2016 = 2.677, Q1), DOI: 10.3390/s18010294.

9.2.2 Book chapter

- [43] **Iza-Paredes, C.**; Mezher, A. M.; Aguilar Igartua, M.; "Performance Comparison of H. 265/HEVC, H. 264/AVC and VP9 Encoders in Video Dissemination over VANETs", International Conference on Smart Objects and Technologies for Social Good, 2016, pp. 51-60.

9.2.3 International conferences

- [41] **Iza-Paredes, C.**; Mezher, A. M.; Aguilar Igartua, M. "Adaptive Video-streaming Dissemination in Realistic Highway Vehicular Ad-Hoc

Networks", Proceedings of the 13th ACM Symposium on Performance Evaluation of Wireless Ad-Hoc, Sensor, Ubiquitous Networks, 2016, pp. 1-10.

· [42] **Iza-Paredes, C.**; Mezher, A. M.; Aguilar Igartua, M. "Evaluating Video Dissemination in Realistic Urban Vehicular Ad-Hoc Networks", Proceedings of the 19th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems, 2016, pp. 78-82.

· [54] Mezher, A. M.; Oltra, J. J.; Aguiar, L. U.; **Iza-Paredes, C.**; Barba, C. T.; Aguilar Igartua, M. "Realistic environment for VANET simulations to detect the presence of obstacles in vehicular ad-hoc networks", Proceedings of the 11th ACM symposium on Performance evaluation of wireless ad-hoc, sensor, ubiquitous networks, 2014, pp. 77-84.

9.2.4 Spanish conferences

· [45] **Iza-Paredes, C.**; J. A. U. Ramírez; N. P. L. Marquez; L. Lemus; A. M. Mezher; and M. Aguilar Igartua. "Multimedia communications in vehicular adhoc networks for several applications in the smart cities". In XIII Jornadas de Ingeniería Telemática (JITEL2017), Spain, 2017.

· [40] **Iza-Paredes, C.**; Mezher, A. M.; Aguilar Igartua, M., "Performance evaluation of dissemination protocols for emergency messages in Vehicular Ad-Hoc networks", XII Jornadas de Ingeniería Telemática (JITEL 2015), Palma de Mallorca, Spain, 2015.

· [56] Mezher, A. M.; **Iza-Paredes, C.**; Urquiza-Aguiar, L.; Moreira, A. T. Igartua, M. A. "Design of smart services and routing protocols for VANETs in smart cities", XII Jornadas de Ingeniería Telemática (JITEL 2015), Palma de Mallorca, Spain, 2015.

· [55] Mezher, A. M.; **Iza-Paredes, C.**; Barba, C.; Aguilar Igartua, M. "A Dynamic Multimetric Weights Distribution in a Multipath Routing Protocol using Video-Streaming Services over MANETs", XII Jornadas de Ingeniería Telemática (JITEL 2015), Palma de Mallorca, Spain, 2015.

9.2.5 Stay at a foreign university

With the aim of promoting the qualitative international of this research, the author made a three-month stay with the research group of Professor

Isabelle Guérin-Lassous [6] in the DANTE Inria team at the École Normale Supérieure de Lyon from July 1th to September 30th, 2017. The result of this stay is an article titled "A reactive unicast solution for video streaming over VANETs". The article is pending for publication and it is part of the "Design of MAC protocols for VANETs networks" project funded by the ENS Lyon. For more information on this research see section 9.3.1.

9.3 Future directions for research

The research presented in this thesis focuses on the design of efficient dissemination algorithms for V2V communications. Nevertheless, there is a lot of scope for work to be done in the future in this direction. Some of those ideas are described below:

9.3.1 A reactive unicast solution for video streaming over VANETs

Video streaming in VANETs is in growing phase with several challenges that must be addressed. In this context, this future research focuses on an unicast video streaming services designed to operate over VANETs and formulates it into an optimization problem with the objective to maximize the average video quality received by users and minimizing the travel time while satisfying the constraints. A service provider could stream the video via roadside units (RSUs) infrastructure to vehicles driving through as it can be seen in Figure 9.1. We have established a highway scenario as a bidirectional road, straight and has multiple tracks. RSUs are located along the road. Below we detail the main assumptions, the input and intermediate parameters, the main objective, the restrictions, the output parameters and constraints of this project.

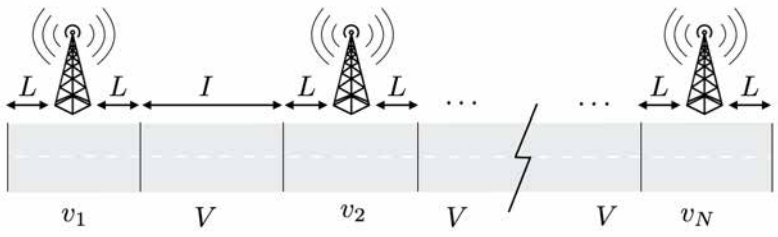


Fig. 9.1: Highway scenario.

Input parameters

- N = number of RSUs
- D = end-to-end distance $E2E$ (km)
- A = traffic intensity (vehicles/km)
- L = signal range ($\sim$ 500 m)
- B = bandwidth (Mbps)
- M = size of the video (MB)
- V = (max) velocity of a vehicle (km/h)

Assumptions

- Downlink using IEEE 802.11p
- RSUs uniformly distributed over D
- Movies are stored on each RSU
- Vehicles can always move at speed V whenever they want while it is possible

Objective

- Minimizing the E2E delay T while satisfying the constraints

Intermediate parameters

- I = inter-RSU distance (km) = $I = \frac{D}{N-1} - 2L$
- n_k = mean number of vehicles in k-th RSU = $n_k = 2 \cdot L \cdot A$
- s = time without connection (between 2 RSUs) (km) = $s = I/V(sec)$
- $r_i(v_i, n_k)$ = (estimated) amount of data downloaded in the k-th RSU given the velocity of vehicle i is v_i and the number of vehicles in the cell is n_k
- $b_i(v_i)$ = time spent by a vehicle in k-th RSU given that its speed is v_i = $b_i = \frac{2L}{v_i}$

Output parameters

- v_i = velocity of the vehicle within the k-th RSU (km/h) = $v_i \leq V$
- T = E2E delay (sec) = $\sum_{i=1}^{N-1} \frac{2L}{v_i} + (N-1).\frac{I}{V}$

Constraints

- $\frac{r_1}{B} \geq 2L/v_1 + I/V$ = enough data for the first hop
- T = E2E delay (sec) = $T = \sum_{i=1}^{N-1} \frac{2L}{v_i} + (N-1).\frac{I}{V}$
- $\frac{r_1+r_2}{B} \geq 2L/v_1 + 2L/v_2 + 2I/V$ = enough data for the first two hops
- $\frac{\sum_{i=1}^{N-1} r_i}{B} \geq 2L \sum_{i=1}^{N-1} \frac{1}{v_i} + (N-1)\frac{I}{V}$ = enough data for the whole set of hops
- $\forall j \in [1, N-1], \frac{\sum_{i=1}^{j} r_i}{B} \geq 2L \sum_{i=1}^{j} \frac{1}{v_i} + j\frac{I}{V}$ = enough data for the first j hops

Preliminary results

We have implemented the project with $N = 3$ RSUs and $A = 1$ vehicle (see Figure 9.1). The total distance traveled by the vehicle is $D = 10$ km. The RSUs are located in 2500 m, 4000 m and 5500 m. Vehicles and RSUs exchange beacon messages with information on their speed and position. The speed of vehicle is $V = 25$ m/s when it is out of transmission range. All parameters used in this preliminary evaluation are defined in Table 9.1.

Operation

When a vehicle identifies an RSU in its neighbour table, the vehicle sends a video service request. Immediately, the RSU sends the video frames and the vehicle reduces its speed. The vehicle buffers the video packets sent by the RSU. When the vehicle leaves the coverage of the RSU, it registers the last received frame. When the vehicle enters the coverage range of another RSU, it sends a new video request but only for the remaining frames. The vehicle reaches the maximum speed allowed when it is outside the coverage range of the RSU. The vehicle regulates its speed based on the amount of MB received when it is within the coverage range of the RSU.

Validation

The mathematical model that validates the preliminary results is based on the following equations:

$$\text{Total download } [MB] = \frac{2 \cdot L}{v_1} \cdot \frac{B\ [Mbps]}{8} \tag{9.1a}$$

$$\text{Time spend by vehicle in RSU } [sec] = \frac{2 \cdot L}{v_1} \tag{9.1b}$$

Each vehicle has a buffer whose statistics are presented as preliminary results of our evaluation in the Tables 9.2, 9.3 and 9.4 for different bitrate values. With these results we have successfully validated the operation of our unicast transmission platform. Finally, we will carry out extensive simulations for different vehicles' densities to obtain optimized values of v_i and T ($E2E$ delay).

N	number of RSUs	3
D	E2E distance (km)	10
A	traffic intensity (vehicles/km)	1
L	signal range ($\sim$ 500 m)	520
B	codec (Mbps)	3, 6, 9 , 18
M	size of the video (MB)	646.7872
V	(max) velocity of a vehicle (km/h)	90
$v1$	(min) velocity of a vehicle (km/h)	36

Table 9.1: Input parameters.

Preliminary Results

			Info Vehicle[0]-RSU$_0$		
Model	**BitRate [Mbps]**	**Speed [km/h]**	Time spent in RSU$_0$ [s]	Distance travelled with service (2L) [km]	**Total Downloaded [MB]**
Mathematical	3	36	101.927894912666	1.02034	38.24
Experimental	**3**	**36**	**101.927894912666**	}**1.02034**	**33.3945**
Mathematical	6	36	101.925180233214	1.02034	76.5
Experimental	**6**	**36**	**101.925180233214**	**1.02034**	**63.8844**
Mathematical	9	36	101.925103880033	1.02034	114.66
Experiment	**9**	**36**	**101.925103880033**	**1.02034**	**91.7365**
Mathematical	18	36	101.925046394437	1.02034	229.33
Experiment	**18**	36	**101.925046394437**	**1.02034**	**161.278**

Table 9.2: BitRate validation RSU$_0$

			Info Vehicle[0]-RSU$_1$		
Model	**BitRate [Mbps]**	**Speed [km/h]**	Time spent in RSU$_1$ [s]	Distance travelled with service (2L) [km]	**Total Downloaded [MB]**
Mathematical	3	36	101.924823451687	1.0205	76.46
Experimental	**3**	**36**	**101.924823451687**	**1.0205**	**67.1163**
Mathematical	6	36	101.925255983459	1.0205	152.94
Experimental	**6**	**36**	**101.925255983459**	**1.0205**	**128.464**
Mathematical	9	36	101.924923871621	1.0205	229.32
Experiment	**9**	**36**	**101.924923871621**	**1.0205**	**184.061**
Mathematical	18	36	101.922594140587	1.0205	458.65
Experiment	**18**	36	**101.922594140587**	**1.0205**	**322.961**

Table 9.3: BitRate validation RSU$_1$

			Info Vehicle[0]-RSU$_2$		
Model	**BitRate [Mbps]**	**Speed [km/h]**	Time spent in RSU$_2$ [s]	Distance travelled with service (2L) [km]	**Total Downloaded [MB]**
Mathematical	3	36	101.921978041379	1.02039	114.68
Experimental	**3**	**36**	**101.921978041379**	**1.02039**	**101.246**
Mathematical	6	36	101.920775596984	1.02039	229.38
Experimental	**6**	**36**	**101.920775596984**	**1.02039**	**193.585**
Mathematical	9	36	101.919408502175	1020.39	343.97
Experiment	**9**	**36**	**101.919408502175**	**1020.39**	**276.887**
Mathematical	18	36	101.91930511166	1020.39	687.94
Experiment	**18**	36	**101.91930511166**	**1020.39**	**485.599**

Table 9.4: BitRate validation RSU$_2$

9.3.2 Machine learning in VANETs

Machine learning (ML) is a scientific discipline in the field of artificial intelligence (AI) that is used in systems that learn automatically. Learning in this context means identifying complex patterns in tones of data [19]. The machine that learns is an algorithm that manages and checks data in order to be able to predict future behavior. ML systems improve autonomously over time without human intervention. The use of machine learning in VANETs can be useful to improve the performance of this kind of networks. Specifically, we plan to use principal component analysis (PCA), which is a technique used to emphasize variations and extract patterns from a dataset. The first step is to apply a ML technique offline. Then, use PCA online to make a self-learning to choose the best routes to transfer the information, trying to decrease the packet losses in the network. PCA will provide, after applying an offline analysis of data, the distribution of energies that each metric used in the forwarding algorithm represents. That is, we plan to apply a ML-based scheme to design the weights used to compute a multimetric score to choose the best next hop node in the forwarding algorithm. Thus, we could estimate the correct weights of each one of the considered metrics. After that, and by recalculating the correct weights instead of giving equal weights, best forwarding routes will be chosen. To improve the results, we will test different ML algorithms to find the one that performs better in VANETs.

9.3.3 Location privacy in VANETs

One of the most relevant aspects for the vehicular network is location privacy. Location privacy is the ability of a vehicle to prevent third parties from recording the current location and location changes. To achieve the location privacy in VANETs, vehicles periodically change their pseudonyms. Because a vehicle uses different pseudonyms on the road, the impossibility of linking pseudonyms can guarantee the privacy of the vehicle's location. However, if a vehicle changes its pseudonym on a wrong occasion, changing the pseudonyms would not serve to protect the location privacy since an adversary could link a new pseudonym with the old one. Thus, it might still be possible to fully track vehicles between pseudonym changes. Increasing the frequency of changes can help, but it also increases the incurred overhead. Hence, there is a need for new and improved privacy protecting mechanisms that provide stronger guarantees. In future work, we will use the proposed framework in this research to develop a hybrid privacy protocol that uses the appropriate privacy scheme according to the vehicle context.

9.3.4 VANETs and autonomous vehicles

Autonomous vehicles (AVs) are a promising driverless type of vehicle that can be part of the VANETs in the near future. AV need to communicate with other cars (V2V) and with the infrastructure around (V2I), in order to move in the roads interacting with the environment without problems, copying the driver's behaviour, adapting the driving according to the circumstances such as speed limit, pedestrian crossing the street or water in the road. Both kind of communications are necessary to detect pedestrians or obstacles (localization), movements of other cars (planning) to take a decision of what to do. One major challenge most cities share is to find efficient ways to manage mobility. According to a study by Texas $A\&M$ Transportation Institute in 2015 the time US commuters are stuck in traffic has risen by 133% since 1982 which equals a total of 42 hours. This means that on average drivers spend almost two full days in their vehicles per year. On average drivers loose an extra of 72 litres of fuel per year during traffic jams. In total, fuel emissions have gone up by 520% since the 1980s, which is a huge strain on the environment. On the other hand, as more and more people move to city outskirts, traffic congestion during rush hours is likely to become cities primer challenge. While most commuters drive into the city centre by car to get to work, most cities try to manage this problem by introducing traffic management systems and restrictive policies to regulate cars accessing the centre. As traffic density increases, managing traffic and congestion will become more complex. In this context, AV and VANETs could alleviate drastically many issues related to mobility in cities, improving driving safety, decreasing pollution and reducing traffic congestion.

9.3.5 VANETs, electric vehicle and smart grid

The growing need of countries to reduce energy consumption and the increasing concern for environmental problems have encouraged the adoption of electric vehicles as an alternative transportation option to conventional internal combustion vehicles. Recently, the development of the concept of smart grid in the electric network has advanced in the field of electric vehicles in the form of technological advances that allow communication between the vehicle and the electricity grid. Vehicle-to-grid (V2G) technology allows the exchange of bi-directional energy between electric vehicle and electric network, generating the possibility of developing numerous new services to improve the electric network, such as maximum load, regulation and rotation of electric power reserve, load leveling and reactive power consumption. The electrification of the hybrid electric vehicle reduces dependence on the transport of fossil fuels and reduces greenhouse gas emissions. The economic and environmental benefits of hybrid electric vehicles are greatly reshaping

the modern transport sector. The electrification of transport presents several challenges for the smart grid (SG), such as the quality of the energy, the reliability of the service and the control thereof. In addition, the intermittent nature of renewable energy resources (RERs) requires distributed, efficient, reliable, flexible and dynamic energy storage technologies. The storage battery of the electric vehicles (EVs) is a promising solution to settle the electrical generation based on the RERs within the SG. One of the most efficient feature of the transport sector is the concept of V2G that helps to store surplus energy and to return this energy to the main network during periods of high demands.