FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Successive Interference Cancellation in Vehicular Networks to Relieve the Negative Impact of the Hidden Node Problem

Carlos Miguel Silva Couto Pereira

Dissertation conducted under the
Master in Electrical and Computers Engineering
Major Telecommunications

Supervisor: Ana Aguiar (Ph.D.)

Co-Supervisor: Jens Mittag (Dipl.-Inform.)

September, 2011

U.PORTO

FEUP FACULDADE DE ENGENHARIA UNIVERSIDADE DO PORTO

MIEEC - MESTRADO INTEGRADO EM ENGENHARIA ELECTROTÉCNICA E DE COMPUTADORES **2010/2011**

A Dissertação intitulada

"Successive Interference Cancellation in Vehicular Networks to Relieve the Negative Impact of the Hidden Node Problem"

foi aprovada em provas realizadas em 29-09-2011

o júri

José António Ruela Simões Fernandes

Presidente Professor Doutor José António Ruela Fernandes
Professor Associado do Departamento de Engenharia Electrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

Professor Doutor Adriano Jorge Cardoso Moreira
Professor Associado do Departamento de Sistemas de Informação da Universidade do Minho

Professora Doutora Ana Cristina Costa Aguiar
Professora Auxiliar Convidada do Departamento de Engenharia Eletrotécnica e de Computadores da Faculdade de Engenharia da Universidade do Porto

O autor declara que a presente dissertação (ou relatório de projeto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extratos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são corretamente citados.

Carlos Miguel Silva Couto Pereira

Autor - Carlos Miguel Silva Couto Pereira

Abstract

In Vehicular Ad-hoc Networks (VANETs), communications are made between vehicles (V2V) and between vehicles and roadside infrastructures (V2I). VANETs are a promising approach to increase the safety on roads. However, fast fading characteristics of the received signal due to the high mobility of the vehicles and the hidden node problem can lead to unsynchronized packet transmissions, which in turn may result in packet collisions and therefore packet losses. Furthermore, safety messages are based on one-hop broadcast, where there are no mechanisms implemented for feedback or for reducing collisions due to the hidden node problem, such as Request to Send/Clear to Send (RTS/CTS).

It is known that it is possible to, under specific conditions, successfully decode and receive even colliding packets. The technique used to achieve this is called Successive Interference Cancellation (SIC).

Recently, *PhySim-WiFi* integrated a physical layer implementation of the Orthogonal Frequency Division Multiplexing (OFDM) PHY specification for the 5 GHz band into the NS-3 network simulator which permits the study of signal processing techniques, such as SIC, in VANETs.

In this context, we use NS-3 with *PhySim-WiFi* to characterize packet collisions in VANETs. Then, we proceed with the analysis of the advantages and disadvantages of implementing SIC in receivers.

The feasibility of the receivers is directly related with the user offered load to the channel and can become infeasible for extreme channel congestion situations due to the high number of packet collisions that occur in the system. However, when the user offered load to the channel is low there are few packet collisions and, therefore, SIC doesn't introduce throughput gains.

According to our assessment, the probability of packet reception can be increased by 5 to 20 % for packets sent in the entire communication range of the receiver, for scenarios where the user offered load to the channel is approximately 3.3 Mbps, and achieves the maximum of 40 % of packet recovery, for scenarios with approximately 1.1 Mbps.

Resumo

Em redes veiculares ad-hoc (VANETs), as comunicações são feitas entre veículos (V2V) e de veículos para infra-estruturas situadas na berma da estrada (V2I). VANETs são uma abordagem promissora para aumentar a segurança nas estradas. No entanto, as características de *fading* rápido do sinal recebido, devido à grande mobilidade dos nós, e o problema do nó escondido (*hidden node problem*) podem levar a transmissões dessincronizadas de pacotes, que podem resultar em colisões de pacotes e, portanto, perdas de pacotes. Além disso, mensagens destinadas à segurança são baseadas em *one-hop broadcast*, onde não há mecanismos implementados para *feedback* ou para reduzir colisões devido ao problema do nó escondido, tal como o *Request to Send/Clear to Send* (RTS/CTS).

É conhecido que é possível, mediante condições específicas, descodificar e receber com sucesso pacotes que colidam. A técnica que é usada para isto chama-se Successive Interference Cancellation (SIC).

Recentemente, *PhySim-WiFi* integrou uma implementação da camada física da especificação de Orthogonal Frequency Division Multiplexing (OFDM) PHY para a banda de 5GHz no simulador de rede NS-3 que permite o estudo de técnicas de processamento de sinal, como SIC, em VANETs.

Neste contexto, usamos o NS-3 com *PhySim-WiFi* para fazermos uma caracterização detalhada das colisões de pacotes em VANETs. De seguida, procedemos à análise das vantagens e desvantagens de implementar SIC nos receptores.

A viabilidade dos receptores está directamente relacionada com a carga do utilizador oferecida ao canal e pode tornar-se intolerável em situações de congestionamento extremo de canal por causa do elevado número de colisões que ocorrem no sistema. No entanto, quando a carga do utilizador oferecida ao canal é baixa, existem poucas colisões de pacotes e, por isso, SIC não traz ganhos de throughput.

De acordo com a nossa avaliação, a probabilidade de recepção de pacotes pode ser melhorada entre 5 a 20 % para pacotes enviados dentro da distância de comunicação do receptor, para cenários em que a carga do utilizador oferecida ao canal é aproximadamente 3.3 Mbps, e atinge o máximo de 40 % de recuperação de pacotes, para cenários em que a carga com aproximadamente 1.1 Mbps.

Acknowledgments

I would like to thank Jens Mittag for accepting me in his group to develop this work and for all the help he gave me during these last months concerning the work and my stay in Karlsruhe. I also want to express my gratitude to Professor Ana Aguiar, who supported and helped me so that I could fulfill this work.

To my friends for all the laughts we share.

To my close family for their unconditional support.

To Raquel for being the most important person in my life.

Carlos Pereira

“I do not fear computers. I fear the lack of them.”

Isaac Asimov

Contents

List of Figures

List of Tables

Abbreviations and Acronyms

AC	Access Category
ACK	Acknowledgment
AIFS	Arbitration Interframe Space
ASTM	American Society for Testing and Materials
CBR	Constant Bit Rate
CCA	Clear Channel Assessment
CCH	Control Channel
CDMA	Code Division Multiple Access
CR	Communication Range
CS	Carrier Sense
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSR	Carrier Sensing Range
CTS	Clear to Send
CW	Contention Window
dB	decibel
dBm	dB referenced to 1 milliwatt
DCF	Distributed Coordination Function
DFT	Discrete Fourier Transform
DIFS	DCF Interframe Space
DSSS	Direct Sequence Spread Spectrum
DSRC	Dedicated Short-Range Communications
EDCA	Enhanced Distributed Channel Access
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
GI	Guard Interval
GHz	Gigahertz
GPL	General Public License
ICI	Inter-Carrier Interference
IEEE	Institute of Electrical and Electronics Engineers
IFFT	Inverse Fast Fourier Transform
IFS	Interframe Space
ISI	Inter-Symbol Interference
ITS	Intelligent Transport Systems
KHz	Kilohertz
MAC	Medium Access Control Layer
MANET	Mobile Ad-Hoc NETwork
Mbps	Megabit per second
MHz	Megahertz

MCM	Multicarrier Modulation
MSDU	MAC Service Data Unit
MUD	Multiuser Detection
OFDM	Orthogonal Frequency Division Multiplexing
PCF	Point Coordination Function
PIFS	PCF Interframe Space
PHY	Physical Layer
QPSK	Quadrature Phase-Shift Keying
QoS	Quality of Service
RTS	Request to Send
SCH	Service Channel
SIFS	Short Interframe Space
SIC	Successive Interference Cancellation
SINR	Signal to Interference-plus-Noise Ratio
TC	Traffic Category
TRG	Two-Ray Ground
VANET	Vehicular Ad-hoc NETwork
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
WAVE	Wireless Access for Vehicular Environments
WLAN	Wireless Local Area Network

Chapter 1

Introduction

This chapter aims to provide an overview of the work. First, a short motivation is presented, followed by the objectives and the main contributions of this thesis. Finally, the thesis' structure is outlined.

1.1 Motivation

Mobility and flexibility are making wireless technologies prevail over other methods of data transfer. Communications between vehicles (V2V) and between vehicles and roadside infrastructures (V2I) form Vehicular Ad-hoc Networks (VANETs) in which nodes[1] can communicate wirelessly in a self-organizing way without the need of a central access point. In VANETs, there are two types of applications envisioned: safety and non-safety. Although non-safety applications can be important to provide infotainment to drivers allowing new business areas, safety applications will permit road traffic to be safer, assisting drivers on the detection of dangerous traffic situations in advance by cooperative awareness, which ultimately can reduce fatalities. In the United States of America, according to preliminary data for 2008 [1], motor vehicle accidents are the first cause of death in the age group 1 - 44 years, and it is expected that VANETs will play an important role in reducing these numbers.

VANETs face common challenges of ad hoc networks, e.g., reliability, scalability and stability, but in VANETs, considering the peculiar characteristics of the communications, these problems gain a different insight. VANETs settle in the recently published Orthogonal Frequency-Division Multiplexing (OFDM)-based IEEE 802.11p, which is based on modifications and amendments to IEEE 802.11a for adapting it to vehicular environments. For safety applications, the IEEE 802.11-Based One-Hop Broadcast mode is used without any type of feedback mechanisms, like acknowledgment messages, since it could create broadcast storms. Congestion avoidance mechanisms, as Request to Send/Clear to Send (RTS/CTS), are also not implemented because it would

[1] devices inside vehicles or roadside infrastructures

introduce considerable overhead in the channel and also the exposed node problem. IEEE 802.11p uses the Distributed Coordination Function (DCF) to coordinate the access to the medium to detect multiple accesses in order to avoid collisions. DCF employs Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with binary exponential contention algorithm in which users sense the channel and delay transmission if they detect that another user is currently transmitting. The hidden node problem can lead to unsynchronized packet transmissions by nodes that are outside of each other's sensing range, which in turn may result in packet collisions (i.e., overlap in time of two or more packets at the receiver) and losses at possible receivers in between. Additionally, fast fading characteristics of the received signal due to the high mobility of nodes introduce unsynchronized transmissions caused by nodes that are supposedly inside the sensing range of a transmission but cannot detect it and interfere.

It is known that it is possible, under specific conditions, to successfully decode and receive even overlapping packets, almost achieving Shannon's channel capacity theorem [2]. The technique that is used to achieve this is called Successive Interference Cancellation (SIC). SIC is a physical layer technique that allows a receiver to decode successively packets that arrive simultaneously. Consider that two packets arrive concurrently at the receiver. Usually, even using latest device capabilities, such as capture effect, only the strongest signal at the receiver can be decoded, treating the other signal as interference. SIC permits the recovery of the weaker signal by subtracting the stronger signal from the combined signal and extracting the weaker signal from the residue. SIC has already been applied to ZigBee [3] and to Direct Sequence Spread Spectrum (DSSS) based IEEE 802.11 PHY specification in [4], to recover packets from collisions and is frequently used in Code Division Multiple Access (CDMA) systems, to perform multi-user detection [5]. VANETs communications can easily suffer from time- and frequency-selective fading channels, which add different complexity and feasibility to the receivers. Furthermore, IEEE 802.11p uses an OFDM PHY in which only 4 pilot-subcarriers are used for channel estimation, thus it is not straightforward that we can also apply SIC in VANETs.

Due to high costs of VANETs deployment, it is necessary to use simulators to perform evaluations. NS-3 is a well-known and widely used network simulator; however, it significantly abstracts the physical layer details and the channel models [6]. Torrent-Moreno et al. [7] included capture effect and channel models extensions in the predecessor of NS-3, NS-2, to assess the performance of IEEE 802.11-Based One-Hop Broadcast in coordinating the medium access to avoid packet collisions. The work evaluated the benefits and losses on using, respectively, capture effect and probabilistic channel models. Furthermore, it also characterized in detail the hidden node problem and performed a scalability analysis based on the user offered load to the channel.

Recently, *PhySim-WiFi* integrated a physical layer implementation of the OFDM PHY specification for the 5 GHz band into NS-3 [8]. This module gives the opportunity to study signal processing techniques, such as SIC, and to perform a more accurate characterization of packet drops and packet collisions in VANETs environments. Only with a detailed analysis of packet collisions it is possible to identify correctly the possible throughput gains of implementing interference cancellation in the receivers and to determine if it is a mechanism feasible to be employed in VANETs devices.

1.2 Objectives

The main objective of this thesis was to understand the advantages and disadvantages of implementing interference cancellation in VANETs. For that, it is necessary to 1) characterize packet drops; 2) characterize packet collisions with respect to the geographical position of the receiver, sender and interferer(s); 3) assess the number of packets that will be possible to recover from collisions using interference cancellation; 4) perform evaluation of the trade-offs (i.e., benefits vs. feasibility) of implementing SIC in transceivers.

1.3 Contributions

This thesis makes contributions in VANETs with the following aspects:

- A detailed characterization of packet drops: Using *PhySim-WiFi* for NS-3, we analyze packet drops by presenting a description of the causes and in which part of the frame reception they happen. With this approach we have a first insight of the impact of collisions in the performance of the system.

- A detailed characterization of packet collisions: We analyze in detail packet collisions. First, we identify the Probability that packet can be involved in a collision. Then, we present the Energy distribution of colliding packets. And finally, we show the Number of packets overlapping. This way it is possible to understand how collisions vary in the system when there is a variation of the nodes' transmission parameters and nodes' density.

- An analysis of benefits and feasibility of SIC: We identify the throughput gains in packet reception introduced by SIC, and at the same time, we analyze the complexity needed to perform it.

1.4 Structure

This document is organized according to the following structure: The current chapter is an introduction to the thesis; Chapter 2 presents a review of the State of the Art and related work, as well as an overview of NS-3; Chapter 3 describes the methodology of the characterization of packet collisions; in Chapter 4, we present the results and the evaluation; Chapter 5 contains a brief review of the contributions, the conclusions and future work.

Chapter 2

State of the Art

2.1 Vehicular Ad-Hoc Networks

In October 1999, the Federal Communications Commission (FCC) allocated the frequency spectrum at 5.9 GHz exclusively for V2V and V2I communications in the USA. Later, in 2003, the Dedicated Short-Range Communications (DSRC) emerged. DSRC is a communication service that operates in the 75 MHz licensed spectrum at 5.9 GHz. In Europe, in August 2008, the European Telecommunications Standards Institute (ETSI) allocated 30 MHz of spectrum in the 5.9 GHz band from 5875 MHz to 5905 MHz with a possible extension of 40 MHz [9]. The DSRC spectrum is presented in Figure 2.1.

The spectrum for North America is divided into 10 MHz bandwidth channels with a total of 7 different channels and a 5 MHz safety margin at the lower end of the assigned spectrum, as shown in Figure 2.2. Channel 178 is the control channel (CCH), which is used for broadcasting transmissions and establishing communications. Channels 172 and 184 are reserved for special users. The remaining channels are service channels (SCH) and are used for service applications and to manage two-way communication in V2V and in V2I [11], but if a vehicle does not "listen" anything within 100 milliseconds, it switches back to control channel. Note also that there is the possibility of two adjacent service channels may be used as a single 20 MHz channel [12].

The allocated frequency allows vehicles and roadside infrastructures to form VANETs.
VANETs are one subclass of Mobile Ad-Hoc NETworks (MANETs), in which nodes can communicate wirelessly without the need of a central access point. VANETs are distinguished from MANETs by the self-organization of the nodes, real-time communications, unreliable channel conditions and hybrid network architectures, which integrate ad hoc networks, wireless Local Area Networks (WLANs) and cellular technologies. In VANETs, the devices in vehicles are named On Board Units (OBUs) and roadside infrastructures are named Road Side Units (RSUs). VANET is one of the influencing areas for the improvement of Intelligent Transportation System (ITS). Beaconing is the process of periodically, and locally, broadcast status information, e.g.,

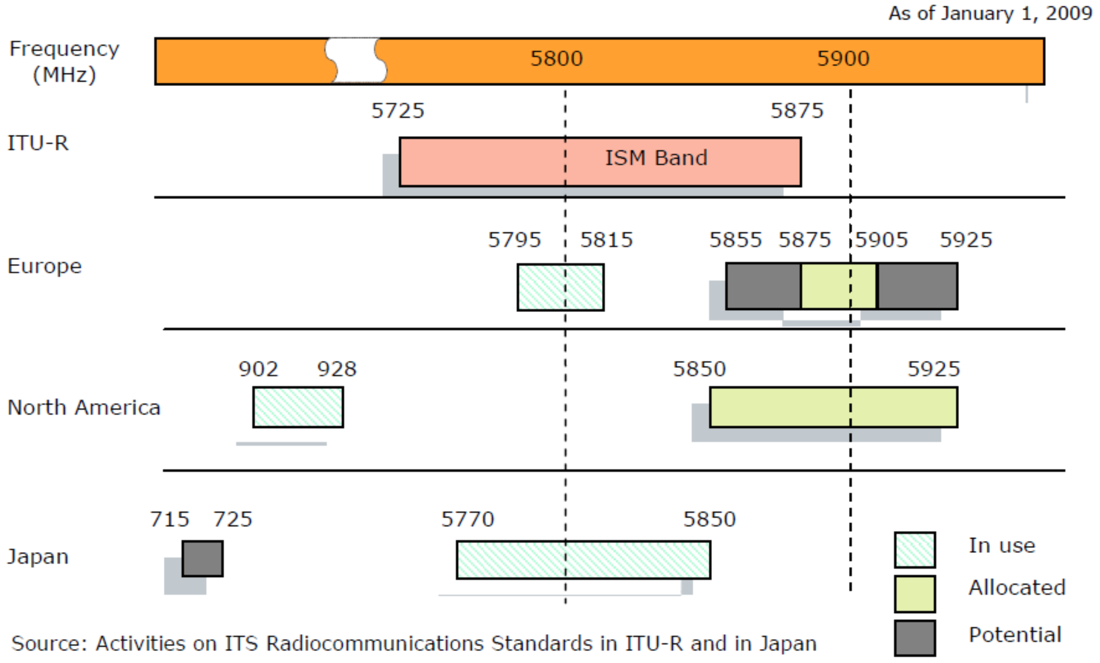


Figure 2.1: Spectrum allocation for DSRC. Extracted from [10].

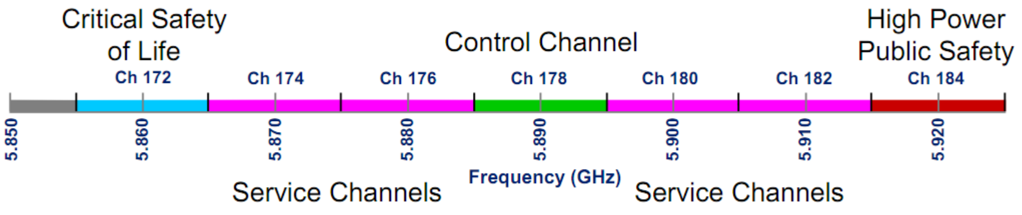


Figure 2.2: 802.11p Operating Channels. Extracted from [13].

their geographical position, speed, or direction and therefore permitting to detect dangerous traffic situations in advance. Motivations of VANET technology are not limited to safety. Enhancement of the traveller mobility, increase on the efficiency of the transport system, decrease of the travelling time and boost on-board luxury are amongst the vast reasons for why VANETs are receiving the well-deserved attention [14].

Recently, the IEEE 802.11 Working Group published the IEEE 802.11p Wireless Access in Vehicular Environment (WAVE) standard to adapt former IEEE 802.11 - 2007 to vehicular networks and to add support for Intelligent Transportation Systems (ITS) [15]. IEEE 802.11p is an evolution from American Society for Testing and Materials (ASTM) E2213-03: Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications [16]. The PHY and MAC layers are based in the

IEEE 802.11a - 1999 and IEEE 802.11e - 2005 standards, respectively. In a broader context, as shown in Figure 2.3, IEEE 802.11p WAVE is a part of several standards, which will jointly enable wide scale telematics.

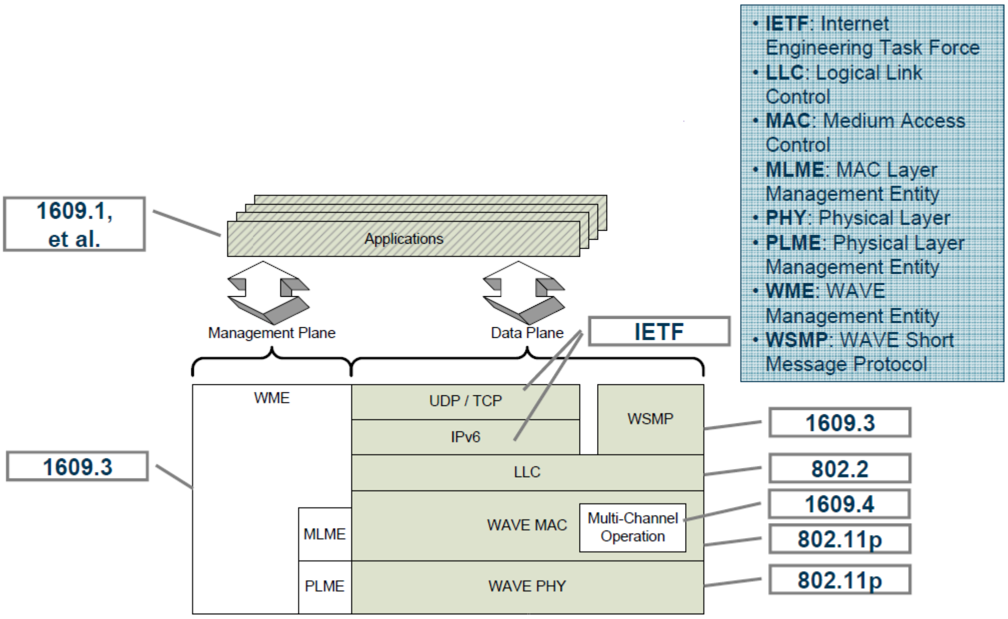

• IETF: Internet Engineering Task Force
• LLC: Logical Link Control
• MAC: Medium Access Control
• MLME: MAC Layer Management Entity
• PHY: Physical Layer
• PLME: Physical Layer Management Entity
• WME: WAVE Management Entity
• WSMP: WAVE Short Message Protocol
1609.1, et al.
Applications
Management Plane
Data Plane
IETF
WME
UDP / TCP
IPv6
WSMP
LLC
MLME
WAVE MAC
Multi-Channel Operation
PLME
WAVE PHY
1609.3
1609.3
802.2
1609.4
802.11p
802.11p

Figure 2.3: IEEE 802.11p WAVE Protocol Stack. Extracted from [17].

IEEE 802.11p WAVE provides V2V and V2I communications. It proposes small modifications to the data link and physical layers of the OSI model to provide a more reliable connection and quick setup for high-speed vehicles.

2.2 Technology

2.2.1 IEEE 802.11.p

Modifications and amendments on IEEE 802.11 were made for adapting it to vehicular environments, resulting in IEEE 802.11p.

2.2.1.1 Phy Layer

Briefly, Orthogonal Frequency Division Multiplexing (OFDM) is a special case of multicarrier modulation (MCM) which uses orthogonal carriers. OFDM has many advantages over conventional modulation schemes [18]. OFDM systems adapts to time- and frequency-domain channel quality variations of the transmission channel [19]. OFDM is protected against frequency-selected fading since divides the wideband signal into many narrowband subcarriers.

An IEEE 802.11 frame for OFDM-based communication is composed of a preamble, a signal header and the data unit section with the payload. Figure 2.4 shows an example of an IEEE

802.11p frame. Except for the amendment of parameters to allow high user mobility and longer ranges of communications (up to 1000 meters), the physical layer properties of 802.11p are similar to the already widely used on the 802.11a standard, which uses OFDM modulation. In both standards it is employed a 64-subcarrier OFDM but only 52 are used for transmissions. Out of these 52 subcarriers, 48 are for transmitting data and the remaining 4 are called pilot-subcarriers. The pilot-subcarriers are used for channel estimation, tracking frequency and phase offset. Short and long training symbols are located at the beginning of each data packet and used for signal detection, coarse frequency offset estimation, time synchronization, and channel estimation.

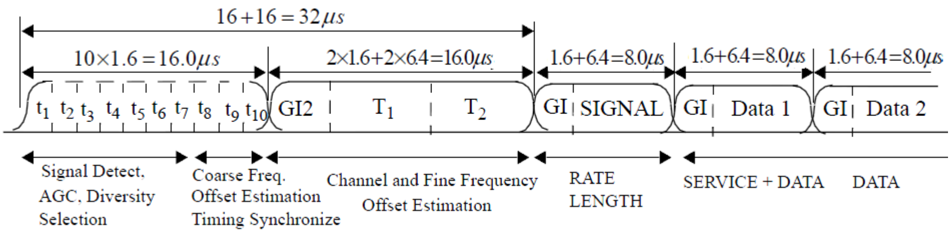

16+16=32μs
10×1.6=16.0μs
2×1.6+2×6.4=16.0μs
1.6+6.4=8.0μs
1.6+6.4=8.0μs
1.6+6.4=8.0μs
t1 t2 t3 t4 t5 t6 t7 t8 t9 t10
GI2
T1
T2
GI SIGNAL
GI Data 1
GI Data 2
Signal Detect, AGC, Diversity Selection
Coarse Freq. Offset Estimation Timing Synchronize
Channel and Fine Frequency Offset Estimation
RATE LENGTH
SERVICE + DATA
DATA

Figure 2.4: IEEE 802.11p frame with OFDM preamble and PLCP header (using a 10 MHz channel). Based on [20].

Fading channel is combated with the coding and interleaving of information bits before they are modulated on subcarriers [12]. There are guard intervals (GIs) to relieve Inter-Symbol Interference (ISI) introduced by multipath propagation effects.

Propagation conditions in vehicular communications are different to the ones projected for 802.11, based on nomadic indoor usage [21]. Table 2.1 exhibits the comparison of the main PHY parameters between IEEE 802.11a and IEEE 802.11p.

IEEE 802.11p decreases the available frequency bandwidth of each channel to 10 MHz, which doubles all parameters in time domain when compared to IEEE 802.11a while the data rate is halved (3 to 27 Mbps). ISI is reduced due to the doubled guard interval. Inter-carrier interferences (ICI) are mitigated as well because the Doppler spread is much smaller than half the subcarrier separation distance of 156.25 KHz. It was reported in [22] that lower data rates promote a robust message exchange by offering better opportunities for countering noise and interferences. Meanwhile, the transmission power in 802.11p can be higher than in 802.11a in order to support larger communication range in VANETs.

A quick overview of OFDM operating mode is presented next (based on [23]). Figure 2.5 shows a block diagram of the transmitter for the OFDM PHY. For the rate of 6 Mbps, the default rate for VANETs, the input data is modulated by a Quadrature Phase-Shift Keying (QPSK) modulator. Then, the symbols are converted from serial-to-parallel resulting in parallel QPSK symbols, which correspond to the symbols transmitted over each of the subcarriers (discrete components). These discrete frequency components are converted into time by performing an inverse Discrete Fourier Transform (DFT), which is efficiently implemented using the Inverse Fast Fourier Transform (IFFT) algorithm. After the addition of the cyclic prefix, time samples are ordered to serial

Parameters	IEEE 802.11a	IEEE 802.11p
Bit Rate (Mbps)	6, 9, 12, 18, 24, 26, 48, 54	3, 4, 5, 6, 9, 12, 18, 24, 27
Bandwidth (MHz)	20	10
Modulation Mode	BPSK, QPSK, 16-QAM, 64-QAM	BPSK, QPSK, 16-QAM, 64-QAM
Coding Rate	$\frac{1}{2}, \frac{2}{3}, \frac{3}{4}$	$\frac{1}{2}, \frac{2}{3}, \frac{3}{4}$
Number of Subcarriers	52	52
IFFT/FFT Period (μs)	3.2	6.4
Guard Interval (μs)	0.8	1.6
OFDM Symbol Duration (μs)	4	8
Preamble Duration (μs)	16	32
Subcarrier Spacing (MHz)	0.3125	0.15625

Table 2.1: Comparison of the main PHY parameters between IEEE 802.11a and IEEE 802.11p.

and passed to analogic (D/A converter) resulting in the baseband OFDM signal, which is then up converted to a frequency f0.

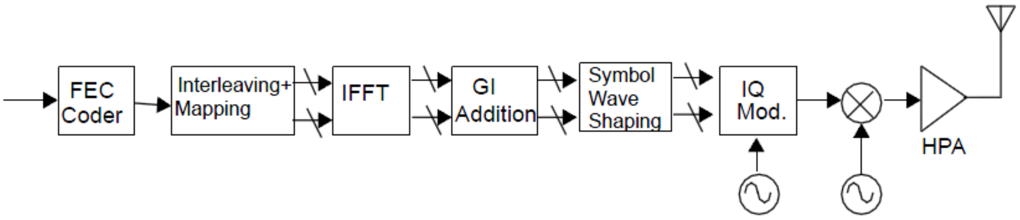


Figure 2.5: Block diagram of the transmitter for the OFDM PHY. Extracted from [24].

On the receiver side the reverse process is executed (Figure 2.6).

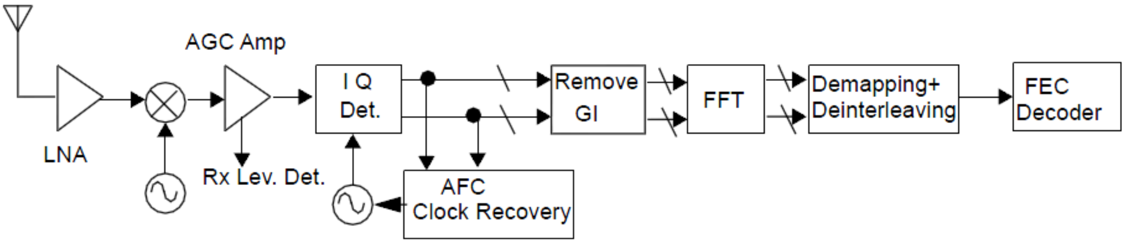


Figure 2.6: Block diagram of the receiver for the OFDM PHY. Extracted from [24].

The demodulator uses the pilot and the training symbols to estimate the channel. An important step at the receiver is synchronization. Correct synchronization occurs by organizing the data into reliable synchronized frames. A synchronization symbol is present in the beginning of all frames to indicate the starting position of the frame. Wireless communications usually have noisy communication links, so it is normal that received data is not always correct or is affected by collisions, thus, there is no certainty that the receiver is able to recognize the synchronization symbol.

2.2.1.2 MAC Layer

The MAC frame format of IEEE 802.11 is constituted by a set of fields with a fixed order in all frames. Only the first three and last fields must be present in all frames and compose the minimal possible frame. The remainders are only present in certain frames types and subtypes. The frame body has a maximum size of the MAC Service Data Unit (MSDU) size (2304 octets) plus any overhead from security encapsulation [20]. Figure 2.7 presents a general MAC frame.

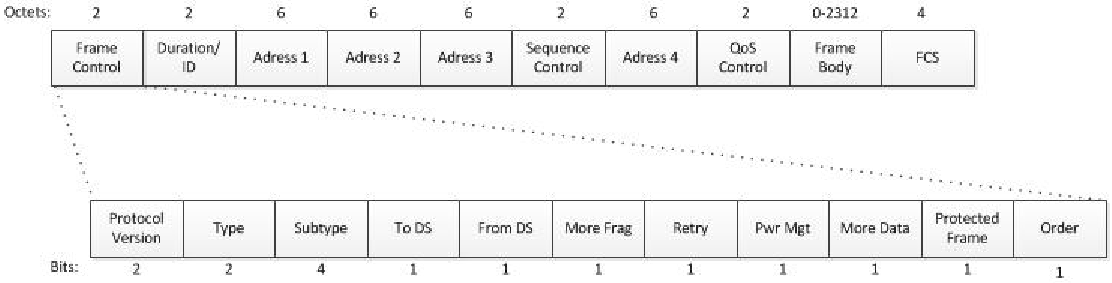


Figure 2.7: General MAC frame format with explicit frame Control field. Based on [20].

IEEE 802.11 MAC supports two modes of operation: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). While DCF is implemented in all stations and is used to coordinate the medium access in the ad hoc mode, PCF is optional and is used only in the infrastructure mode. VANETs require operation in the ad hoc mode, therefore, IEEE 802.11p is based in the DCF mechanism.

DCF uses carrier sense multiple access with collision avoidance (CSMA/CA). Figure 2.8 illustrates DCF operation.

Taking as example Figure 2.8, DCF can be described as the following. Before starting a transmission, Station 1 performed a physical carrier sensing, i.e., Station 1 sensed the medium for any ongoing transmission. Since the medium was sensed idle, it activated a contention timer called DCF Interframe Space (DIFS), after which the medium continued idle and the station was able to transmit. Representation of Interframe Space in IEEE 802.11 is presented in Figure 2.9. Stations 2, 3 and 4 also wanted to start a transmission, but sensed there was already a transmission ongoing in the medium, so they have to wait until the medium became again idle plus a time with the duration of DIFS, and since the the medium continued to be idle they activated a random contention timer. This randow contention timer ensures low probability of collision and fair access opportunities

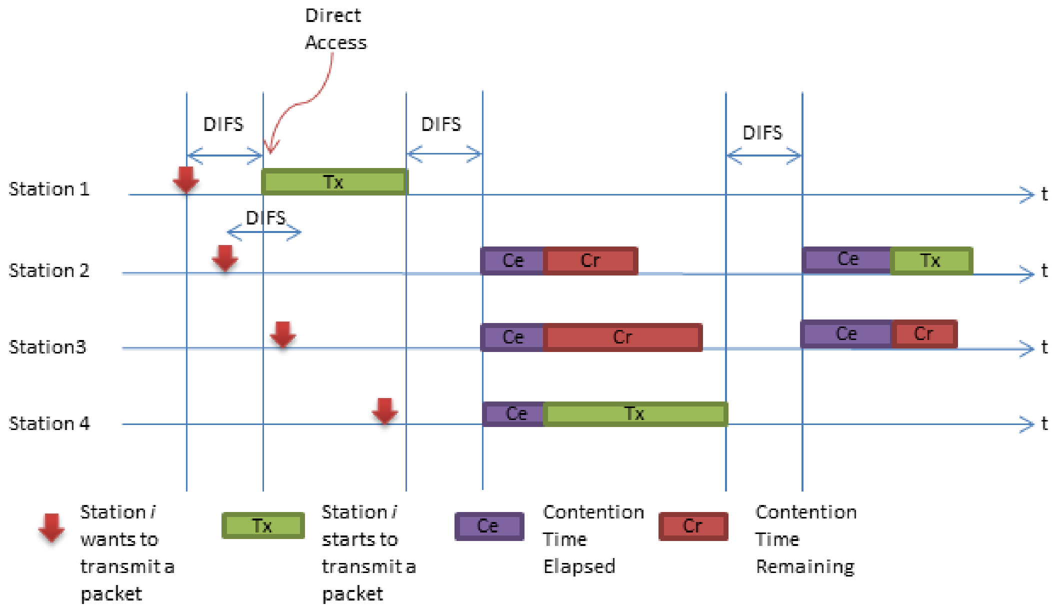


Figure 2.8: Example of IEEE 802.11 DCF operation.

for all stations and is chosen randomly from a uniform distribution [0, CW], where CW is the contention window size and its units are slot times. The contention timer is decremented only if the medium is detected to be idle. The station has permission to start the transmission after the timer reaches 0 and the channel is still idle at that moment. Continuing with the example, Station 4 selected the smallest contention timer, thus, it started to transmit before Stations 2 and 3. The contention timer of these stations was freezed when Station 4 started to transmit, but continued to decrease after the medium became idle plus a time with the duration of DIFS. Since Station 2 had the smallest remaining contention timer, it transmitted first than Station 3.

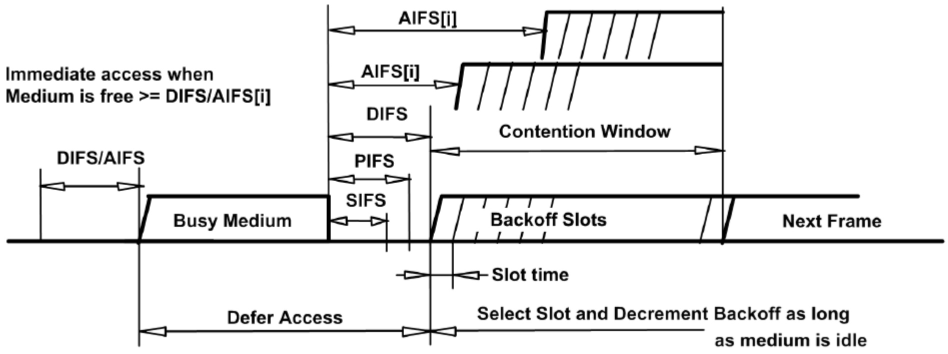


Figure 2.9: Interframe Space in IEEE 802.11. Extracted from [20].

The contention procedure is imposed by a binary exponential contention algorithm, where each unsuccessful attempt to transmit the same packet is preceded by contention within a window that is double the size used previously; however, contention windows do not get their values doubled in IEEE 802.11 broadcast mode. During this contention time if another transmission starts before the contention timer expires, this one is inhibited until that transmission ends and when the transmission ends the timer is reactivated.

DCF is not a perfect mechanism. The well-known hidden node problem[1] can lead to unsynchronized packet transmissions by nodes that are outside of each other's sensing range, which in turn may result in packet collisions at possible receivers in between. Additional packet collisions can be caused by two stations that select the same contention slot timer to transmit. IEEE 802.11 DCF is a best-effort mechanism since it does not support Quality of Service (QoS); therefore, all stations compete with the same priority and there is no mechanim to differentiate applications with priority or with time requirements.

For safety applications, IEEE 802.11p uses the IEEE 802.11-Based One-Hop Broadcast mode which means it uses DCF without any type of feedback mechanisms, like acknowledgment messages, and without congestion avoidance mechanisms, as Request to Send / Clear to Send (RTS / CTS).

Enhanced Distributed Channel Access (EDCA) is an enhanced version of IEEE 802.11 DCF used in the IEEE 802.11e, to coordinate channel access and, at the same time, guarantee QoS requirements. EDCA is also based on CSMA/CA. The essential of EDCA operation mode is that, when the channel is busy, the contention mechanism differs. IEEE 802.11e prioritizes messages by providing different Traffic Categories (TCs) that are also called Access Categories (ACs). In EDCA, when the medium is determined busy before the counter reaches zero, the station has to wait for the medium to become idle plus an Arbitration Inter Frame Spacing (AIFS) before continuing to count down the contention timer. This timer is reduced by one beginning the last slot interval of the AIFS period (in legacy DCF, the contention counter is reduced by one beginning the first slot interval after the DIFS period). Also, in 802.11 DCF the content timer always doubles after any unsuccessful transmission while in IEEE 802.11e after an unsuccessful transmission attempt a new content window is calculated with the help of the persistence factor (PF) (related to a specific TC) and another uniformly distributed contention counter is taken out of this new CW, in order to reduce the probability of a new collision [25].

IEEE 802.11p has envisioned real-time communications, therefore, for non-broadcast traffic, IEEE 802.11p MAC layer is based on IEEE 802.11e EDCA QoS extension [26] where different applications categories have different Arbitration Inter Frame Space (AIFS) and CW values. Although based on IEEE 802.11e EDCA extension, IEEE 802.11p uses specific parameters for its EDCA extension. In table 2.2 is displayed the parameter settings for different application traffic types [27]. The higher the access category is, the higher the priority for transmission of that frame is. For each AC exists a packet queue. The four ACs contest internally for the selection of a packet to transmit. Whichever packet selected must also compete for the channel externally with its own contention parameters.

[1] See Section 2.3.3.1 for more details in the hidden node problem.

AC	CWmin	CWmax	AIFSN
3	3	7	2
2	3	7	3
1	7	225	6
0	15	1023	9

Table 2.2: Default parameter settings for different application categories in 802.11p.

2.3 Challenges of VANETs

2.3.1 Mobility

The channel condition of VANETs is highly dynamic due to the high mobility of vehicles and the frequently changing road conditions. Fast fading characteristics of the received signal due to the high mobility of the sending or receiving vehicles introduces unsynchronized transmissions, since even nodes located in the close surrounding might not detect an ongoing transmission and interfere when they actually should not. Doppler Shift is introduced by high relative velocities of the interacting objects. The variation of the channel characteristics over the duration of a given block of data is caused by multiple wavefront effects, each with potentially different frequency shift. In OFDM, the Doppler Shift destroys the orthogonality between subcarriers. The loss of orthogonality will introduce Inter-Carrier Interferences (ICI) and significantly degrade the performance. This degradation gains a substantial importance as the carrier frequency and vehicle velocity increase [28]. An increase of the Delay Spread, the deviation of times of the received signal components, is also a consequence of the high mobility of the nodes in VANETs.

2.3.2 Scalability

Although conventional medium access in ad-hoc mode may be sufficient in scenarios with low user offered load scenarios, in high user offered load scenarios, an increased loss of messages may occur. Since channels assigned to VANETs only have a bandwidth of 10 MHz, variations in the user offered load to the channel, e.g., variations in the vehicular density, transmission rate, transmission power or packet size, may introduce channel congestion and have a degrading effect on the performance causing a decrease of packet reception probability, in other words, there is an increase on the packet drop and packet collision probabilities.

2.3.3 MAC operation

VANETs, like other wireless networks, face some difficulties relative to MAC operation, but a main difference arises: in VANETs, there is no central communication coordinator because of the ad-hoc nature.

2.3.3.1 Hidden Node Problem

As described in IEEE Std 802.11 - 2007 [20], a hidden station[2] is “a station (STA) whose transmissions cannot be detected using carrier sense (CS) by a second STA, but whose transmissions interfere with transmissions from the second STA to a third STA". Take as example the topology of Figure 2.10 with node B being surrounded by two nodes: Each node is within communication range of node B, but the nodes cannot communicate with each other.

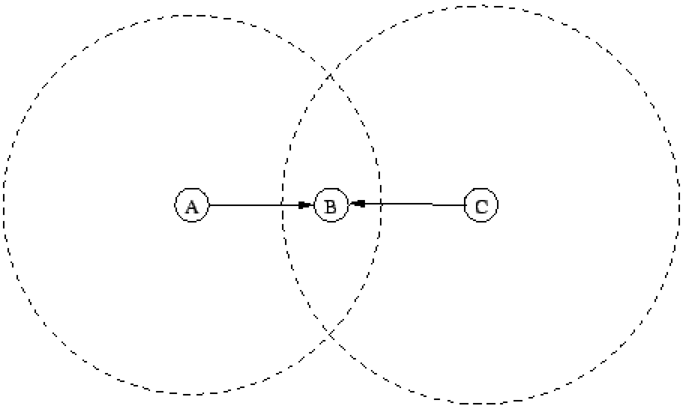


Figure 2.10: Hidden Node.

The problem is when nodes A and C start to send packets simultaneously to node B. Suppose node A starts its transmission. Since node C is too far away to detect A’s transmission, it assumes that the channel is idle and begins its transmission, therefore causing a collision in node B with node A’s transmission. From the point of view of A, C is a hidden node since C cannot detect node A’s transmission. In wireless networks it is not feasible to implement Carrier Sense Multiple Access with Collision Detection (CSMA/CD) in order to sense the medium and send at the same time. Instead, as refered to in 2.2.1.2, IEEE 802.11 uses CSMA/CA mechanism to coordinate the access to the medium to detect multiple accesses in order to avoid collision. In Figure 2.10 since node A and C cannot sense the carrier, the use of only CSMA/CA can cause collisions, scrambling data.

2.3.3.2 Absence of RTS/CTS and feedback mechanisms

To overcome the problem of collisions brought by hidden nodes, an optional four-way handshake mechanism, implemented prior to transmission [29], is used in IEEE 802.11. Take, as example, Figure 2.11.

If a node wants to send a data packet, it will first wait for the channel to become available and then transmit a Request To Send (RTS) packet. The receiver, assuming it listens to an available channel, will immediately respond with a Clear to Send (CTS) packet that allows the first node to start the transmission. This CTS packet does an important additional function, that is to inform

[2] Also known as node.

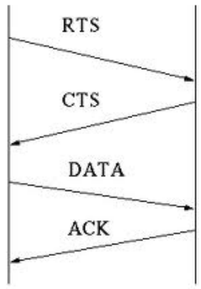


Figure 2.11: Four-way handshake.

neighboring nodes, especially hidden nodes relatively to the transmitter, that they will have to remain silent for the duration of the transmission. After the transmitter sends the DATA packet, the receiver sends an Acknowledgement (ACK) packet back to the transmitter to verify that it has correctly received the packet, after which the channel becomes available again. However, in safety-oriented VANETs applications most traffic will be broadcast traffic, which is sent without a prior RTS/CTS handshake and without acknowledgments. RTS/CTS are designed for unicast communications and like as described in [30] such a handshake is only appropriate if the amount of data transmitted is much higher than the overhead introduced by the RTS/CTS handshake, reminding that, in VANETs, periodically, only a few data is broadcast with the current position and movement, and possibly with additional location information. Furthermore, the vehicle that is transmitting cannot guarantee the correct reception at the vehicles in the neighborhood because feedback mechanisms, like ACK messages, are not implemented since it could cause broadcast storms in areas with high vehicular density or high transmission rate. Since feedback mechanisms are not implemented, the contention window, referred in Section 2.2.1.2, is always the same, which can have impact in the number of transmissions starting at the same contention time slot causing additional collisions at the receivers.

2.4 Simulation of VANETs

Network simulators are used for diverse reasons including validation of approximate analysis, understanding of complex interactions, and evaluation among alternatives. Network simulators play an important role in studying vehicular communications due to the cost of deployment of such systems.

2.4.1 The NS-3 Network Simulator

NS-3 [31] is a popular, well maintained and open license (GPLv2) discrete-event simulator oriented to network research. It is designed to be fast, flexible and accurate. NS-3 is a new simulator, intended to replace NS-2 and is not backwards compatible to NS-2, dropping NS-2 historic burdens. NS-3 is fully written in C++ but creates optional language bindings like Python.

NS-3, like most of the network simulators, abstracts significantly the physical layer details and the channel models [6]. The NS-3 standalone implementation considers the packet as an inseparable collection of bits as well as the smallest simulation unit, which does not permit to distinguish individually the bits with errors and, thus, the frame is fully received or not at all. Network simulators do not permit a thorough understanding in how packet collisions occur and their consequences to the systems' performance and therefore do not permit the analysis of possible gains of interference cancellation.

2.4.2 *PhySim-WiFi* Module

PhySim-WiFi aims at giving a physical layer perspective to the NS-3 network simulator. The *PhySim-WiFi* module for NS-3 contains a physical layer implementation of the OFDM PHY specification for the 5 GHz band and also emulates the wireless channel. This research work has its origin in the development of this module since it allows the application of more accurate channel models and also the study of low-level receiver techniques and their impact on the proper reception of packets [6]. *PhySim-WiFi* represents the frame in terms of bits and complex time samples which permits the study of packet collisions in detail, assessing the benefits of interference cancellation.

The *PhySim-WiFi* implementation does not require major modifications to NS-3, since it is a drop-in replacement of the default *YansWifiPhy* model. In this work, NS-3.9 with the *PhySim-WiFi* 1.0 module was used; however, we performed modfications to *PhySim-WiFi* in order to fulfill the objectives proposed to this work. We already include the modifications in the overview of the simulator.

In this section, first, the architecture of the physical layer emulation within NS-3 and the physical layer state machine will be presented. Then, we present three important parts of the module for the objective of this work: frame construction, channel modeling and frame reception.

2.4.2.1 Design Overview

The physical layer emulator imitates the behavior of a real IEEE 802.11 chipset.

The four main steps performed by the physical layer are presented in Figure 2.12. In step 1, the frame is transformed into a sequence of bits. In step 2, after modulation the bits are encoded into a sequence of complex time domain samples. These samples are the input for the channels models. Event 3 and 4 represent the demodulation and the verification of frame errors. The verification is done by comparing the transmitted and the received bits, and is executed after using forward error correction bits [8].

2.4.2.2 Physical Layer State Machine

The physical layer simulator can be in 5 different states during its operation (Figure 2.13). The *IDLE* state is maintained while there is no transmission or reception ongoing and the energy sensed in the medium is below the Clear Channel Assessment (CCA) threshold. If the energy detected in the medium is above CCA threshold and no preamble is detected, then the state is *CCA_BUSY*.

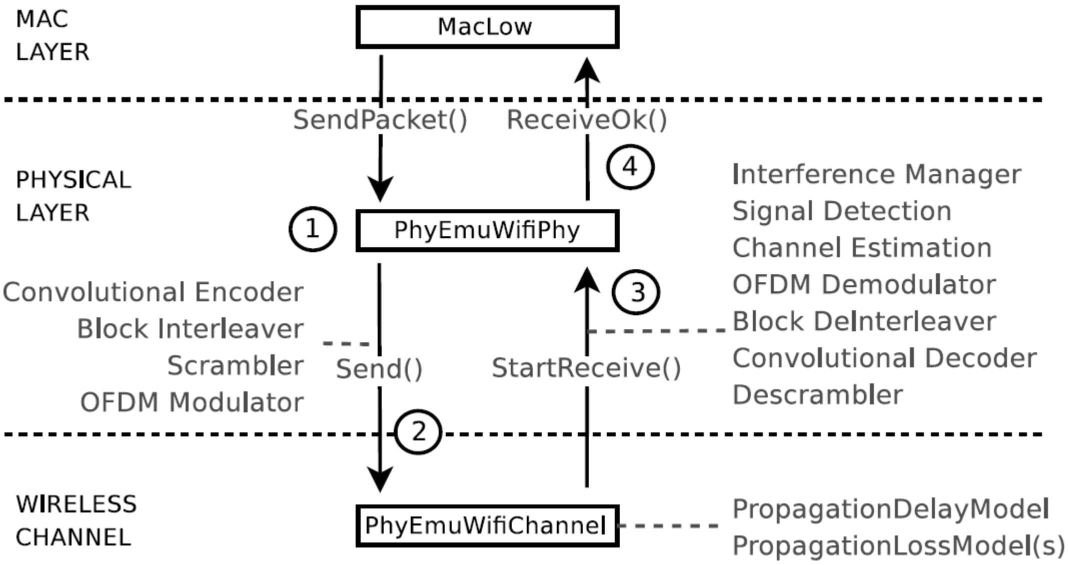


Figure 2.12: Architecture of the physical layer emulation within NS-3. Extracted from [6].

During the *CCA_BUSY* or *IDLE* states, if a signal is decoded, the physical layer simulator changes to *SYNC* state. In the *SYNC* state if the header is successfuly decoded, then the state switches to *RX*, otherwise the state will be again *CCA_BUSY* or *IDLE* depending on the energy sensed in the medium. This shift also happens in the end of a reception. During the *CCA_BUSY* state, the transmissions are blocked; furthermore, transmissions can only occur during IDLE or SYNC states.

Transitions from *RX* to *SYNC* and from *SYNC* to *SYNC* were added to achieve frame capture capabilitites. Whether the receiver is in the in the *RX* State or in the *SYNC* State, if a second frame arrives at the receiver with Signal to Interference-plus-Noise Ratio (SINR) above the capture threshold, the receiver performs a re-synchronization to the second frame and tries to decode it.

2.4.2.3 Frame construction

In *PhySim-WiFi*, the payload has the size specified in the header of the frame and is generated randomly in case of real data is not provided. The payload is encoded with the parameters defined by the user. For VANETs, by default, the payload rate is 6 Mbps and QPSK is used. The payload encoding is represented in Figure 2.14. Briefly, this encoding includes a Scrambler to eliminate long sequences consisting of ’0’s or ’1’s, a Convolutional Encoder to add redundancy, and a Block Interleaver to ameliorate the problem of burst errors and to separate the bit stream into blocks with the same size which are able to fit in an OFDM symbol. For the data rate of 6 Mbps, each block is modulated with QPSK to which are added pilot symbols in 4 of the 52 sub-carriers. In the end Block Interleaver modulates the block in OFDM symbols, each one with 80 time samples.

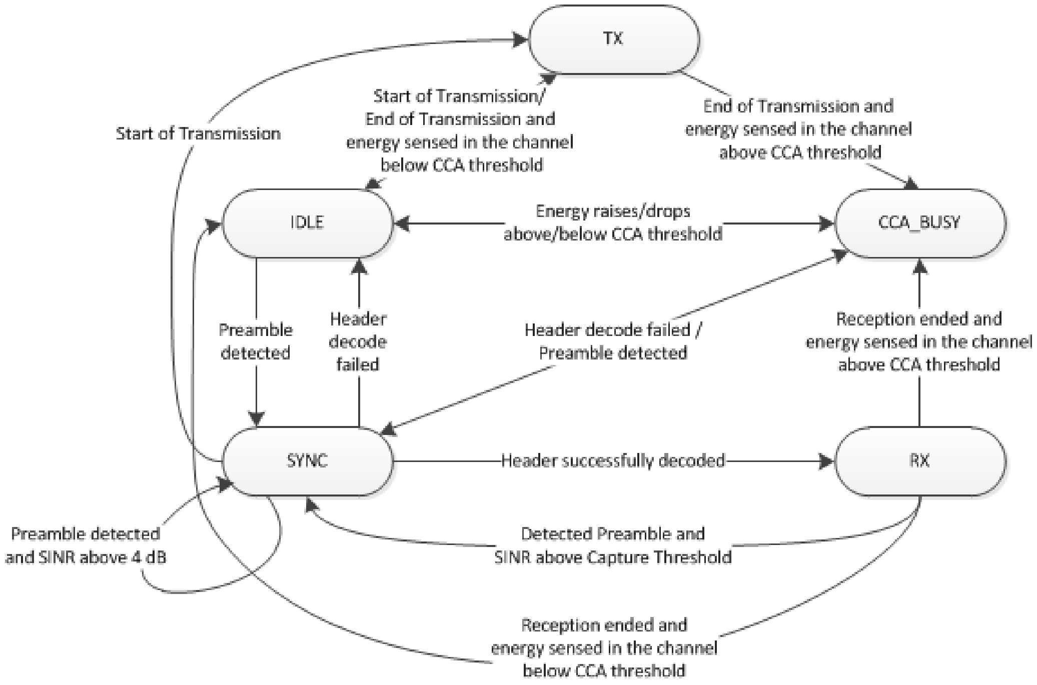


Figure 2.13: The *PhySim-WiFi* state machine. Based on [6].

The preamble of the frame and the signal header are coded with the most robust rate, 3 Mbps, and with the most robust modulation scheme, BPSK. This encoding follows the same steps as payload encoding except for the absence of bit scrambling. After the encoding, the preamble and the signal header are added to the payload, which altogether are concatenated into a vector of complex time samples. The transmission power and transmitter antenna gain factors are applied to the samples after their energy is normalized to unit power [6]. If the medium is sensed cleared (i.e., energy sensed is below clear channel assessment threshold) and the transceiver has a request from upper layers to send a packet, the transmitter will cancel any attempt to receive packets in order to transmit. A small unit of information, called *PhySimWifiPhyTag*, is created to store the complex time samples and other information used by the signal processing sub-modules. Every packet has attached a *PhySimWifiPhyTag*. A small random frequency offset is applied in the receiver to the time samples in order to recreate the effect of oscillator offsets of the transmitter.

2.4.2.4 Modeling the Wireless Channel Effects

The wireless channel module permits chaining several propagation loss models, i.e., the output of one model serves as input for the next model. Examples are presented in Figure 2.15.

The *PhySim-WiFi* implementation makes use of the IT++ processing library [32]. IT++ library provides a large collection of channel models. *PhySim-WiFi* supports basic pathloss models but also large- and small-scale fading models as well as multi-tap channel models. Multi-tap channel models permits the modeling of time and frequency-selective channels.

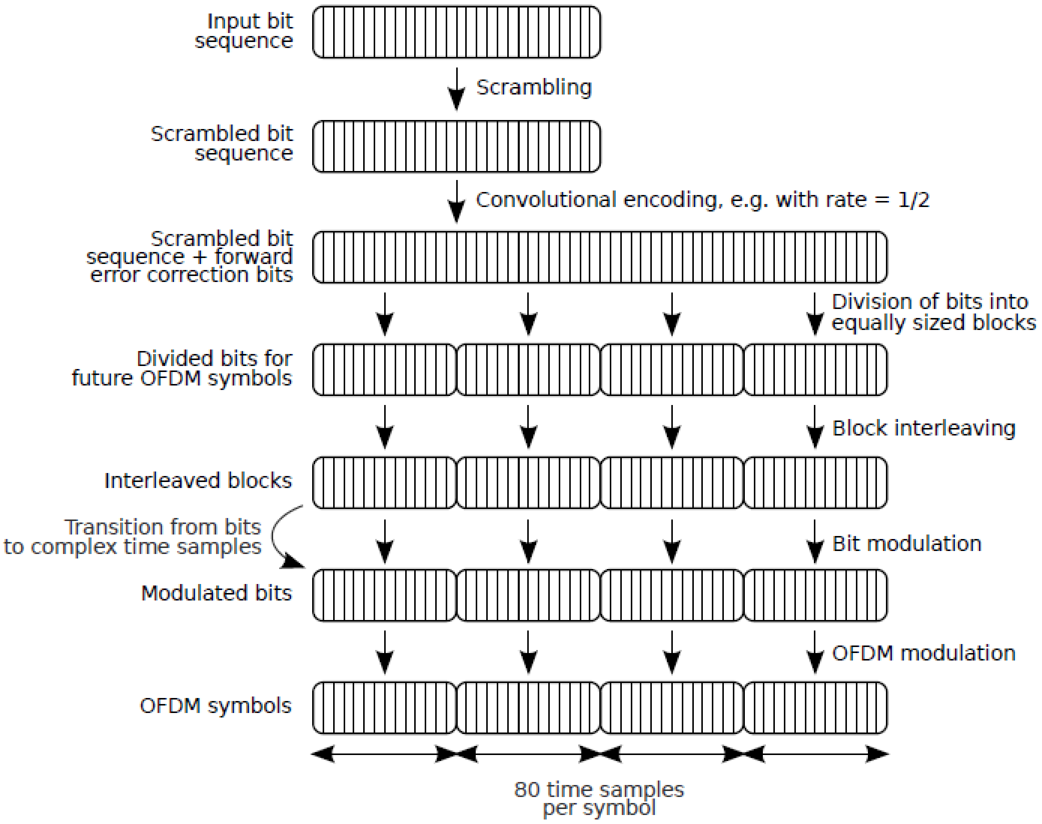

Input bit sequence
Scrambling
Scrambled bit sequence
Convolutional encoding, e.g. with rate = 1/2
Scrambled bit sequence + forward error correction bits
Division of bits into equally sized blocks
Divided bits for future OFDM symbols
Block interleaving
Interleaved blocks
Transition from bits to complex time samples
Bit modulation
Modulated bits
OFDM modulation
OFDM symbols
80 time samples per symbol

Figure 2.14: Encoding of the payload. Extracted from [8].

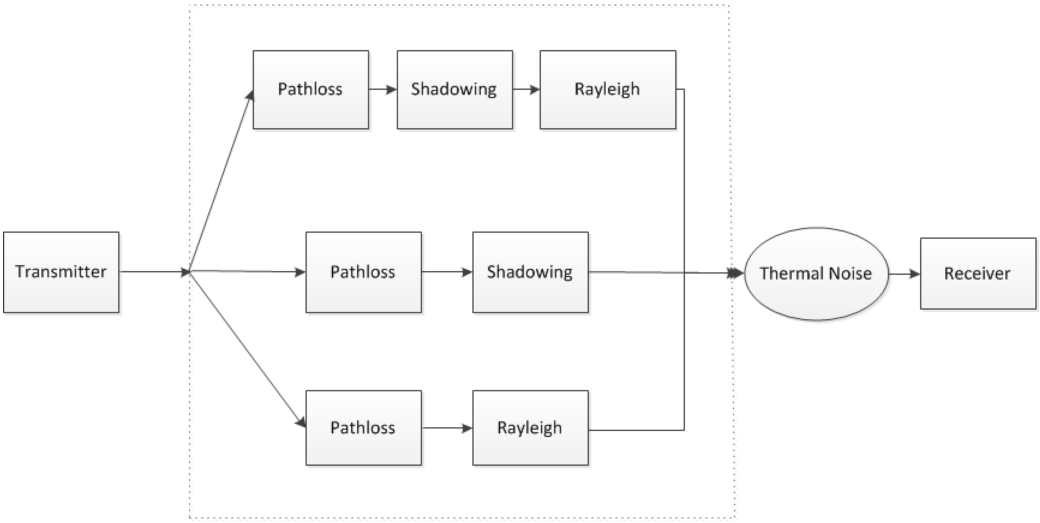


Figure 2.15: Channel modelling.

2.4.2.5 Frame Reception Overview

The four events of the reception process are shown in Figure 2.16: *StartReceive()*, *EndPreamble()*, *EndHeader()* and *EndRx()*. During simulations, the simulator permits the use of callback functions to perform evaluations of the scenarios.

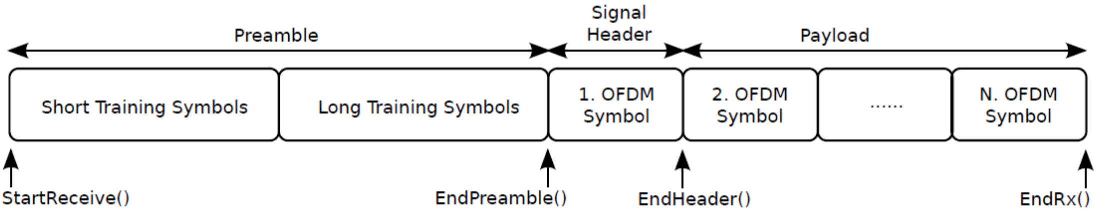


Figure 2.16: Frame Reception. Extracted from [8].

StartReceive() - For every frame sent by a node, there will be a *StartReceive()* event in the rest of the nodes. *StartReceive()* event (Figure 2.17) is executed when the first sample of a frame arrives at a receiver. Only the frames received with energy equal or higher than thermal noise (-104 dBm) are considered and their complex time samples are added to the *InterferenceManager*, which contains the list of all frames arrived to each receiver in order to account for interference. If the receiver is in the *IDLE* or *CCA_BUSY* state, the simulator generates the *StartRxOkTrace* callback and schedules the second event. When the receiver is in the TX state, it will ignore the incoming packet in order to send its own packet and will generate the *StartRxErrorTrace* callback. If the receiver is in the *SYNC* or *RX* state and the signal arrived with SINR equal or above the capture threshold then the simulator performs the capture effect, generates the *StartRxOkTrace* callback and schedules the second event, otherwise the packet is dropped and it is generated the *StartRxErrorTrace* callback.

EndPreamble() - The second event, *EndPreamble()* (Figure 2.18), begins after the duration of the preamble. If the receiver is in *RX* state and detects a preamble (i.e., signal detection and synchronization are successful) of a signal arrived with a preamble's SINR equal or above the capture threshold, then the simulator performs the capture effect, schedules an EndHeader() event and generates the *EndPreambleOkTrace* callback. If the receiver is not in the *RX* and detects a preamble of a signal arrived with SINR equal or above 4 dB, it schedules an EndHeader() event and generates the *EndPreambleOkTrace* callback. Additionally to this, if the receiver is in the *SYNC* State the receiver performs the capture effect. If a signal arrives, depending on the receiver state, with SINR below 4 dB or below the capture threshold, it is dropped and an *EndPreambleErrorTrace* is generated.

EndHeader() - The header decoding is performed in the third event, called *EndHeader()* (Figure 2.19). If the values presented in the header are coherent and the receiver continues in *SYNC* state, then a fourth, and last event, is scheduled, otherwise it is generated a *HeaderErrorTrace* callback and the packet is dropped.

EndRx() - In the last event of a frame reception, *EndRx()* (Figure 2.20), the data symbols are decoded and the correspondent data bits are compared to the ones transmitted. A successful reception happens only if both are identical [6, 8]. If a packet collides with other(s) packet(s), then it is considered a *Capture Reception* and a *RxOkTrace* callback is generated, else it is a *Alone Reception*. Whenever the received data is not equal to the transmitted data a *RxErrorTrace* callback is generated and the packet is considered as a drop.

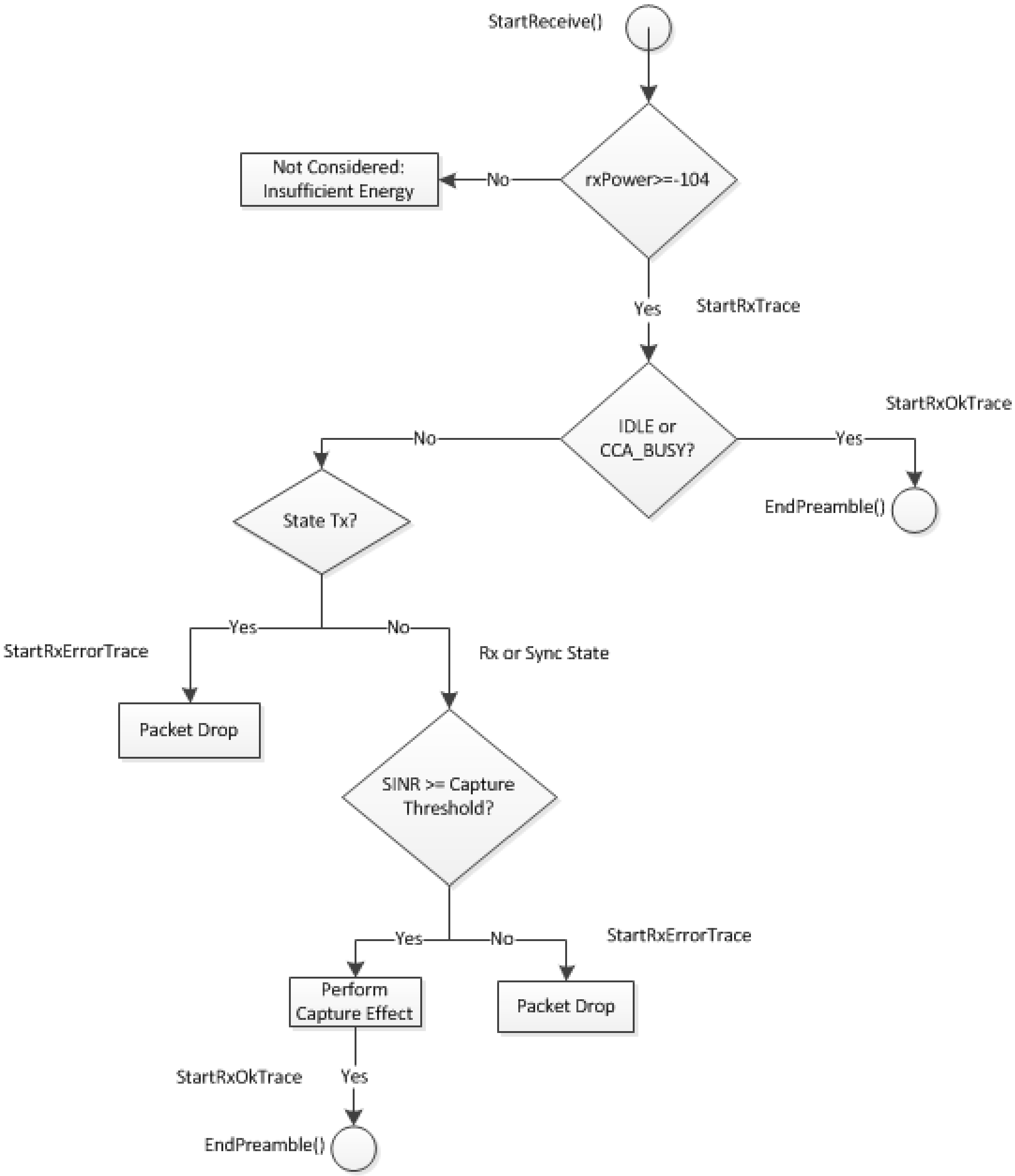


Figure 2.17: *StartReceive()* event.

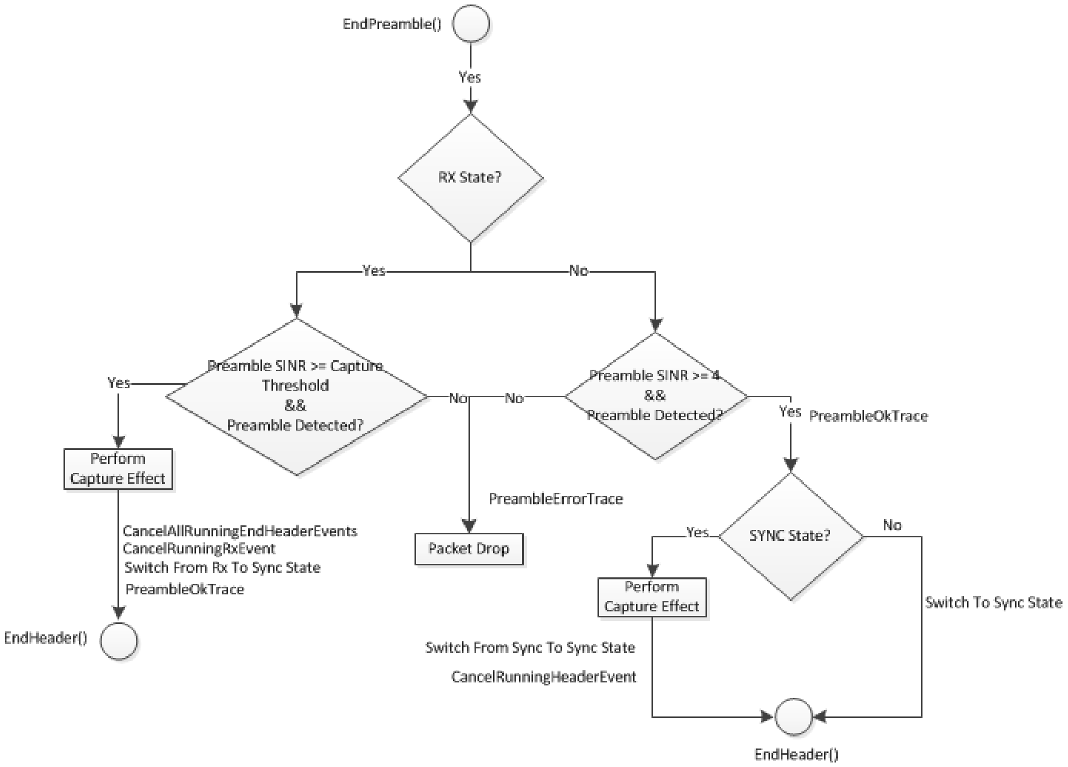


Figure 2.18: *EndPreamble()* event.

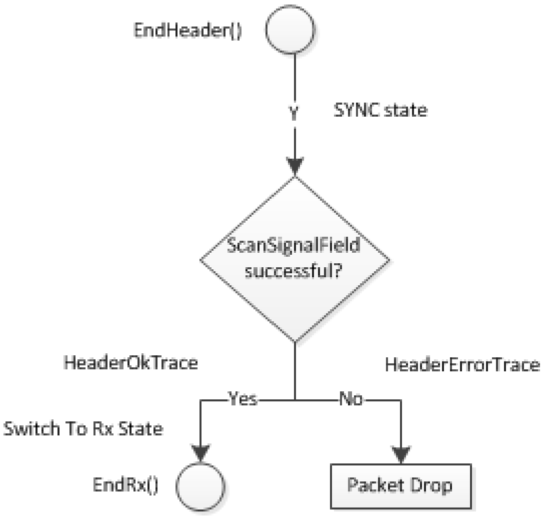


Figure 2.19: *EndHeader()* event.

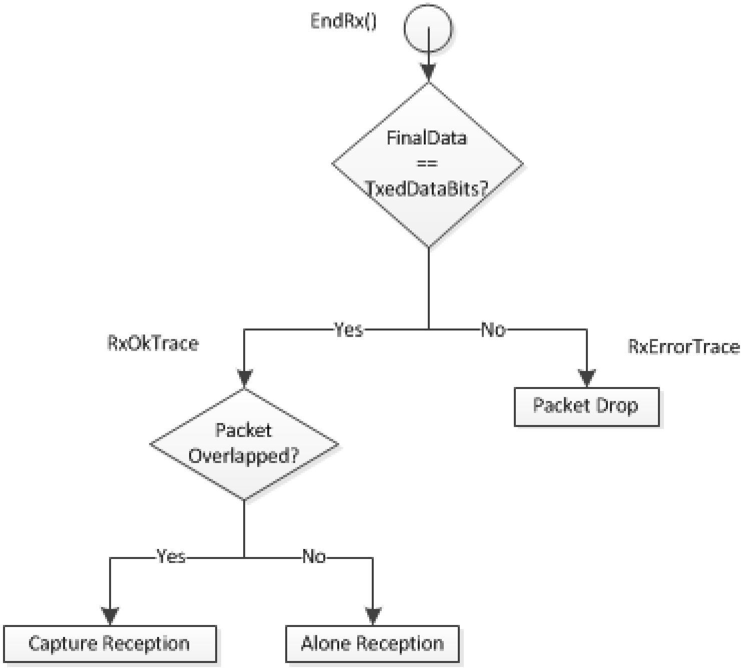


Figure 2.20: *EndRx()* event.

2.5 Interference cancellation

Interference cancellation techniques exploit the fact that interfering signals have structure determined by the data that they carry, distinguishing them from noise [3].

2.5.1 Successive Interference Cancellation

It is known that it is possible, under specific conditions, to successfully decode and receive even overlapping packets, almost achieving Shannon's channel capacity theorem [2]. The technique that is used to achieve this is called Successive Interference Cancellation (SIC). SIC is a nonlinear type of Multiuser Detection (MUD) scheme in which users are decoded successively. SIC consists of a physical layer technique that allows a receiver to decode packets that overlap in time. Considering two packets overlapping at a receiver, normally, using capture effect and under certain conditions, only the strongest signal could be decoded, treating the other signal as noise. SIC permits the recovery even of the weaker signal by subtracting the strongest signal (i.e., highest SINR) to the combined signal and extracting the weaker signal from the residue.

The generics steps of a SIC receiver is presented in Figure 2.21. Energy detection and synchronization happen just like in a conventional receiver [3]; however, SIC receivers have to check for multiple users. The prerequisite of the algorithm is that in each iteration there must be a signal with SINR sufficient to be recovered, as in any conventional receiver. This way, the receiver can detect multiple users and at the same time decode the strongest signal. After decoding the

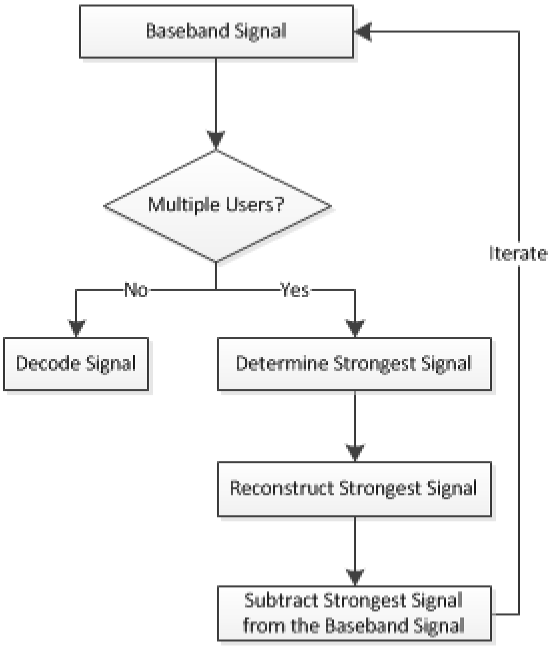

Baseband Signal
Multiple Users?
No
Yes
Decode Signal
Determine Strongest Signal
Reconstruct Strongest Signal
Subtract Strongest Signal from the Baseband Signal
Iterate

Figure 2.21: Example of a SIC algorithm.

bits from the strongest signal, the original signal is reconstructed from these bits, generating an ideal copy of the signal. Then, this copy is subtracted (i.e., cancelled) from the combined signal resulting in the remaining transmissions plus an approximation error, which act as a feedback for the detector to continue the process. The approximation error is due to the approximation in the reconstruction of the strongest signal [3].

2.6 Related work

Although there are some works on the assessment of the performance of IEEE 802.11-Based One-Hop Broadcast in coordinating the medium access to avoid packet collisions, only [7] analyzes the hidden problem providing, according to the communication ranges of the nodes, a transmission distance 'robust' against hidden nodes. In the work, the authors performed simulations with NS-2 using capture effect and different channel propagation models to understand their benefits or losses in the scenarios. They also include a scalability analysis by increasing the transmission power and transmission rate frequency and hence increasing the user offered load to the channel. As expected, they verified that for an increase of user load offered to the channel, an increase of packet drops and collisions would happen, mostly due to the hidden node. In the study, the physical layer configuration values envisioned at that time for VANETs were used; however, some differences to the present should be referred. The maximum transmitting power used was -9.1 dBm, which corresponds to 200 meters of communication range. This value is considerably lower than the IEEE 802.11p default transmitting power of 20 dBm. Using a transmit power of 20 dBm causes an increase of nodes in the same communication range and therefore an increase of the user offered load to the channel. The data rate was set to 3 Mbps instead of the default rate of 6 Mbps. A lower data rate corresponds to a more robust rate. The contention window was defined to 511 slots after preliminary simulations to reach a value which represented a low probability of two nodes inside the same communication range would select the same contention slot to transmit. In 802.11p, the standard CW is 15. Therefore, considering the differences in those values in addition to NS-2 limitations, we can conclude this thesis can present some relevant differences using more realistic parameters.

SIC has already been applied to ZigBee [3], to IEEE 802.11b in [4] and is frequently used in Code Division Multiple Access (CDMA) systems to perform multi-user detection [5]. In [3] they concluded that SIC outperformed conventional receivers during collisions, by turning 45 % of competing links from hidden terminals into links that can send together in this network and in [4], the spatial multi-access with their technique had throughput gains of 45-76 % with a 5.5 Mbps data rate, and 31-61 % with 11 Mbps. Although several works have applied SIC schemes for OFDM systems, they all address the suppression of ICI, none with the purpose to ease packet drops due to collisions.

To the best of our knowledge, there is no work done in characterizing packet collisions or using SIC receivers in OFDM-based IEEE 802.11p communications. The latest development of a physical layer simulator sufficiently accurate and the recent standardization of IEEE 802.11p are among the possible reasons for this.

Chapter 3

Characterization of Packet Collisions

This chapter presents the methodology adopted to accomplish the objectives proposed for this thesis. We present a summary of our approach to the problem.

Firstly, in Section 3.1, we start by defining the main terms needed to characterize packet collisions, by gathering or defining terms that ensure we are aligned with the state of the art and we have the foundations necessary to perform a correct assessment of VANETs' communications performance. Secondly, we implement in NS-3 with *PhySim-WiFi* a set of metrics that in our opinion permits to evaluate the degradation in the communications performance introduced by packet collisions and assess the possible throughput gains obtained by the introduction of a SIC scheme in the receivers. These metrics are presented in Section 3.2. Thirdly, in Section 3.3, we present the scenario configurations to use in a wide variety of simulations. The parameters we choose to vary in the simulations are the ones that best characterize the communications performance. Using the metrics implemented and the variations in the scenarios, we are able to thoroughly characterize the packet collisions and assess the advantages and disadvantages of implementing SIC. Finally, Section 3.4 shows the modifications incorporated in *PhySim-WiFi* module to perform the evaluations proposed.

3.1 Definitions

The most important terms for this work are defined below.

Signal - A signal is the complex representation of one or multiple bit(s). Signals are used to carry the bits that constitute a data packet. As such, a data packet is represented by a sequence of signals.

Node - A node is a system entity that is equipped with a transceiver. It is able to transmit and decode signals.

Network - A network is established if a set of nodes is able to communicate with each other.

Packet Transmission - A packet transmission is the event (i.e., the point in time) at which the physical layer finished the transformation of data bits to a sequence of signals and starts transmitting the signal to the channel. Consequently, it is the time at which the first signal is put on the channel.

Node transmission behavior - The transmission behavior of a node defines how much data a node is transmitting to the network. The transmission behavior includes the rate (in packets per second) at which packets are generated, the size (in bytes) of the payload of each packet, the data rate (modulation scheme and coding rate) that is used to encode each packet, as well as the transmission power (in dBm) that is used for transmission. From now on, when we refer packet size, in fact we are referring to the payload size.

Scenario - A scenario is a concrete instance of a network and is described by the number of nodes that are participating in the network, the nodes' spatial distribution, the mobility behavior of each node, the channel configuration, as well as each node's transmission behavior. Example: 50 nodes, uniformly distributed along a highway with 4 lanes and a length of 2 km, no mobility (i.e., static), a simple Friis path loss channel model, each node transmitting 10 packets per second using a packet size of 500 bytes, a data rate of 6 Mbps in a 10 MHz channel and a transmission power of 20 dBm.

Channel Model Configuration - The channel configuration defines how signals attenuate with respect to the distance between sender and receiver, and how they fade with respect to time. Examples: 1) The channel includes a path loss that follows the Friis model[1]. No fading is considered. 2) The channel includes a path loss that follows the Two-Ray Ground (TRG) pathloss model[2]. No fading is considered.

Communication Range (CR) - The maximum distance at which a node's packet can be decoded by a second node, considering it did not suffer fading and there was no interference at its arrival. Under these circumstances, a packet has to arrive at the receiver with energy equal to or higher than -95 dBm, to be successfully decoded. This range is only applicable for deterministic channel models, such as TRG.

Carrier Sensing Range (CSR) - The maximum distance at which a node can determine that there is a transmission ongoing in the channel, assuming the use of a deterministic channel model, such as TRG. The CCA threshold is set to -95 dBm; therefore, any packet arriving with energy equal to or higher than -95 dBm can be sensed. However, every packet arriving at a node with energy equal to or higher than -104 dBm is counted for interference.

User load offered to the channel - The estimated useful offered load to the channel, i.e., without considering the overhead from the MAC Header and the PHY Preamble. Considering a

[1] Friis model considers there is no multipath and the signals propagate through free space, i.e., under ideal conditions.

[2] Two-Ray Ground pathloss model considers that a single ground reflection dominates the multipath effect, thus, the received signal is an aggregation of two components: the transmitted signal propagating through free space and the transmitted signal reflected off the ground [23].

scenario with 20 nodes per kilometer in a highway with 4 lanes, the nodes with a communication range of 1000 meters (assuming the use of a deterministic channel model), with the nodes sending 10 packets per second, each packet with 500 bytes, the user offered load to the channel (in Mbps) can be estimated by:

$$Load \approx 40[\text{Veh./Commu.Range}] \times 10[\text{packets/s}] \times 500[byte] \times 8[\text{bit/byte}] = 1.6\text{Mbps} \tag{3.1}$$

Packet Arrival - The packet arrival is the event at which the first signal of a transmitted packet arrives at a certain node with a energy greater than thermal noise, i.e., greater than -104 dBm. All packets arriving with signal strength below thermal noise are considered to be part of the noise and are not counted as a packet arrival or to interference.

Packet Reception - A packet reception is the successful decoding of packet's signal representation and can only be determined after all signals have arrived at the receiving node. As such, packet arrival and packet reception reflect different events and different points in time. Further, to characterize the circumstances under which the reception was achieved, a distinction between

1. reception in the absence of any interference (termed Alone Reception), and
2. reception despite the existence of interference (termed Capture Reception)

is made.

Interference - Interference is the sum of the energy of all interfering transmitters I = $\sum_i I_i$ to a given received transmission. A packet is treated as and accounted to interference if its signal strength is greater than thermal noise.

Thermal noise - The noise introduced by the antenna's receiver itself. The thermal noise's power $P_{Thermalnoise} = KT_0B$, where the Boltzmann constant K is $\approx 1.38 \times 10^{-23}$, the temperature T_0 is 300 in Kelvin and the bandwidth B is 10 MHz for VANETs. Therefore, thermal noise for VANETs is -104 dBm.

Background Noise - Amount of signal created from all noise sources (including thermal noise).

Cumulative noise - Sum of the background noise and the interference.

SINR - Defined as the ratio between a signal S and interference I plus noise N: $SINR = \frac{S}{I+N}$, where SINR reflects the capability of a device to recover data from a given signal.

Packet Collision - Packets collide when two or more packets overlap in time, at a given receiver.

Capture Effect - The phenomenon where a reception is interrupted and cancelled to give place to a re-synchronization of a stronger packet. The packet from the reception that is interrupted is dropped.

Packet Drop - A packet is dropped whenever the physical layer is not able to successfully decode it. The causes of failure[3] can be:

1. **TX State** - Node is currently transmitting a packet itself,
2. **Insufficient Energy** - The signals of the packet arrived with signal strength below background noise,
3. **Capture Effect** - The receiver dropped the packet in detriment of other packet with a SINR above the 8 dB capture threshold,
4. **Processing** - The receiver was not able to decode properly the signal, i.e., there was a collision with one or more packets or due to imperfections on the signal decoding of the receiver,
5. **SYNC State** - The receiver was already in SYNC state and the signals of the packet arrived with a SINR below the 8 dB capture threshold,
6. **RX State** - The receiver was already in RX state and the signals of the packet arrived with a SINR below the 8 dB capture threshold.

For each of the 4 events described in Section 2.4.2.5 there is a set of causes of packet drops.

- In StartReceive() event, Figure 3.1, packet drops can be because of TX State, SYNC State, RX State or Insufficient Energy:

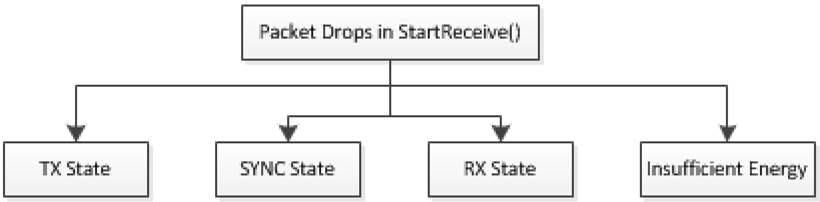


Figure 3.1: Causes of packet drops in StartReceive() event.

- In EndPreamble() event, Figure 3.2, packet drops can be because of SYNC State, RX State, Processing or due to Capture Effect:

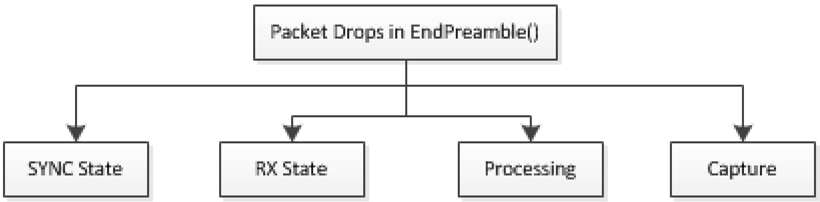


Figure 3.2: Causes of packet drops in EndPreamble() event.

- In EndHeader() event, Figure 3.3, packet drops can be because of RX State or Processing:

[3] Note: Fading was not considered in this work.

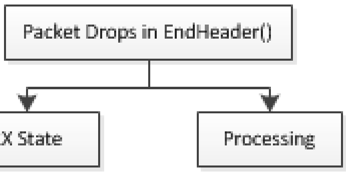


Figure 3.3: Causes of packet drops in EndHeader() event.

- In EndRx() event, Figure 3.4, packet drops are because of Processing, in other words, the transmitted bits are not equal to the bits decoded at the receiver:

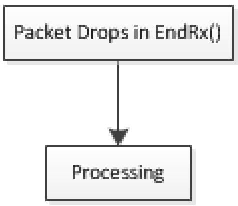


Figure 3.4: Causes of packet drops in EndRx() event.

- Additionally, as Figure 3.5 and Figure 3.6 show, every time a packet is sent or the Capture Effect is performed, respectively, any reception in course is cancelled:

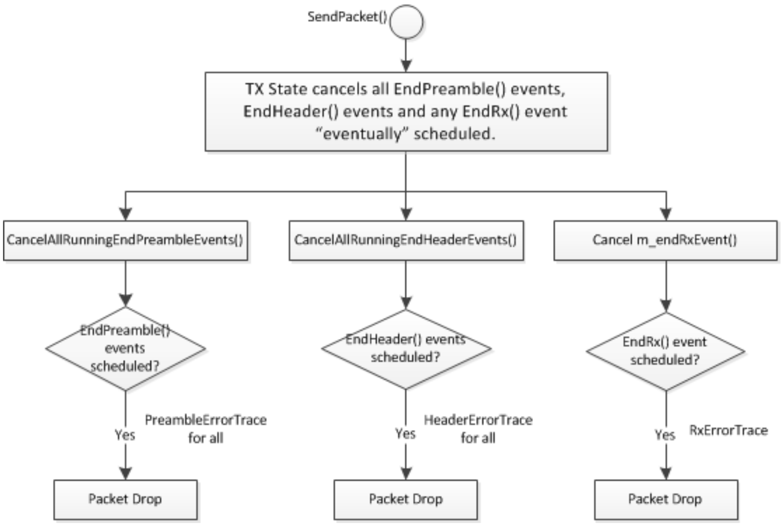

SendPacket()
TX State cancels all EndPreamble() events, EndHeader() events and any EndRx() event "eventually" scheduled.
CancelAllRunningEndPreambleEvents()
CancelAllRunningEndHeaderEvents()
Cancel m_endRxEvent()
EndPreamble() events scheduled?
EndHeader() events scheduled?
EndRx() event scheduled?
Yes
PreambleErrorTrace for all
Yes
HeaderErrorTrace for all
Yes
RxErrorTrace
Packet Drop
Packet Drop
Packet Drop

Figure 3.5: SendPacket() event cancels all running EndPreamble(), EndHeader() and any EndRx() events.

3.2 Evaluation Parameters and Metrics

Along the simulations, the user offered load to the channel is a main aspect to consider, since the system's performance is directly influenced by it. The user offered load primarily depends on

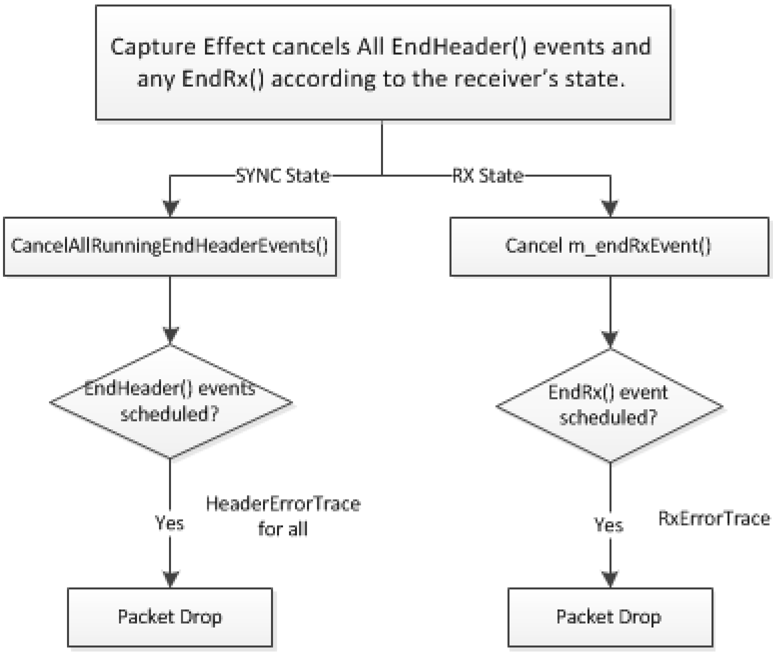

Capture Effect cancels All EndHeader() events and any EndRx() according to the receiver's state.
SYNC State
RX State
CancelAllRunningEndHeaderEvents()
Cancel m_endRxEvent()
EndHeader() events scheduled?
EndRx() event scheduled?
Yes
HeaderErrorTrace for all
Yes
RxErrorTrace
Packet Drop
Packet Drop

Figure 3.6: Capture Effect cancels all running EndHeader() and any EndRx() events.

the node's transmission behavior (i.e., transmission rate, packet size and transmission power) and on the node density in the communication range. Although the user offered load to the channel can be estimated by Equation 3.1 in Section 3.3, the reality is slightly different due to protocols' operation and therefore for each simulation we record, in a file, the user offered load to the channel.

All of the metrics described below are implemented with respect to distance between sender and receiver.

We start our analysis with a superficial overview of the system's performance by implementing the *Packet Reception Probability* and *Packet Drop Probability* metrics, which give the probability of a packet be received or dropped, respectively, with respect to the distance between sender and receiver. In fact, these two metrics are complementary. First, the *Packet Drop Probability* is implemented independently of the circumstances, i.e., we implement it without making an in-depth characterization. This way, we have a rough perspective of the system's scalability and we are able to identify in which of the events, defined in Section 2.4.2.5, drops are more likely to occur. Only after that, we implement the *Packet Drop Probability* depending on the circumstances: drop due to TX State, Insufficient Energy, Capture Effect, Processing, SYNC State or RX State. Furthermore, we identify the most important causes of packet drops in each event.

Having packet drops described, the next step is to characterize packet collisions in order to understand the severity of the interference and the complexity of implementing interference cancellation, implementing the following metrics from the point of view of every single packet. First, we implement the *Probability that packet can be involved in a collision* metric to identify, for a given distance between sender and receiver, the probability of a packet being involved in a collision with other packets and perform a first assessment on the advantages of SIC implementation. Then, we implement the *Energy distribution of colliding packets* metric to infer the severeness of the interference from colliding packets; furthermore, with this metric we can differentiate the causes of packet collisions (between transmissions in the same contention slot and the hidden node problem), by observing the energy distribution of the overlapping packets. Finally, the *Number of packets overlapping* metric is implemented to evaluate the complexity needed for a SIC implementation. In other words, this metric shows the number of packets that overlapped with each packet involved in a collision and, therefore, we can determine the number of iterations our SIC implementation should perform. The more packets colliding at the same time, the more iterations a SIC implementation needs to perform in order to recover all packets. In this metric, we consider a collision when each of the packets arrive with energy above -95 dBm, which is the energy a signal needs to have in order to a node successfully decode it, considering it did not suffer fading and there was no interference at its arrival.

The final metric, *Probability of Recovery through SIC*, is implemented to assess the throughput gains, with respect to the distance between sender and receiver, introduced by a perfect SIC implementation. By considering the receiver performs perfect decoding and reconstruction of a packet that was captured, the receiver is able to perfectly cancel its interference from the rest of the signals and therefore we have an upper-bound for the gains in recovering packets from collisions with captured packets, using a SIC implementation. Nevertheless, this metric allows to conclude, taking into consideration the disadvantages from the previous metrics, if SIC is worth being implemented in VANETs.

In summary, to characterize the communication's performance, packet collisions and trade-offs in the implementation of interference cancellation, the following main metrics are used:

- *The user offered load to the channel.*
- *Packet Reception and Packet Drop Probabilities.*
    - Independent of the circumstances.
- *Packet Drop Probability.*
    - Dependent of the circumstances.
        - Due to TX State.
        - Due to Insufficient Energy.
        - Due to Capture Effect.
        - Due to Processing.
        - Due to SYNC State.
        - Due to RX State.
- *Characterization of Packet Collisions with respect to distance between sender and receiver.*
    - Probability that packet can be involved in a collision.

    - Energy distribution of colliding packets (Histogram).
    - Number of packets overlapping with each packet (Histogram; Average values).

- *Probability of Recovery through SIC.*

3.3 Scenario Configurations

A highway scenario was always considered; however, different configurations are simulated. Each configuration is simulated with 10 different random number generators, called seeds, to perform averaging of the results. A seed is used to generate a sequence of unique random numbers, which is used during simulations. The random numbers are used to generate the first packet of each node at a time uniformly distributed in the interval between 0 and the inter-packet time for the scenario. In this way, there is little likelihood that packet generation in different nodes is synchronized.

The following parameters are used:

- Node Density:

    - 20 nodes/km. Using highway scenario with 5 km length, there are 100 nodes.
    - 60 nodes/km. Using highway scenario with 5 km length, there are 300 nodes.

  To perform all the evaluations, we selected 10 nodes in the center and a highway with 5 kilometers length in order to avoid border effects.
  We choose two different node densities to reflect scenarios with low number of nodes and with high number nodes per kilometer. This parameter determines the number of nodes which periodically broadcast information in the scenario and, therefore, it is straightforward it has an impact on the performance of the system. For example, an increase in the node density can increase the number of collisions due to transmissions in the same contention slot time and due to the hidden node problem.

- Nodes spatial distribution:

    - Uniform distribution (with a small jitter) on 4 lanes.

  A highway has, normally, 4 or 6 lanes (2 or 3 lanes in each direction, respectively). We perform simulations considering only highways with 4 lanes. We assume the lanes have a width of 2.5 meters and the two directions are separated by 1.5 meters. We opt for a uniform distribution instead of using different distributions, which can lead to nodes experiencing overloaded areas and other experiencing sparse areas in the same scenario.

- Nodes' mobility behavior:

    - No mobility.

Nodes' mobility would bring additional packet drops and packet collisions; however, due to time constraints, it was not possible to incorporate nodes' mobility in the scenario.

- Channel model configuration:

  - Two-Ray Ground Pathloss model.
  - No fading is considered.

  TRG is a first step to gain insights and to understand the system under simple conditions. A second step would be to account for channel fading, which, due to time constraints, was not possible in this thesis.

- Nodes' transmission behavior:
  In each simulation, every node transmit with the same physical and traffic configuration. The traffic model is Constant Bit Rate (CBR), i.e., all packets have the same size and their transmission is periodic.

  - Data Rate: 6 Mbps in a 10 MHz channel (QPSK).
    We use the default data rate with the bandwidth allocated for safety-applications in VANETs.
  - Transmission Power:
    - ∗ 10 dBm.
    - ∗ 20 dBm.

    A packet sent with higher transmission power arrive at longer distances, which means there is an increase of the number of nodes sensing the transmission; therefore, a variation of the transmission power induces a variation of the number of nodes inside the nodes' communication range. Variation of the transmission power is fairly close to the variation of the node density. The 20 dBm of the default transmitting power for safety applications is mainly used. This transmission power corresponds to a communication range and carrier sensing range of 1125 meters. The communication range is near to the 1000 meters range envisioned for VANETs; however, since we are considering one-hop broadcasts, we also include a shorter range for transmissions and hence we include 10 dBm. This value corresponds to a communication range and carrier sensing range of approximately 630 meters.

  - Transmission Rate:
    - ∗ 2 packets/s.
    - ∗ 6 packets/s.
    - ∗ 10 packets/s.

A higher transmission rate means that more packets compete for the channel and hence more packets can collide due to transmissions in the same contention slot time and due to the hidden node problem. We use a transmission rate ranging from 2 packets per second to 10 packets per second, since we are addressing broadcasting in safety-applications. We consider these values coherent with the safety purpose.

- Packet size:
  - 100 bytes.
  - 300 bytes.
  - 500 bytes.

  An increase of packet size increases the number of bits that can be unsuccessfully decoded, and therefore can cause packet drops. Larger packet sizes also mean that receivers take more time for receptions and are more time vulnerable to the hidden node problem. A transmission of 100 bytes lasts for 456 μs, of 300 bytes lasts for 992 μs and of 500 bytes lasts 1520 μs. Small packet sizes are used to recreate safety-applications in VANETs, remembering that, periodically, only a small amount of information is broadcast. Here, 100 bytes are used to simulate low payload without security protocols, 300 bytes to simulate low payload with security protocols and 500 bytes to simulate high payload with security protocols.

3.4 Modifications to *PhySim-WiFi* 1.0

Along this work, modifications were incorporated to *PhySim-WiFi* 1.0 module to perform the evaluations proposed. Briefly, they were:

- Improvements to the Frame Reception process to incorporate the decisions presented in Figures 2.17, 2.18, 2.19 and 2.20.
- Addition of callbacks to evaluate the causes of packet drops illustrated in Figures 3.1, 3.2, 3.3, 3.4, 3.5 and 3.6.
- Implementation of TRG pathloss model.

Chapter 4

Evaluation

In this chapter, we present the most relevant results obtained in the simulations using the metrics and scenario configurations defined in the previous chapter. The results include the characterization of packet drops and packet collisions, as well as the analysis of the advantages and disadvantages of the implementation of SIC in VANETs.

4.1 Simulation Results

For our set of simulations, we use the parameters defined in Section 3.3. Table 4.1 summarizes the most important parameters. The communication's parameters not defined in there are also compliant with IEEE 802.11p standard specifically with one-hop broadcast mode.

Network simulators are well-known for their memory consumption, therefore in addition to memory management along the entire work, we only selected 11 seconds as simulation time. To avoid unwanted border effects, we perform evaluations for 9.5 seconds, excluding 1 second in the beginning and 0.5 seconds in the end.

Thirty six (36) scenarios with different configurations are tested, which correspond to three hundred and sixty (360) simulations. Each simulation took more than 12 hours, each requiring up to 12 GB memory, thus resulting in a total simulation time of 180 days. Since a high performance computing cluster was used, all simulation results could be obtained within one week.

For the clearness of reading, we selected only the most relevant data to present. Furthermore, since the user offered load to the channel recorded in files is very close to the values provided by Equation 3.1, throughout this chapter we only refer to the values resulting from the latter.

4.1.1 Packet Reception and Packet Drop Probabilities

Figure 4.1 illustrates the Packet Reception and Packet Drop probabilities with respect to distance between sender and receiver for an example scenario with fixed parameters.

Using a transmission power of 20 dBm we obtain a communication range of 1125 meters;

Parameters	Values
Data Rate (Mbps)	6
Modulation Mode	QPSK
Coding Rate	$\frac{1}{2}$
Bandwidth (MHz)	10
Node Density (nodes/km)	20, 60
Highway Length (km)	5
Lanes	4
Packet Size (Bytes)	100, 300, 500
Transmission Rate (Hz)	2, 6, 10
Transmission Power (dBm)	10, 20
Channel Propagation Model	TRG
Antenna Height (m)	1.5
Antenna Gain (dB)	0
Background Noise (dBm)	-99
Clear Channel Assessment (dBm)	-95
Capture Threshold (dB)	8
Frequency (GHz)	5.9
Frequency Tolerance (ppm)	10
Simulation Time (s)	11
Contention Window Size	15

Table 4.1: Simulation Configurations Parameters.

therefore, after that distance there is no packet successfully received. For a scenario with user offered load of ≈ 1.8 Mbps by using 20 nodes/km, transmission rate of 10 packets/s, packet size of 500 bytes and transmission power of 20 dBm, we obtain a probability of almost 100 % of packet receptions for distances between sender and receiver shorter than 550 meters. In other words, we obtain a probability of almost 100 % of packet receptions when the packet arrives with energy above ≈ -82 dBm. Packet Reception probability and Packet Drop probability are complementary and thus to preserve the readability of this work we only present the Packet Drop probability in the following analyses.

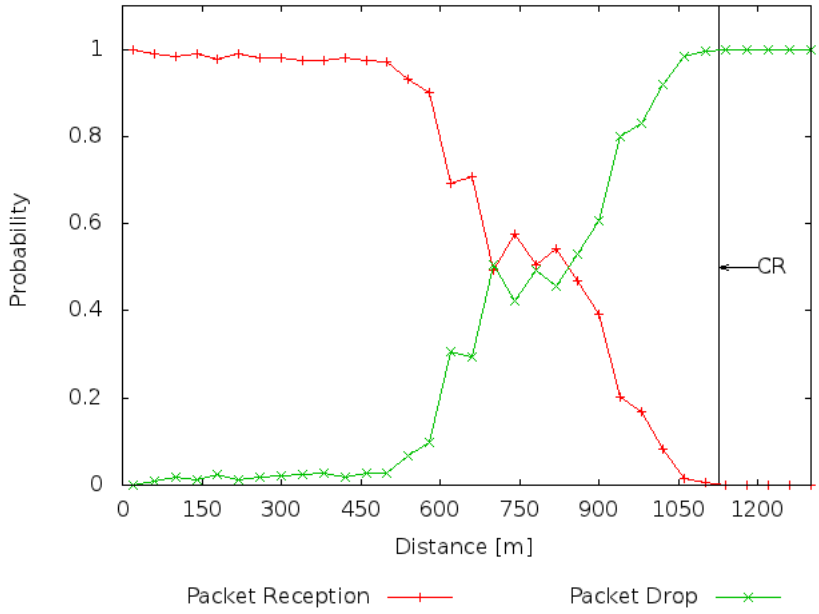


Figure 4.1: Packet Reception and Packet Drop probabilities with respect to distance between sender and receiver using a scenario with 20 nodes/km, transmission rate of 10 packets/s and packet size of 500 bytes. The transmission power of 20 dBm results in a CR of ≈ 1125 meters. The user offered load is ≈ 1.8 Mbps.

In Figure 4.1, it is clear the increase of the probability of packet drops for distances between sender and receiver greater than ≈ 550 meters. This increase is mainly due to hidden nodes and is explained with the help of Figure 4.2. Nodes A and C cannot sense each other, i.e., $Distance_{AB} + Distance_{BC} \geq 1125$ meters. Considering that node A and node C are ≈ 565 meters from node B, if their packets overlap in time at node B, there will be a collision and both packets will probably be dropped, since they arrive with similar energy; however, maintaining the same relation of distance ($Distance_{AB} + Distance_{BC} \geq 1125$) so that nodes are not able to perceive each other, if a node is closer, its packet have more chances to be received due to the SINR relation, while the packet from the more distant node is dropped. Thus, there is an increase in the probability of the packet drops only from ≈ 550 meters.

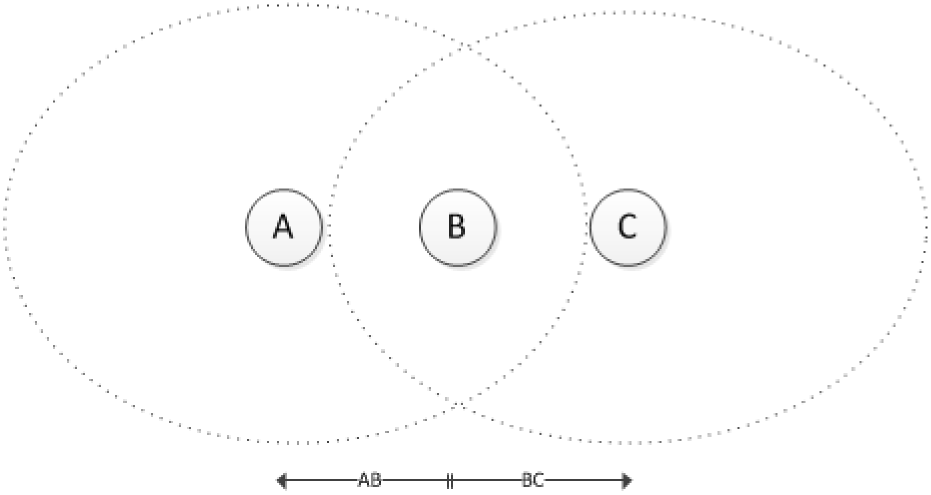


Figure 4.2: Increase of the probability of packet drops due to the hidden node problem.

Impact of the user offered load to the channel

The study of the impact of the variation of the user offered load to the channel is necessary to analyze the performance of VANETs. Variation of the user offered load to the channel can be achieved by varying the nodes inside the CR, the packet size and the transmission rate.

The number of nodes inside the CR has an impact in the user offered load to the channel because it directly affects the number of nodes present in the channel. The variation of the number of nodes inside the CR can be performed by varying the node density or by varying the transmission power.

Variation of the node density is illustrated in Figure 4.3. The scenario with 20 nodes/km has an user offered load of $\approx$ 1.1 Mbps, while the scenario with 60 nodes/km has an user offered load of $\approx$ 3.3 Mbps. The higher node density the higher probability of packet drops for every distance between sender and receiver, reaching a difference of 60 % in the packet drop probability relative to the lower node density for distances between 800 and 1000 meters, i.e., when the packet arrives with energy above ≈ -89 dBm and ≈ -92 dBm, respectively. An increase of node density increases the nodes competing for the access to the channel and the number of transmissions, and it also increases the number of bad receptions due to, for example, collisions introduced by hidden nodes. Furthermore, a significant increase of the node density can expose the limitations of the small and fixed contention window by introducing additional collisions due to transmissions in the same contention slot.

Figures 4.4a and 4.4b show the impact of varying the transmission power in scenarios with different user offered loads to the channel. The scenario with packet size of 300 bytes, transmission rate of 2 packets/s and transmission power of 10 dBm has an user offered load offered of $\approx$ 0.36 Mbps, while the scenario with transmission power of 20 dBm has an user offered load of $\approx$ 0.65 Mbps. The scenario packet size of 500 bytes, transmission rate of 6 packets/s and transmission power of 10 dBm has an user offered load of $\approx$ 1.8 Mbps, while the scenario with transmission

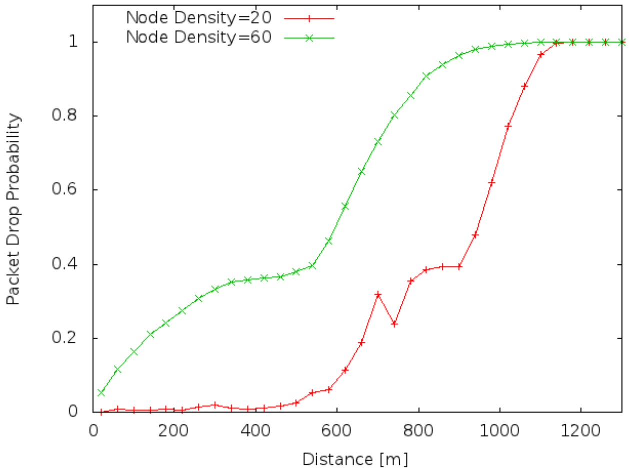
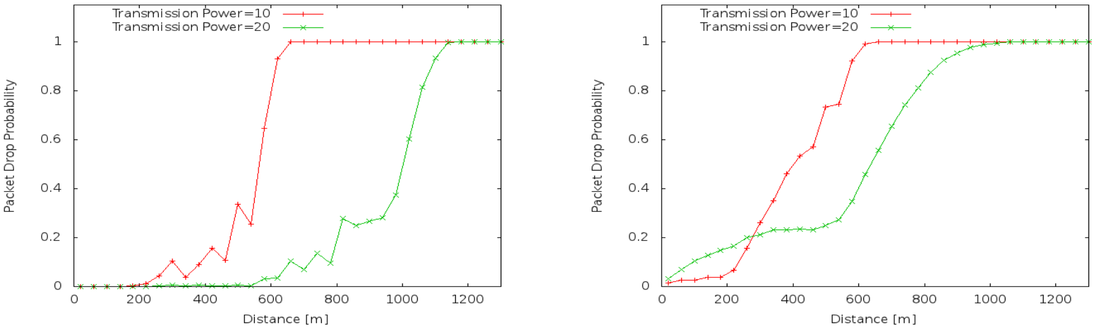


Figure 4.3: Impact of number of nodes inside the CR in Packet Drop probability. Variation of node density using a transmission rate of 10 packets/s, packet size of 300 bytes and a transmission power of 20 dBm.

power of 20 dBm has an user offered load of ≈ 3.3 Mbps. For scenarios with low user offered load to the channel, as Figure 4.4a illustrates, the scenario with 20 dBm of transmission power remains 'robust' against packet drops along half of the CR, while the scenario with 10 dBm only remains 'robust' for one third of the CR; however, for scenarios with a high user offered load to the channel, presented in Figure 4.4b, the robustness of the higher transmission power disappears, since the scenario with 20 dBm has almost 20 % of probability of packet drop in the first half of the CR, while the scenario with 10 dBm continues to have a low probability of packet drops for one third of the CR.

By varying the node density and the transmission power, it is possible to conclude that an increase of nodes inside the CR increases the probability of packet drop.



(a) With packet size of 300 bytes and transmission rate of 2 packets/s.

(b) With packet size of 500 bytes and transmission rate of 6 packets/s.

Figure 4.4: Impact of number of nodes inside the CR in Packet Drop probability. Variation of transmission power using scenarios with 60 nodes/km, transmission rate of 2 and 6 packets/s and packet size of 300 and 500 bytes, respectively.

A higher transmission rate means that more packets compete for the channel, increasing the rate of collisions due to the hidden node or due to transmissions in the same contention slot. Figure 4.5 illustrates the variation of transmission rate using scenarios with 60 nodes/km, transmission power of 20 dBm, packet size of 300 bytes and three different transmission rates. The scenario with transmission rate of 2 packets/s has an user offered load of ≈ 0.65 Mbps, the scenario with transmission rate of 6 packets/s has an user offered load of ≈ 2 Mbps and the scenario with transmission rate of 10 packets/s has an user offered load of ≈ 3.3 Mbps. The scenarios with 2 and 6 packets/s have a close, and also low, probability of packet drop for distances up to half of the CR (≈ 565 meters), after which the two scenarios start diverging and the effects of the difference of the user offered load to the channel become clear, i.e., the scenario with the transmission rate of 6 packets/s starts to perform worse than the scenario with 2 packets/s. The scenario with 10 packets/s clearly performs worse than the other two, for every distance between sender and receiver.

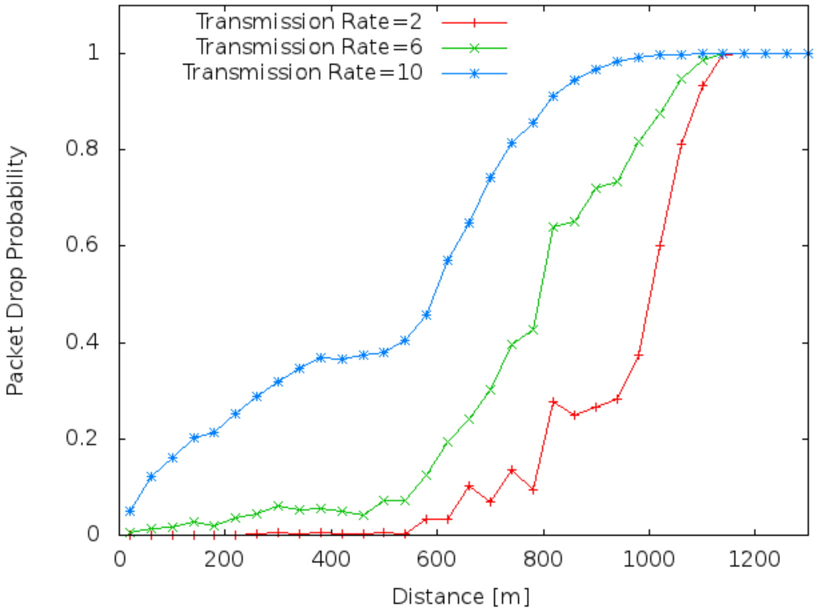


Figure 4.5: Impact of number of nodes inside the CR in Packet Drop probability. Variation of transmission rate using scenarios with 60 nodes/km, transmission power of 20 dBm and packet size of 300 bytes.

Figure 4.6 exhibits the impact of packet size variation in the system's performance. The scenario with packet size of 100 bytes has an user offered load of ≈ 1.1 Mbps, the scenario with packet size of 300 bytes has an user offered load of ≈ 3.3 Mbps and the scenario with packet size of 500 bytes has an user offered load of ≈ 5.5 Mbps. It is possible to conclude that larger packet sizes have higher probability of be dropped. An increase of packet size increases the number of bits that can be unsuccessfully decoded, which increases with the distance between sender and receiver, since the signals arrive weaker at the receiver and are more prone to have errors. Moreover, with the increase of packet size, the receivers stay more time in RX state and therefore are more vulnerable to collisions due to the hidden node problem.

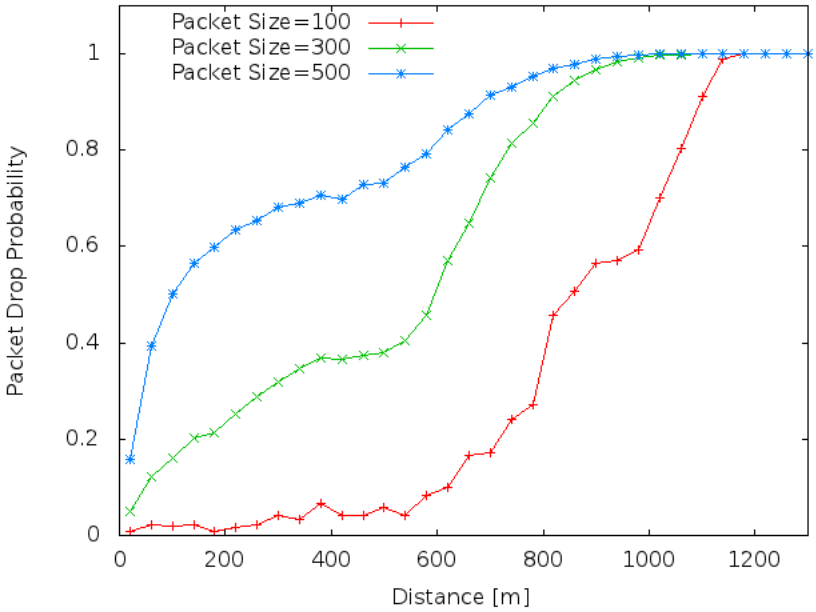


Figure 4.6: Impact of packet size in Packet Drop probability. Variation of packet size using scenarios with 60 nodes/km, transmission rate of 10 packets/s and transmission power of 20 dBm.

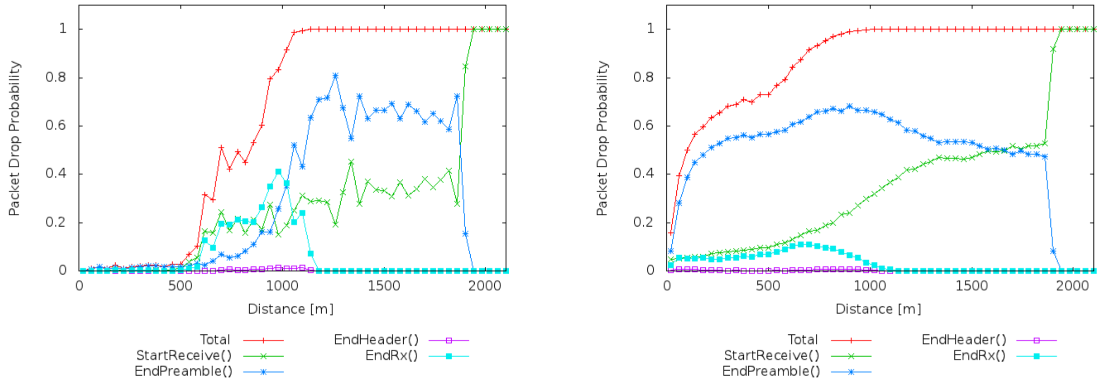
As expected, we show that the user offered load to the channel has a significant impact in the probability of packet reception/drop.

4.1.2 Characterization of packet drops

The probability of packet drop can be characterized for each of the 4 events defined in Section 2.4.2.5 and is illustrated in Figures 4.7a and 4.7b. Figure 4.7a represents a scenario with 20 nodes/km, transmission power of 20 dBm, transmission rate of 10 packets/s and packet size of 500 bytes, which results in an user offered load of ≈ 1.6 Mbps, while Figure 4.7b represents a scenario with 60 nodes/km, transmission power of 20 dBm, transmission rate of 10 packets/s and packet size of 500 bytes, which results in an user offered load of ≈ 5.4 Mbps. Since both have a transmission power of 20 dBm, both have a CR of 1125 meters.

For a low user offered load scenario (see Figure 4.7a) it is possible to highlight four main intervals of the packet drop probability relative to the distance between sender and receiver. The first one is approximately between [0–550] meters, where there are almost no packet drop; the second one is approximately between [550–1125] meters, where packets drops start to increase for StartReceive(), EndPreamble() and EndRx(), and the combined probability of packet drop increases linearly until it reaches 100 %; the third one is approximately between [1125–1900] meters, where packets are dropped mainly in EndPreamble() because the packets have sufficient energy to be sensed, but have insufficient energy to be successfully decoded; the fourth one is for distances longer than 1900 meters, where there are only packet drops in StartReceive(), since packets arrive with energy lower than -104 dBm and therefore are lower than thermal noise.

Figure 4.7b illustrates the probability of packet drop in each of the four events for a high user offered load scenario, using 60 nodes/km. Having higher node density, there are more transmissions, receptions and the user offered load is higher. Inside the CR, the majority of the packet drops happens in EndPreamble(). Even for the first half of the CR, packet drops in EndPreamble() achieve 60 % because of the degrading effect of collisions. When compared with the low user offered load scenario, the probability of packet drop in EndRx() decreases in terms of maximum value, however, it occurs along the entire CR.



(a) With 20 nodes/km.

(b) With 60 nodes/km.

Figure 4.7: Packet Drop probability with respect to distance between sender and receiver for the four reception events. Figure (a) represents a scenario with 20 nodes/km and Figure (b) represent a scenario with 60 nodes/km.

The causes of packet drops in each event are presented next. Excluding differences of magnitude or distribution along the distances between sender and receiver, the causes of packet drops in a low user offered load scenario are the same as in a high user offered load scenario and therefore we only present the first.

Considering the scenario with 20 dBm of transmission power illustrated in Figure 4.8, the probability of packet drop in StartReceive() event is significant, when the distance between sender and receiver is greater than ≈ 500 meters. From this distance and up to ≈ 1900 meters, the packet drops are mainly due to the receiver being in RX State, when the packet arrived. The probability of packet drop in StartReceive() event is 100 %, when the distance between sender and receiver is higher than ≈ 1900 meters. In the figure, it is visible that there are also packet drops due to the receiver being in the TX state at the moment of the arrival of the packet, but the amount is below 5 % and it is for distances far than the CR distance. For StartReceive() event there are no packet drops due to the receiver being in the SYNC State, when the packet arrived.

The main cause of packet drops in EndPreamble() is due to Processing (see Figure 4.9). Although all packets arriving with energy greater than -104 dBm have scheduled an EndPreamble() event, the ones that do not arrive with energy higher than -95 dBm are dropped in EndPreamble, because they do not have sufficient energy to be decoded. Furthermore, even if they arrive with energy higher than −95 dBm, interference from other packets can cause packet drops. In EndPreamble(), there is a very small percentage of packets arriving when the receivers are already in RX State, but have a SINR below the capture threshold and therefore cannot be decoded.

Packet drops in EndHeader() event (Figure 4.10) can be considered insignificant, nevertheless the small number is caused by Processing.

Packet drops in EndRx() event happen due to Processing and Capture Effect (see Figure 4.11). There are no packet drops in EndRx() for distances between sender and receiver longer than the CR due to the fact that all packets are dropped previoulsy in EndPreamble().

Packet drops due to the receiver being in the RX or SYNC State, due to Processing or Capture Effect can be reduced to one cause: due to Packet Collisions.

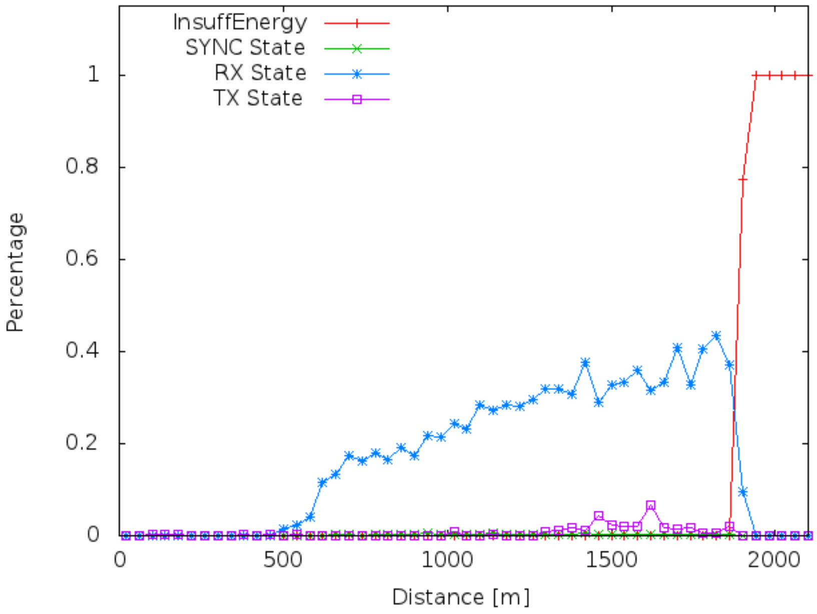


Figure 4.8: Percentage of dropped packets in StartReceive() separated according to causes of drop. Scenario with 20 nodes/km, transmission rate of 10 packets/s and packet size of 500 bytes. The user offered load is ≈ 1.6 Mbps.

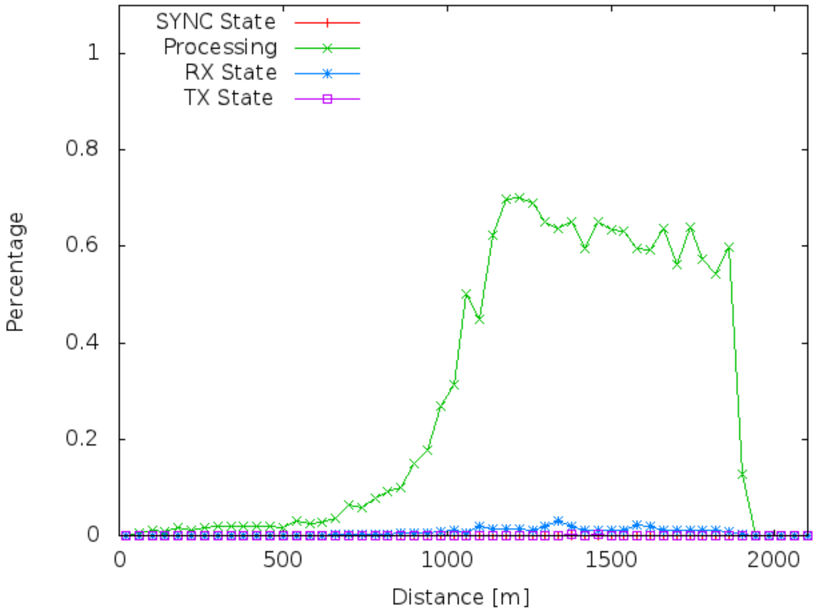


Figure 4.9: Percentage of dropped packets in EndPreamble() separated according to causes of drop. Scenario with 20 nodes/km, transmission rate of 10 packets/s and packet size of 500 bytes. The user offered load is ≈ 1.6 Mbps.

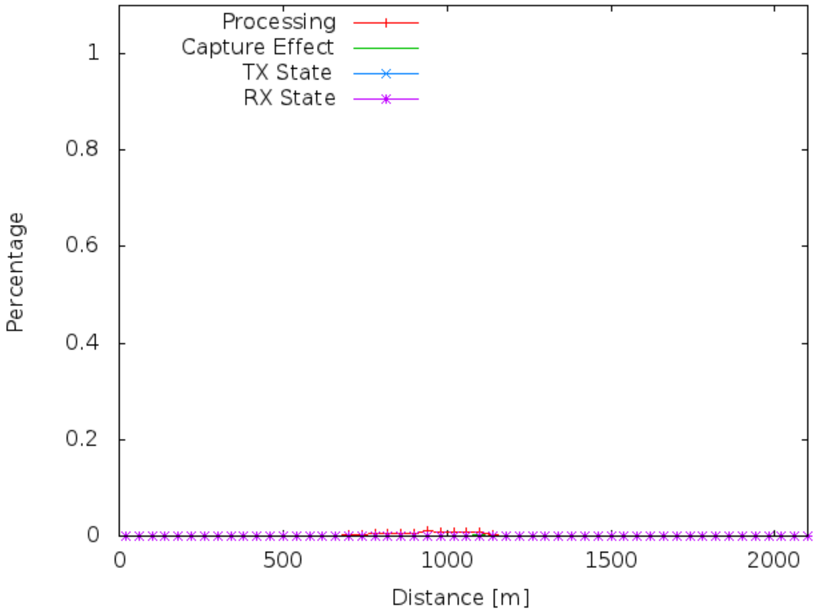


Figure 4.10: Percentage of dropped packets in EndHeader() separated according to causes of drop. Scenario with 20 nodes/km, transmission rate of 10 packets/s and packet size of 500 bytes. The user offered load is ≈ 1.6 Mbps.

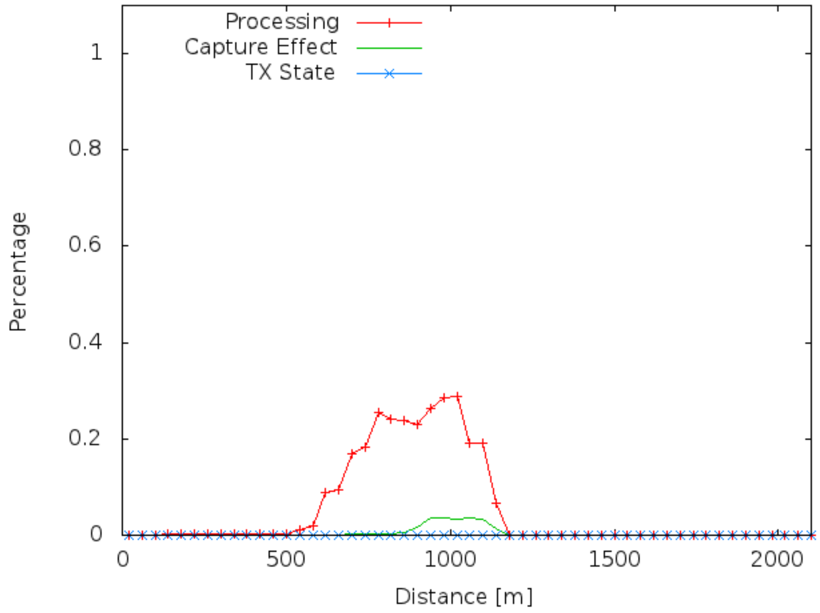


Figure 4.11: Percentage of dropped packets in EndRx() separated according to causes of drop. Scenario with 20 nodes/km, transmission rate of 10 packets/s and packet size of 500 bytes. The luser offered load is ≈ 1.6 Mbps.

4.1.3 Characterization of Packet Collisions

Packet Collisions are the main causes of packet drops when the receivers are in the communication range of the senders. Therefore, in this subsection we characterize packet collisions in order to understand the severity of the interferences and the complexity of a possible SIC implementation.

4.1.3.1 Probability that packet can be involved in a collision

Collisions have a degrading effect in the performance of communications. An error in a single bit can lead to the drop of the whole packet and therefore, for this metric, we assume that collisions happen when two or more packets, arriving with energy equal or higher than -104 dBm, overlap in time at a receiver. Considering all packets arriving with energy above thermal noise provides a first insight in the characterization of packet collisions.

Figure 4.12 helps to shortly illustrate how we estimate this probability. The figure represents packets arriving to a node during a period of time. Only the packets arriving with energy equal or higher than -104 dBm are considered, therefore, Packet 3 is not considered and Packet 4 counts as a packet arriving alone. Packet 1 and Packet 2 collide and hence count as collisions. In this case, the percentage of packets involved in a collision is $\frac{2}{3}$, since there are 3 packets arriving with energy equal or higher than -104 dBm and 2 of them collide.

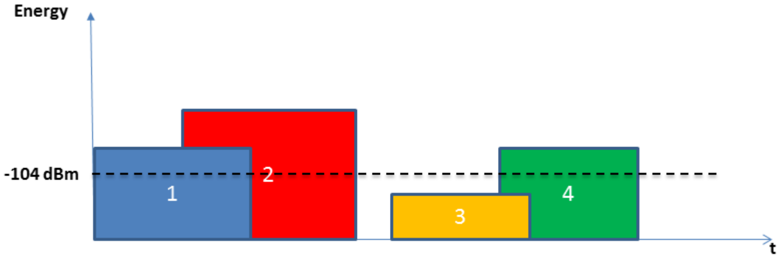
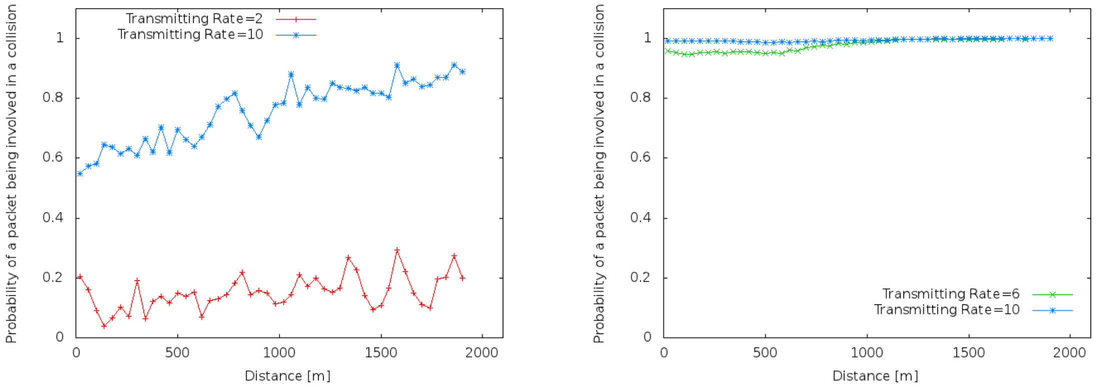


Figure 4.12: Calculation of the Probability that packet can be involved in collision.

Figure 4.13a and Figure 4.13b illustrate the probability of a packet being involved in a collision with respect to the distance between sender and receiver for different transmission rates. Figure 4.13a represents two scenarios with low node density, nevertheless, the variation of transmission rate shows that, even for such scenarios, an increase of user offered load increases the probability of a packet colliding with others. While the scenario with 2 packets/s of transmission rate remains with 20 % of probability of collision along the CR, the packets from the scenario with 10 packets/s of transmission rate suffer from 60 % to 80 % on the probability of collision inside the CR.

Figure 4.13b shows two scenarios with high node density. The impact of the variation of transmission rate in the probability of a packet being involved in a collision for those scenarios is very small, since the high user offered load to the channel causes almost 100 % of probability of a packet being involved in a collision.

This metric permits us to conclude the number of packets involved in collisions directly depends on the user offered load to the channel, and the higher the user offered load is, the more likely will be for a packet being involved in a collision.



(a) With 20 nodes/km.

(b) With 60 nodes/km.

Figure 4.13: Probability of a packet being involved in a collision in scenarios with high and low node density. Variation of beacon rate using 20 nodes/km and 60 nodes/km, transmission power of 20 dBm and packet size of 500 bytes.

4.1.3.2 Energy distribution of colliding packets

The Energy distribution of the colliding packets permits to understand the severeness of the packet collisions and provides a visual explanation of the causes of packet collisions. Table 4.2 exemplifies the calculation of the energy distribution, when each of the packets involved in a collision has only one packet colliding with it. Take the packets transmitted at 50 meters from the receiver as an example. There were two packets that suffered a collision from a packet with −55 dBm of energy and there was one packet that suffered a collision from a packet with −85 dBm of energy, which resulted in a ratio of 0.66(6) and 0.33(3), respectively.

Distance (m)	Energy of the colliding packet (dBm)	Number of occurrences	Ratio
50	−55	2	0.66(6)
	−85	1	0.33(3)
200	−55	1	0.25
	−70	2	0.5
	−80	1	0.25

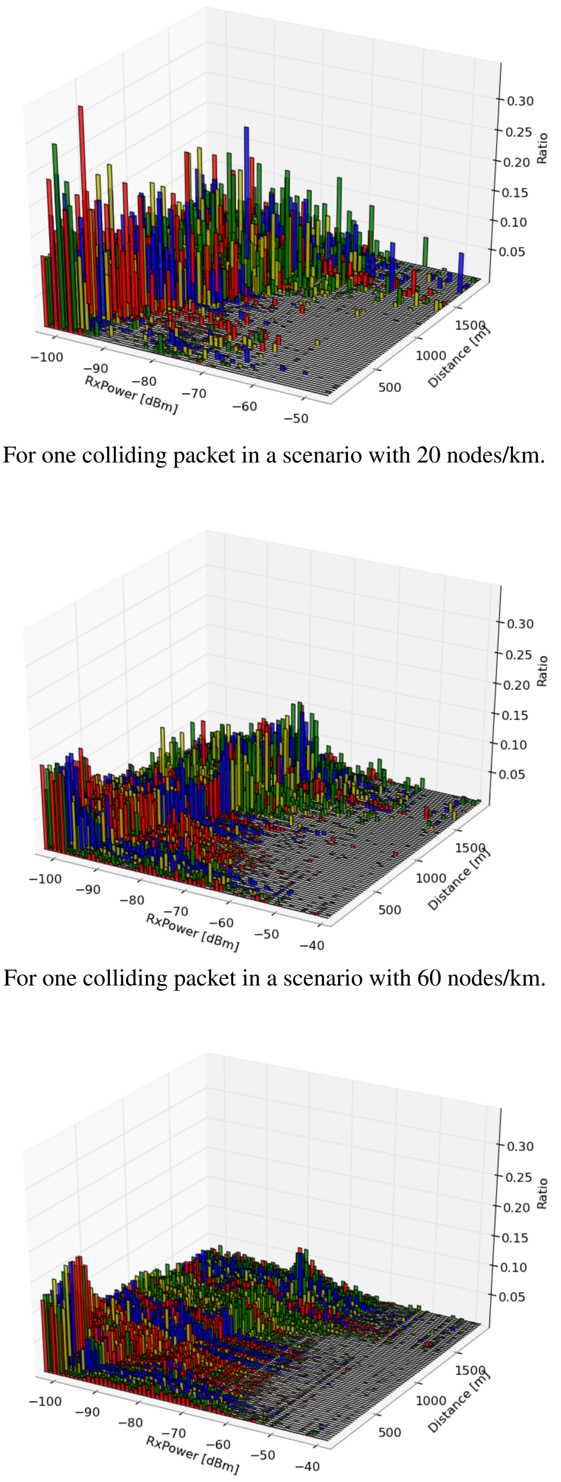
Table 4.2: Calculation of the Energy distribution of colliding packets.

Figure 4.14a and Figure 4.14b illustrate the energy distribution of the colliding packets with respect to the distance between sender and receiver of the packets that suffered collisions with only one packet. Figure 4.14a represents a scenario with 20 nodes/km, transmission rate of 10 packets/s, transmission power of 20 dBm and packet size of 500 bytes, which results in an user offered load of 1.8 Mbps. Generally, as packets arrive from farther distances, the packet that collides with them becomes stronger, therefore, the interference becomes more severe. This is due to the hidden node problem and can be explained, once more, by Figure 4.2. Excluding transmissions in the same contention slot, a sender very close to the receiver suffers only collisions from packets arriving with energy below ≈ -95 dBm, in other words, from packets further than the CR/CSR of both. The packets arriving with energy below -95 dBm cannot be successfully decoded; however, they interfere with other packets and can cause their drop.

In packet collisions, SIC only works when a packet has SINR sufficient to be decoded and cancelled in every iteration, in order to decode the rest of the packets; hence SIC performs better when packets arrive with considerably different energies.

The transmissions in the same contention slot are particularly visible in Figure 4.14b. The figure also represents the energy distribution for a single colliding packet, but using a scenario with 60 nodes/km, transmission rate of 10 packets/s, transmission power of 20 dBm and packet size of 500 bytes, which results in an user offered load of 5.4 Mbps. The collisions of strong packets with other packets transmitted at short distances between sender and receiver result from transmissions in the same contention slot. For instance, the colliding packets arriving with -70 or -80 dBm of energy means that the interfering sender is approximately between 125 and 400 meters. Then, in the worst case, the interfering sender could sense transmissions from nodes at approximately 725 meters from the receiver in the opposite direction; however, as the figure shows, these packets collide even with packets from senders at the close surrounding of the receiver. If two packets arrive with similar energy, then none of them have SINR sufficient to be decoded and therefore both will be dropped and SIC is not able to bring improvements to the packet reception.

Figure 4.14c illustrates the same scenario as Figure 4.14b, but for the case where each of the packets involved in a collision has two packets colliding with it. The figure shows that the energies of the colliding packets become more distributed. Furthermore, the energy of the colliding packets increases for every distance between receiver and the sender of the interfered packet, reaching almost -50 dBm. Therefore, the increase of the number of colliding packets increases the severeness of the interference.



(a) For one colliding packet in a scenario with 20 nodes/km.

(b) For one colliding packet in a scenario with 60 nodes/km.

(c) For two colliding packets in a scenario with 60 nodes/km.

Figure 4.14: Energy distribution of colliding packets in scenarios with high and low node density. Using transmission rate of 10 packets/s, transmission power of 20 dBm and packet size of 500 bytes.

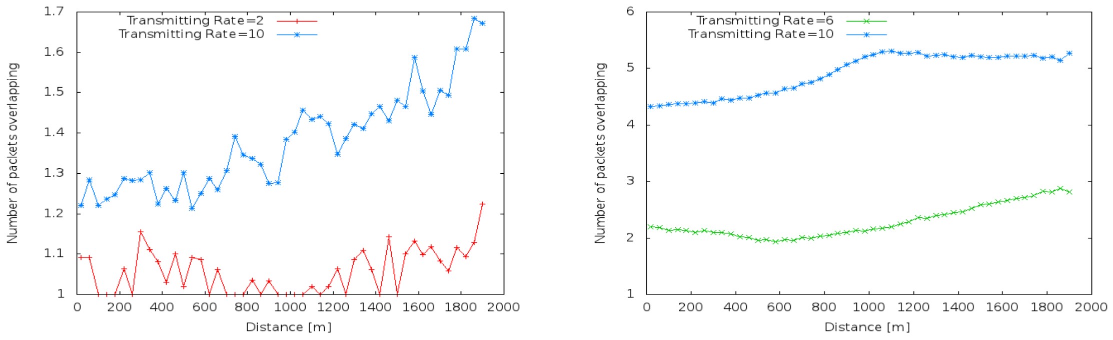
4.1.3.3 Number of packets overlapping

This metric is implemented to evaluate the number of packets overlapping with each packet involved in collisions. For this metric the packets have to arrive with energy equal or higher than -95 dBm, to be taken into account as colliding packet. This way, it is possible to understand, for each packet involved in a collision, how many of the other packets involved in that collision could be considered for possible recovery through SIC.

Figure 4.15a and Figure 4.15b illustrate the average number of packets overlapping with each packet involved in a collision, for scenarios with different node density and with variation of transmission rates. When comparing the scenarios by node density, we can conclude that the average number of packets overlapping is lower for the lower node density, ranging from 1 to 1.7 interferers, depending on the transmission rate (i.e., the user offered load to the channel), whereas the scenarios with high node density have in average 2 to 5 interferers.

Figure 4.16 and Figure 4.17 present the histograms of two scenarios with different node densities. Once again, by varying the node density, we are representing the effects of the variation of the user offered load. The scenario with 60 nodes/km has almost three times more the number of overlapping packets for each packet than the scenario with 20 nodes/km. The scenario with 20 nodes/km has a maximum of mainly 3 interferers, but 90 % of the total overlaps, with respect to distance between sender and receiver, occur with 1 or 2 interferers, while the scenario with 60 nodes/km has approximately 10 interferers (11 interferers and onward are negligible) and the percentage of the total overlaps is divided among them.

If we decided to implement a 2-stage SIC receiver (i.e., a receiver able to cancel the captured packet, then recover a second packet and cancel it, and finally recover a third packet), we could recover almost 90 % of the overlapping packets in the scenario with low density; however, to recover the same percentage in the scenario with high node density, it would be necessary, approximately, a 8-stage SIC receiver. Therefore, the advantages that can be obtained from a SIC implementation with a certain number of stages varies with user offered load to the channel.



(a) With 20 nodes/km.

(b) With 60 nodes/km.

Figure 4.15: Average number of packets overlapping with each packet in scenarios with high and low node density. Variation of transmission rate using scenarios with 20 and 60 nodes/km, transmission power of 20 dBm and packet size of 500 bytes.

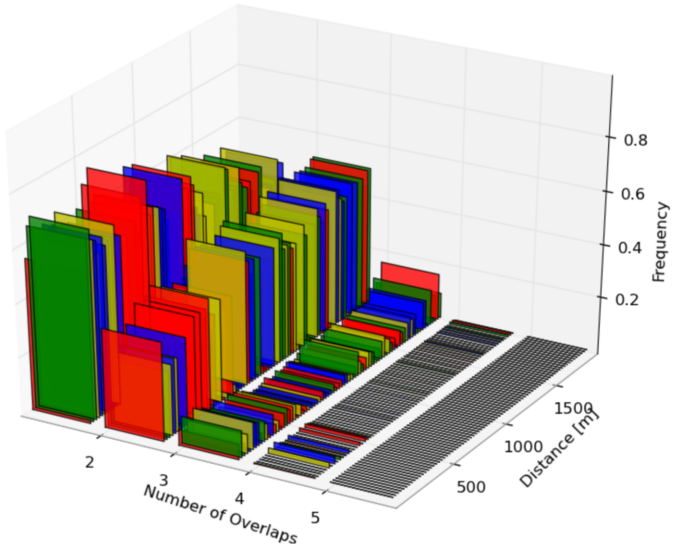


Figure 4.16: Histogram of number of packets overlapping with each packet in a scenario with low node density. Using a scenario with 20 nodes/km, transmission rate of 10 packets/s, transmission power of 20 dBm and packet size of 500 bytes.

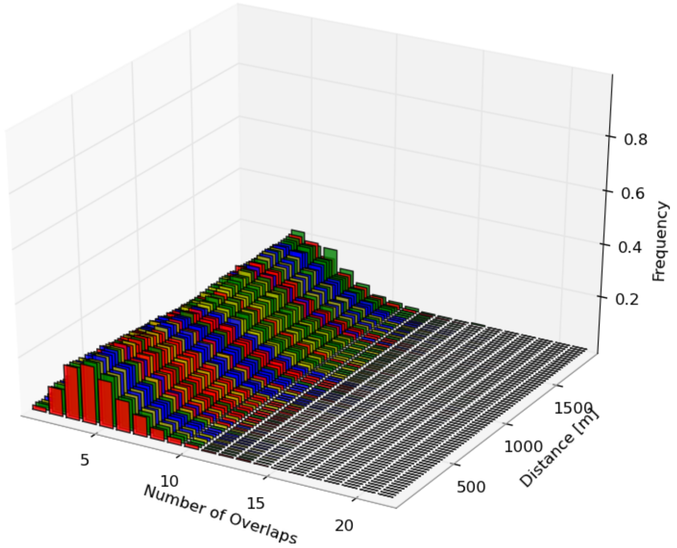


Figure 4.17: Histogram of number of packets overlapping with each packet in a scenario with high node density. Using a scenario with 60 nodes/km, transmission rate of 10 packets/s, transmission power of 20 dBm and packet size of 500 bytes.

4.1.4 Probability of Recovery through SIC

Probability of Recovery through SIC represents the percentage of packets, with respect to distance between sender and receiver, that could be recovered from collisions if receivers performed a perfect SIC implementation. If during a simulation 100 packets arrive to the nodes and 20 of these ones are dropped, but 5 of them can be recovered through our SIC implementation, then there are 5 % of packets that could be recovered. The 5 % are the throughput gains introduced by interference cancellation in this specific example. We assume the receivers perform perfect decoding and reconstruction of the captured packets, and then they are able to perfectly cancel the interferences of the captured packets from the rest of the signals. With this optimistic analysis we obtain the upper-bound for the benefits of a 1-stage SIC implementation for every packet, i.e., we assess the probability of recovery of every packet that collided with a captured packet, considering the latter is perfectly decoded and cancelled from the combined signals.

Figure 4.18 presents the Probability of Recovery through SIC for several scenarios with 20 nodes/km. The relatively low density implies low user offered load to the channel. We use 4 different scenarios in which the user offered load varies from 0.36 Mbps to 1.8 Mbps. For the initial 800 meters of distance between sender and receiver (put differently, for packets arriving with energy above ≈ -89 dBm), the SIC implementation can merely bring 1 % of additional recovered packets. However, from 800 meters up to the communication range ($\approx$1125 meters) the implementation achieves almost 20 % of packet recovery for the scenario with the user offered load of 1.1 Mbps. Nevertheless, the throughput gains introduced by the SIC implementation only become visible for the scenario with user offered load of 0.65 Mbps and onward. The better performance of SIC with the increase of the user offered load might seem counterintuitive, however, it is necessary to consider that the system needs to have packet collisions in order to SIC bring any kind of advantages. If there are no packet drops, not even from packet collision, there cannot be any throughput gain from recovery through SIC. Even the scenario with 1.1 Mbps has a very low probability of packet drops for the initial 800 meters (see Figure 4.7a) and therefore SIC is unnecessary for these distances.

The increase of node density increases the user offered load to the channel, which by itself increases the number of packet collisions and packet drops. Figure 4.19 illustrates the Probability of Recovery through SIC for scenarios with 60 nodes/km. Since there are more packet drops due to packet collisions, the SIC implementation can provide more gains to the packet reception probability. In general, the SIC implementation brings more gains to the scenarios with the user offered load of 3.3 Mbps than to the others. The scenario exhibit 5 % to 10 % of recovered packets almost along the entire communication range. On the one hand, for close distances, the scenarios with lower user offered load have higher packet reception probability and, therefore, have less packet drops and packet collisions, which means SIC cannot bring the same benefits. They are comparable to the scenarios presented in the previous figure. On the other hand, as shown in the previous subsection, the packets in the scenario with higher user offered load (5.4 Mbps) suffer more interferences, since they have more packets colliding with them. Although SIC perfectly cancels the captured packet, the high number of interfering packets lowers the probability of a packet to be recovered.

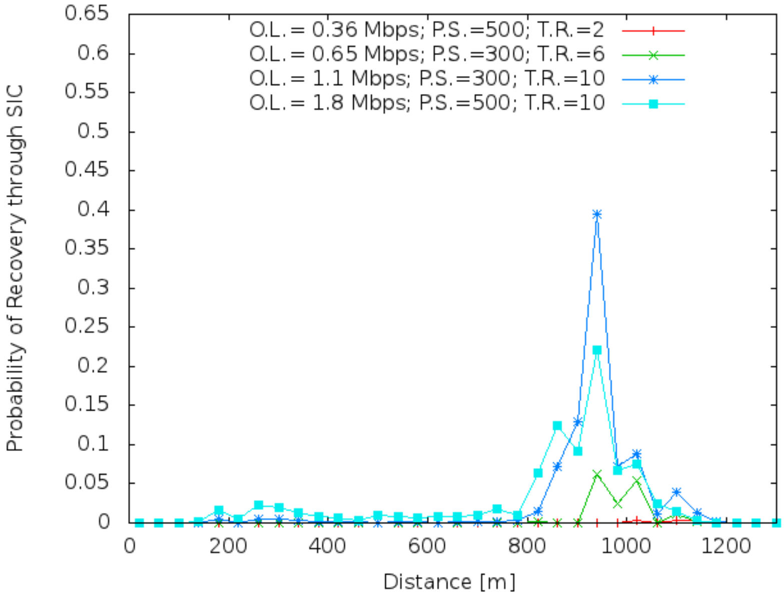


Figure 4.18: Probability of Recovery through SIC for different scenarios using a node density of 20 nodes/km and transmission power of 20 dBm. Variation of the user offered load (O.L.) by varying packet sizes (P.S.) and transmission rates (T.R.).

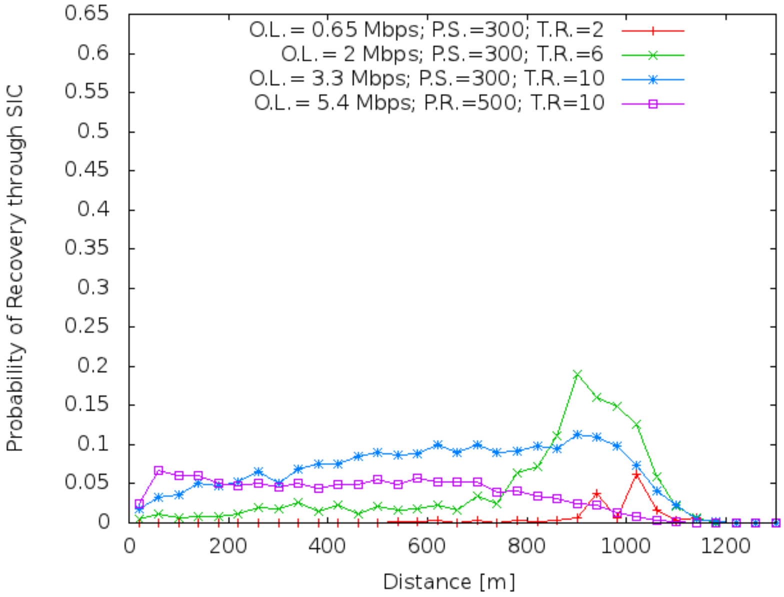


Figure 4.19: Probability of Recovery through SIC for different scenarios using a node density of 60 nodes/km and transmission power of 20 dBm. Variation of the user offered load (O.L.) by varying packet sizes (P.S.) and transmission rates (T.R.).

Chapter 5

Conclusions and Future Work

This chapter firstly provides an overview of the main contributions of this work and the conclusions drawn. And finally, presents guidelines for future work.

5.1 Contributions

The main contributions of this work are the following:

- Exhaustive characterization of the frame reception of VANETs in *PhySim-WiFi*;
- Identification of packet drop causes and their relevance in the Packet Drop Probability;
- Definition of metrics to evaluate VANETs' performance and causes of packet drop;
- Implementation of the metrics in NS-3 with *PhySim-WiFi*;
- Analysis of the impact of the user offered load in the Packet Drop Probability and packet collisions;
- Detailed characterization of packet collisions:
  - Probability that packet can be involved in a collision;
  - Energy distribution of colliding packets;
  - Number of packets overlapping;
- Evaluation of throughput gains with SIC.

5.2 Conclusions

With the simulations, we confirmed that the increase of user offered load to the channel has a degrading effect in the communication's performance, since the probability of packet drop increases for the increase of node density, packet size, transmission power and transmission rate (Figures 4.3, 4.4, 4.5, and 4.6).

As expected, the main cause of packet drops inside the communication range is packet collisions. The amount of collisions depends on the user offered load to the channel and, for instance, scenarios with high user offered load the percentage of packets that suffer collisions can reach 100 % (Figure 4.13). The energy distribution of the colliding packets allowed us to understand the severeness of packet collisions and the energy relationship between sender and interferer; moreover it allowed visualizing the causes of packet collisions, namely due to the hidden node problem and transmissions in the same contention slot. For scenarios with higher user offered load to the channel there is a general increase of the energy of the colliding packets and it becomes more distributed with respect to the distance of between sender and receiver of the interfered packet (Figure 4.14). Regarding the number of packets overlapping with each packet involved in a collision, once again, we concluded that higher user offered load to the channel increases the number of packets interfering in each collision. For scenarios with high user offered load to the channel, e.g. 5.5 Mbps, if we wanted to recover approximately 90 % of the packets involved in collisions, we required a SIC receiver able to iteratively decode and cancel the interference of 8 packets (Figure 4.17).

According to our assessment, the probability of packet reception can be increased by 5 to 20 % for packets sent in the entire communication range of the receiver, for scenarios where the user offered load to the channel is approximately 3.3 Mbps, and achieves the maximum of 40 % of packet recovery, for scenarios with approximately 1.1 Mbps.

5.3 Future work

This work was the first step in a detailed characterization of packet collisions and the assessment of the benefits and feasibility of interference cancellation in VANETs. The use of probabilistic channel models with fading of the signals and the use of node's mobility leave open opportunities to extend our characterization of packet collisions, since they will introduce additional packet collisions. Furthermore, the implementation of SIC similar to [3] or [4] implementations, which are able to decode the strongest packet in each iteration, cancel it from the combined signals and proceed with the decoding (if any) of the rest of the packets, can significantly improve the gains in the recovery of dropped packets.

Now that we know that we can recover from packet collisions, it could be worth studying whether it is helpful to adjust the MAC layer in such a way that it allows for collisions that can be recovered with high probability. As a result, the MAC layer could be tuned to exploit the SIC capability and thus increase the network capacity.

References

[1] Arialdi M. Miniño, Jiaquan Xu, and Kenneth D. Kochanek. Deaths: Preliminary Data for 2008. In *National Vital Statistics Reports, Volume 59, Number 2*, December 2010.

[2] A. J. Viterbi. Very Low Rate Convolutional Codes for Maximum Theoretical Performance of Spread-Spectrum Multiple-Access Channels. *IEEE Journal on Sel. Areas in Communications*, 8:641–649, May 1990.

[3] Daniel Halperin, Thomas Anderson, and David Wetherall. Taking the Sting Out of Carrier Sense: Interference Cancellation for Wireless LANs. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, MobiCom '08, pages 339–350, New York, NY, USA, 2008. ACM.

[4] Kun Tan, He Liu, Ji Fang, Wei Wang, Jiansong Zhang, Mi Chen, and Geoffrey M. Voelker. SAM: Enabling Practical Spatial Multiple Access in Wireless LAN. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, MobiCom '09, pages 49–60. ACM, 2009.

[5] A. Duel-Hallen, J.Holtzman, and Z. Zvonar. Multiuser Detection for CDMA Systems. *Personal Communications, IEEE*, 2:46–58, April 1995.

[6] Jens Mittag, Stylianos Papanastasiou, Hannes Hartenstein, and Erik G. Ström. Enabling Accurate Cross-Layer PHY/MAC/NET Simulation Studies of Vehicular Communication Networks. *Proceedings of the IEEE*, PP(99):1–16, July 2011.

[7] Marc Torrent-Moreno, Steven Corroy, Felix Schmidt-Eisenlohr, and Hannes Hartenstein. IEEE 802.11-Based One-Hop Broadcast Communications: Understanding Transmission Success and Failure under Different Radio Propagation Environments. *Proceedings of the 9th ACM international symposium on Modeling analysis and simulation of wireless and mobile systems, MSWiM '06*, pages 68–77, 2006.

[8] Jens Mittag and Stylianos Papanastasiou. *PhySim-WiFi Manual 1.0*, September 2010.

[9] ETSI. European Telecommunications Standards Institute, News Release, September 2008.

[10] Rohde & Schwarz GmbH & Co. KG. WLAN 802.11p Measurements for Vehicle-to-Vehicle (V2V) DSRC, 2009.

[11] B. S. Gukhool and S. Cherkaoui. IEEE 802.11p modeling in NS-2. In *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*, pages 622–626, October 2008.

[12] Lothar Stibor, Yunpeng Zang, and Hans-Jürgen Reumerman. Evaluation of Communication Distance of Broadcast Messages in a Vehicular Ad-Hoc Network Using IEEE 802.11p. In *Wireless Communications and Networking Conference*, pages 254 – 257, March 2007.

[13] D. Jiang and L. Delgrossi. IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments. In *IEEE, In Vehicular Technology Conference*, pages 2036–2040, May 2008.

[14] Pranav Kumar Singh, Kapang Lego, and Dr. Themrichon Tuithung. Simulation based Analysis of Adhoc Routing Protocol in Urban and Highway Scenario of VANET. In *International Journal of Computer Applications*, volume 12, pages 42–49, January 2011.

[15] Arijit Khan, Shatrugna Sadhu, and Muralikrishna Yeleswarapu. A Comparative Analysis of DSRC and 802.11p over Vehicular Ad hoc Networks, May 2009.

[16] ASTM International. *ASTM E2213-03: Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Wireless Acess in Vehicular Environments WAVE/Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2003.

[17] TechnoCom. The WAVE Communications Stack: IEEE 802.11p, 1609.4 and 1609.3, September 2007.

[18] L. Hanzo, W. Webb, and T. Keller. Single and Multi-carrier Quadrature Amplitude Modulation. In *Wiley-IEEE Press*, April 2000.

[19] Lajos L. Hanzo, M. Münster, B. J. Choi, and Thomas Keller. OFDM and MC-CDMA for Broadband Multi-User Communications, WLANs and Broadcasting. In *Wiley-IEEE Press*, July 2003.

[20] IEEE Computer Society. *IEEE 802.11-2007, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, June 2007.

[21] Laura Bernadó, Nicolai Czink, Thomas Zemen, and Pavle Belanovic. Physical Layer Simulation Results for IEEE 802.11p using Vehicular non-Stationary Channel Model, May 2010.

[22] J. Maurer, T. Fügen, and W. Wiesbeck. Physical Layer Simulations of IEEE802.11a for Vehicule-to-Vehicule Communications. In *Proceedings of the 62nd IEEE Vehicular Technology Conference*, pages 1849–1853, September 2005.

[23] Andrea Goldsmith. *Wireless Communications*. Cambridge University Press, 2005.

[24] IEEE Computer Society. *IEEE Std. 802.11a-1999 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications High-speed Physical Layer in the 5 GHz Band*, 1999.

[25] Stefan Mangold, Sunghyun Cho, Peter May, Ole Klein, Guido Hiertz, and Lothar Stibor. IEEE 802.11e Wireless LAN for Quality of Service, 2001.

[26] W. Fisher. Development of DSRC–WAVE Standards. *IEEE 802.11-07/2045r0*, June 2007.

[27] Yi Wang, Akram Ahmed, Bhaskar Krishnamachari, and Psounis Konstantinos. IEEE 802.11p Performance Evaluation and Protocol Enhancement. *2008 IEEE International Conference on Vehicular Electronics and Safety*, pages 254–259, 2008.

[28] Won Gi Jeon, Kyung Hi Chang, and Yong Soo Cho. An Equalization Technique for Orthogonal Frequency-Division Multiplexing Systems in Time-Variant Multipath Channels. *IEEE Transactions on Communications*, pages 27–32, January 1999.

[29] Phil Karn. MACA - A New Channel Access Method for Packet Radio. *ARRL 9th Computer Networking Conference*, September 1990.

[30] R. K. Schmidt, T. Köllmer, T. Leinmüler, B. Böddeker, and G. Schäfer. Degradation of Transmission Range in VANETs caused by Interference. In *PIK - Praxis der Informationsverarbeitung und Kommunikation. Volume 32, Issue 4*, pages 224–234, October 2009.

[31] The NS-3 network simulator. http://www.nsnam.org, 2011. [Online; accessed July 18th, 2011].

[32] The IT++ library. http://www.nsnam.org, 2011. [Online; accessed July 18th, 2011].