$N^\circ$ **42507**

UNIVERSITÉ DE LILLE 1 SCIENCES ET TECHNOLOGIES

École Doctorale Sciences Pour l'Ingénieur

**THÈSE**

pour obtenir le grade de
Docteur de l'Université Lille 1: sciences et technologies

**Spécialité: Micro et Nanotechnologies, Acoustique et Télécommunications**
préparée à l'Institut d'Electronique de Microélectronique et de Nanotechnologie

présentée et soutenue publiquement le 13 décembre 2017 par:

**Grecia ROMERO**

# Identification of the impact mechanisms of the electromagnetic interferences on the Wi-Fi communications

**Membres du jury**

| | |
|---|---|
| Rapporteurs: | |
| Pr. **Daniel ROVIRAS** | CNAM Paris |
| Dr. **Guillaume FERRE** | Université de Bordeaux |
| Examinateurs: | |
| Pr. **Maryline HELARD** | Université de Rennes |
| Pr. **Charly POULLIAT** | Université de Toulouse |
| Invitée: | |
| Dr. **Gemma MORRAL** | SNCF |
| Directeur de thèse: | |
| Pr. **Eric SIMON** | Université de Lille |
| Encadrante: | |
| Dr. **Virginie DENIAU** | IFSTTAR Villeneuve D'Ascq |

# Acknowledgment

I thank all who in one way or another contributed to the completion of this thesis. First, I thank God for giving me courage, strength and confidence to achieve this goal.

I would like to express my sincere gratitude to my advisor Dr. Virginie DENIAU, for her support of my Ph.D study and related research, for her patience, motivation, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis.

I would like to offer my special thanks to Prof. Eric SIMON for accepting me as his PhD student and for giving me the opportunity to pursue my PhD, thanks for these three years. Thanks to professor Martine LIENARD for giving me access to the laboratory and research facilities. I would like to extend my gratitude to all the members of the Telice group for their cordiality, and also thanks to Christophe GRANSART for his helpful comments.

I am particularly grateful to my jury committee Prof. Daniel ROVIRAS, Dr. Guillaume FERRE, Prof. Maryline HELARD, Prof. Charly POULLIAT and Dr. Gemma MORRAL, for their insightful comments and encouragement.

I would also like to acknowledge with much appreciation the crucial role of my angels William, Rosmilar and Julio, without their precious support, I could have never done this without you. Thank you for having faith in me and always encouraging me to continue pursuing my goals. I will be immensely grateful to you all my life.

I express my heartfelt gratitude to my lifelong friends: Yuli, Asdrubal, Carlos, Eliecer, Henry, Hilario, Elimar, Ulises, Capi and Ataya. In spite of the distance our friendship remains strong. I consider myself the luckiest person in the world to have such supportive friends, standing behind me with their love and support.

I am particular grateful to my colleagues and friends at the telecommunication Department of University of Carabobo in Venezuela, in particular, Prof. Del Pino, Prof. Fedon, Prof. Benjamin, Prof. Albornoz, Mejias, Cesar, Eduardo, Ahmad, Henry and all the teachers from who I learnt since my engineering studies and without their guidance, I would not have been here, blessing and support.

A special gratitude to my friends in France, Benjamin, Carina, Gwen, Madeleine, Navish, Ludo, Floreal, Stefanie, Jef, Cedric, Guillaume, Bernard, Adeline, Celine, Elise, Tony, my Remis, yoga and runcrew59 friends, for being present during these last three years in the good and bad times of my life. Your suggestions and encouragement helped me integrate into French life. Thanks for supporting me spiritually throughout the writing process of this thesis and my life in general.

Last but not the least, I would like to thank my family, especially my mother for her love, support, and constant encouragement I have gotten over the years. Thank you for making me who I am.

# Résumé

Le développement des communications sans fil a causé la surcharge des bandes de fréquences utilisables. Afin de poursuivre ce développement, les nouveaux systèmes sans fil doivent utiliser efficacement le spectre sans interférer avec les autres systèmes. Ainsi, ces nouveaux systèmes sans fil doivent être capables de détecter l'environnement électromagnétique (EM) afin d'être configurés de manière optimale et de devenir robustes dans cet environnement. Pour accomplir une configuration optimale face aux environnements EM, il est impératif de comprendre comment ces environnements EM affectent les systèmes de communication.

Dans cette thèse, nous nous sommes particulièrement intéressés au secteur des transports, notamment les trains à grande vitesse. Dans ce secteur, on peut trouver des interférences EM intentionnelles (IEMI) et des interférences EM non intentionnelles (EMI). Cette thèse porte sur les deux types d'interférences. Nous avons considéré comme interférences électromagnétiques non intentionnelles (EMI) les signaux d'interférences électromagnétiques transitoires produites par les pertes de contact entre la caténaire et le pantographe. Ces interférences sont très présentes sur les trains à grande vitesse. Pour les interférences EM intentionnelles (IEMI), nous avons utilisé des signaux d'interférence générés par des brouilleurs faible puissance que l'on trouve dans le commerce.

Nous avons choisi la norme IEEE 802.11n comme système de communication en raison de son développement actuel dans le secteur des transports. Afin d'étudier la vulnérabilité du réseau de communication IEEE 802.11n face à ces différents types d'interférences, nous avons effectué différentes expériences en chambre anéchoïque puis avons interprété les résultats de ces expériences.

Nous avons alors identifié le mécanisme d'accès au canal comme un point potentiellement vulnérable aux deux types d'interférences. En effet une interférence de faible puissance pourrait faire croire que le canal est occupé, empechant toute communication.

Concernant les IEMI, nous avons de plus remarqué que la période de balayage (SP) de la bande de fréquence du signal de brouillage est un paramètre important pour l'efficacité du brouillage. La période de balayage la plus nuisible était à 20 $\mu s$, car le brouillage couvre alors tout le canal.

Pour les signaux d'interférences EM transitoires, nous avons identifié la période DCF Interframe Space (DIFS) comme un autre paramètre vulnérable de la norme, car à partir d'un certain niveau de puissance d'interférence et dès que l'intervalle de répétition entre les transitoires (T) est inférieur à 24 $\mu s$, la communication est systématiquement interrompue. Ce chiffre est à mettre en relation avec la période DIFS.

# Abstract

The increase in the wireless communication development has overloaded the usable frequency bands. In order to continue with this development, new wireless systems must use the spectrum more efficiently to avoid interference with other systems. Thus, these new wireless systems must be capable of sensing EM environment in order to be configured optimally and to become robust in this environment. To accomplish an optimal configuration considering the EM environment, it is imperative to understand these EM environments affect communication systems.

In this thesis, we are particularly interested in the transportation sector, especially in high speed trains. In this sector both unintentional EM interferences (EMI) and intentional EM interferences (IEMI) can be found. This thesis is focused on both interference types. We considered unintentional EM interferences (EMI), such as transient EM interference signals produced by contact losses between the catenary and the pantograph. These interference are present on high speed trains. For intentional EM interferences (IEMI) we used interference signals as those generated by low power commercial jammers.

We have chosen the IEEE 802.11n standard as the communication system due to the fact that the current developments in the transportation sector is based on the Wi-Fi technology. In order to study the vulnerability of the IEEE 802.11n communication network facing these different interference types, we carried out different experiments in a semi-anechoic chamber and then we interpreted the results of these experiments.

We identified the channel access mechanism as a vulnerable feature of IEEE 802.11n. As a mater of fact, in the presence of a low power interference, the channel can be con-

sidered busy by the channel access mechanism, preventing any communication.

With regard to the IEMI, we have noticed that the sweep period (SP) of the frequency band of the jamming signal is an important parameter on the jamming performance. The most harmful sweep period was to 20 $\mu s$, because the jamming covers the whole channel.

For transient EM interference signals, we identified the DCF Interframe Space (DIFS) period as another vulnerable parameter of the standard. Because when the repetition interval between transients (T) is lower than 24 $\mu s$, with a certain interference power level, the communication is systematically interrupted. This figure is of the same order of magnitude as the DIFS period.

# Contents

# List of Figures

# List of Tables

# List of acronyms

| | |
|---|---|
| ACK | Acknowledgment |
| AP | Access Point |
| APS | Alimentation Par le Sol |
| ARF | Auto Rate Fallback |
| AWG | Arbitrary Waveform Generator |
| BCC | Binary Convolutional Code |
| BPSK | Binary Phase Shift Keying |
| CCA | Clear Channel Assessment |
| CCA-ED | Clear Channel Assessment-Energy Detect |
| CCK | Complementary Code Keying |
| CRC | Cyclic Redundancy Check |
| CS | Carrier Sense |
| CS/CCA | Carrier Sense/Clear Channel Assessment |
| CSMA/CA | Carrier Sense Multiple Access with Collision Avoidance |
| CTS | Clear To Send |
| CW | Contention Window |
| DCF | Distributed Coordination Function |
| DFT | Discrete Fourier Transform |
| DSSS | Direct Sequence Spread Spectrum |
| DIFS | Distributed Interframe Space |
| EIFS | Extended Interframe Space |
| EM | Electromagnetic |
| EMC | Electromagnetic Compatibility |
| EMI | Unintentional Electromagnetic Interference |
| EQM | Equal Modulation |
| FC | Frame Control |
| FCS | Frame Check Sequence |
| FEC | Forward Error Correction |

| | |
|---|---|
| FFT | Fast Fourier Transform |
| GI | Guard Interval |
| IEEE | Institute of Electrical and Electronics Engineers |
| IEMI | Intentional Electromagnetic Interference |
| IFS | Inter Frame Space |
| ISI | Inter Symbol Interference |
| ISM | Industrial Scientific and Medial |
| LDPC | Low-Density Parity-Check |
| NAV | Network Allocation Vector |
| MAC | Media Access Control |
| MCS | Modulation and Coding Scheme |
| MIMO | Multiple Input Multiple Output |
| OFDM | Orthogonal Frequency Division Multiplexing |
| OSI | Open System Interconnection |
| PHY | Physical |
| PLCP | Physical Layer Convergence Procedure |
| PMD | Physical Medium Dependant |
| QAM | Quadrature Amplitude Modulation |
| QPSK | Quadrature Phase Shift Key |
| RIFS | Reduced Inter Frame Space |
| RBAR | Receiver Based Auto Rate |
| RSSI | Received Signal Strength Indicator |
| RTS | Request to Send |
| SDM | Spatial Division Multiplexing |
| SIFS | Short Interframe space |
| SNR | Signal to Noise Ratio |
| ST | Slot Time |
| STBC | Space-Time Block Coding |
| STFT | Short Time Fourier Transform |
| SRS | Systeme de Recharge Statique |
| TCP | Transmission Control Protocol |
| UEQM | Unequal Modulation |
| UDP | User Datagram Protocol |
| WECA | Wireless Ethernet Compatibility Alliance |
| Wi-Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |

ll

# List of variables

| | |
|---|---|
| $\Delta f$ | Subcarrier spacing |
| A | Interference signal amplitude |
| D | Time duration |
| $f_s$ | Sampling rate |
| $f_0$ | Center frequency of Wi-Fi channel |
| $i(t)$ | Interference signal |
| ISR | Interference to Signal Power Ratio |
| $\mathrm{P}_I$ | Interference signal power |
| $\mathrm{P}_S$ | IEEE 802.11n communication signal power |
| SP | Sweep period or time duration to scan the frequency band of interest |
| T | Repetition interval between successive transients |
| $\mathrm{T}_{rise}$ | Rise time |
| $T_u$ | Duration of the useful part of the OFDM symbol |

ll

# Introduction

These days, wireless communications are anywhere and become indispensable for people. By the broadcast nature of wireless communications, the electromagnetic (EM) spectrum must be shared by all forms of wireless communication, including WLAN, cellular telephones, radio and television broadcasting, GPS position locating, aeronautical and maritime radio navigation, and satellite command and control. The growth of these systems has caused the spectrum's overload because the usable frequency bands are limited.

Therefore, the spectrum must be used more efficiently in order that these wireless technologies coexist without interfering among them. Indeed, one possible solution is that these systems become intelligent, that means they may be able to sense the EM environment in order to be configured optimally and to be robust in this environment.

To allow an optimal configuration, it is necessary to understand precisely the interference mechanisms on the communication systems. Therefore, we seek to comprehend how an interference signal affects a communication signal.

In particular, we are interested in the transportation sector. This sector is rapidly evolving and the wireless communications are essential to optimize new transport services and to enhance the passenger experience. For instance, wireless communications offer the possibility of Internet connection on board transports, as well as to provide quick and updated information to the passengers about the journeys.

Moreover, the transportation sector is innovating in order to reduce $CO_2$ emissions by using renewable energies and to follow the ecological transition towards electric ve-

hicles. These electric vehicles comprise a set of electrical components (a high-voltage power source, a frequency converter, an electric motor and high-power cables) which constitutes new sources of EM interference (EMI) able to disturb wireless communications.

Another significant evolution of the transportation sector is the intelligent autonomous transport systems. For instance, the ATO (Automatic Train Operation) is a device used to automate train operations. One of the challenges for this transportation system is the cybersecurity. Therefore, we must also take into account that the wireless systems have to be able to be resilient to cyber attacks. Among diverse cyber attacks, we are interested in communication jammers, which are intentional EM interference (IEMI) transmitters.

Thus, this research work is focused on both the EMI and the IEMI, which can be found in the transportation sector, especially in high speed trains. To carry out this study, we consider a Wi-Fi communication network due to the current development of several applications in the automotive and railway sectors based on the Wi-Fi technology. For example, the solution studied to provide Internet on board trains is based on the deployment of Wi-Fi hot spot on board coaches. Can also be mentioned the IEEE 802.11p standard, which is a specific Wi-Fi version dedicated to automotive applications and which will permit the information transmission between cars.

Thereby, the first chapter is dedicated to the description of the IEEE 802.11n which is the Wi-Fi version studied in this thesis. We will give an overview of this standard, introduce its main characteristics and highlight the key parameters which will be necessary to analyze the measurement results in chapter 3.

Then, the second chapter presents the EM interferences which can be present in the transportation sector. They are classified as unintentional and intentional EM interferences. Among the unintentional EM interference (EMI), we focus on the transient EM interferences produced by contact losses between the catenary and the pantograph in high speed trains. Next, the intentional EM interferences (IEMI) are presented, including an analysis of a conventional jammer.

In order to understand the impact of these intentional and unintentional EM interferences on an IEEE 802.11n communication network, this thesis will assess the communication performance under the presence of each interference type.

The third chapter gives the details of the whole experimental approach, including testing tools, measurement equipment and the general test setup used during the tests. This is followed by the description of each experiment carried out to evaluate the vulnerability of the IEEE 802.11n standard to the IEMI and the EMI. Different tests were carried out by varying the characteristics of the interference signals and identifying the relationship between the parameters of the interference signals and the communication performance degradation. Then, the measurement results and their interpretations will be presented, taking into account the impact of the signal processing performed at the receiver stage. Finally, we present our general conclusions and the perspectives of this work.

**Publications:**

The results of this research work have been published in IEEE Transactions on electromagnetic compatibility and in two conference publications URSI 2017. I received the *Young Scientists Award* for the paper [2]. Those are listed below:

1 Virginie Deniau, Christophe Gransart, Grecia L. Romero, Eric Pierre Simon, and Joumana Farah. "IEEE 802.11n Communications in the Presence of Frequency-Sweeping Interference Signals", *IEEE Transactions on Electromagnetic Compatibility*. Volume : 59. Issue: 5. 2017

2 Grecia Romero, Eric Pierre Simon, Virginie Deniau, Christophe Gransart and Mohamed Kousri. "Evaluation of an ieee 802.11n communication system in presence of transient electromagnetic interferences from the pantograph-catenary contact", 2017 *URSI General Assembly and Scientific Symposium (GASS)*, august 19-26, 2017.

3 Mohamed Raouf Kousri, Virginie Deniau, Jean Rioult, Grecia Romero and Eric Simon. "Comparative study of transient disturbances impact on 2G and 4G telecommunication systems in a railway context", 2017 *URSI General Assembly and Scientific Symposium (GASS)*, august 19-26, 2017.

Chapter 1

# IEEE 802.11n standard

Nowadays, everyone wants to have Internet connection at all time, to access to their online services anywhere. In order to fulfill this expectation, Wi-Fi networks are deployed in different places, including transports (trains, buses, etc ) to offer Internet connection and service access. These new services permit to the passengers to optimize their travel time and feeling productive. Then, the quality of the Internet connection is important for the attractiveness and the image of public transports. However, the transport environment can be exposed to significant electromagnetic interferences. For this reason, Wi-Fi service should work well in different electromagnetic environments.

In order to study the vulnerability of the IEEE 802.11 standard face to specific electromagnetic environments, the most determinant features of the Wi-Fi vulnerability have to be identified and their effect on the communication robustness in the presence of electromagnetic interferences has to be assessed. Indeed, this can permit to design future communication solutions more robust in specific electromagnetic environments.

We chose the IEEE 802.11n standard which incorporates the most recent technology solutions, such as OFDM (*Orthogonal Frequency Division Multiplexing*) signals that can be used in the 5G communications for example in a filtered version. Moreover, IEEE 802.11n uses the 2.4 GHz band, which is the most common band in Wi-Fi communication systems nowadays.

In this first chapter, the evolution of the IEEE 802.11 standard up to 802.11n is briefly described. We then focus on the main characteristics of the IEEE 802.11n stan-

dard, which is employed in this thesis, in highlighting the key parameters which will be necessary to analyze the measurement results in chapter 3.

## 1.1 IEEE 802.11

First of all, a brief introduction of the *Open System Interconnection* (OSI) model is provided. Indeed, the OSI lower layers are used by the IEEE 802.11 standard. The OSI model is a reference model of seven layers that describes the process of communication between two devices in a telecommunication network. Figure 1.1 depicts the OSI model, the upper layers represent the software that implements network services (applications). The lower layers relate to data transport, such as routing, addressing, flow control and electrical signals.

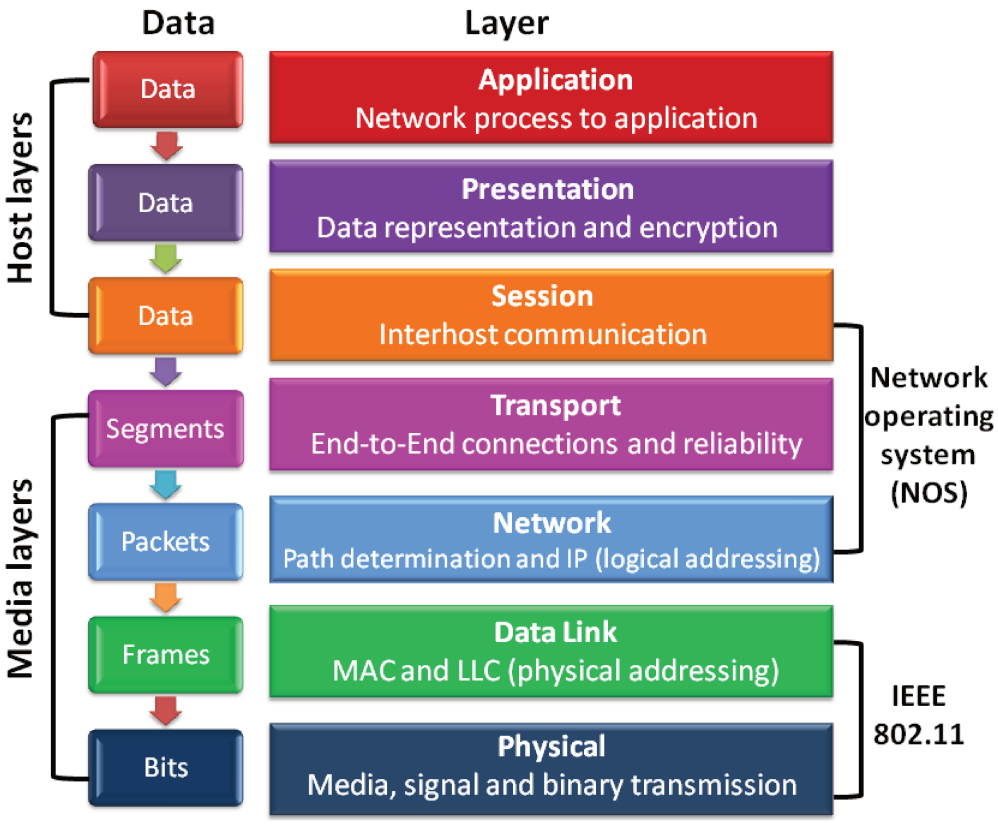



Figure 1.1 – OSI model.

The *Media Access Control* (MAC) and *Physical* (PHY) layer specifications are covered by the IEEE 802.11 standard. This standard is developed by the *Institute of Electrical and Electronics Engineers* (IEEE) for *Wireless Local Area Networks* (WLANs).

The first IEEE 802.11 standard was released in 1997 under the name of IEEE 802.11 with nominal data rates of 1 and 2 Mbps. Two years later, two amendments were added to the IEEE 802.11 standard:

- IEEE 802.11a-1999, known as 802.11a, enables raw data rates up to 54 Mbps in the *Industrial Scientific and Medial* (ISM) frequency band of 5 GHz using *Orthogonal Frequency Division Multiplexing* (OFDM) technology.

- IEEE 802.11b-1999, known as 802.11b, is an extension of the original IEEE 802.11 specification by using *Direct Sequence Spread Spectrum* (DSSS) [1] technology . 802.11b employs the modulation technique known as *Complementary Code Keying* (CCK)[2] that provides raw data rates up to 11 Mbps in the 2.4 GHz ISM band.

The 802.11b implementation was introduced on the market before the 802.11a [Cos10]. The 802.11b obtained a larger part of the market than 802.11a even reaching lower transmission rates. Indeed, the chips for the 2.4 GHz band were easier and cheaper to manufacture than the ones for the 5 GHz band.

In 1999, a group of leading industry companies came together to form the *Wireless Ethernet Compatibility Alliance*(WECA), now known as Wi-Fi Alliance [Wi-17]. This group aims to facilitate a better interoperability, quality, and user experience for IEEE 802.11 devices from a broad range of vendors. The Wi-Fi Alliance adopted the term Wi-Fi - that means *Wireless Fidelity* - for products that satisfy interoperability certification testing.

[1] DSSS is a spread spectrum modulation technique that is performed by multiplying the original data signal and a pseudo-noise (PN) digital signal. The result is in a wideband time continuous scrambled signal.

[2] CCK is a modulation scheme similar to DSSS which uses a shorter chipping sequence in order to obtain higher data rate.

Since then, the family of specifications developed by the IEEE for WLAN communications has had subsequent amendments with increasingly higher data rates. Each new amendment is incorporated in the latest version of the standard. The standard and the amendments provide the basis for wireless network products. We distinguish the particular specifications (e.g. 802.11a, 802.11b, 802.11g...) by the last letter.

In 2009, the IEEE 802.11n [Sta12] was officially released. This amendment improved the previous 802.11 standards by adding *Multiple Input Multiple Output* (MIMO) technology. IEEE 802.11n employs *Orthogonal Frequency Division Multiple* (OFDM), operates on both 2.4 GHz and 5 GHz frequency bands and it allows wider channel bandwidths (40 MHz versus 20 MHz). As a result, 802.11n increased the theoretical data throughput from 54 Mbps to 300 Mbps in a 20 MHz channel, and 600 Mbps in a 40 MHz channel [Ins].

## 1.2 IEEE 802.11n standard

*IEEE 802.11n - Amendment 5: Enhancements for Higher Throughput* has been included in the IEEE 802.11-2007 standard.

In contrast to the previous version, the IEEE 802.11n has a number of additional attributes in both the MAC and PHY layers, to get a significant increase of data throughput. The more significant attributes are:

- The use of MIMO, with *Spatial Division Multiplexing* (SDM) and *Space-Time Block Coding* (STBC).

- The possibility to employ 20 MHz or 40 MHz bandwidths. All previous versions have a 20MHz channel bandwidth. IEEE 802.11n has an optional mode where the channel bandwidth is 40 MHz. While the channel bandwidth is doubled, the number of data subcarriers is slightly more than doubled, going from 52 to 108.

- The use of 52 data subcarriers per 20 MHz channel instead of 48 subcarriers to its predecessors 802.11a/g. The number of subcarriers reaches 108 with a 40 MHz

channel.

- The frame aggregation, which permits to transmit several frames into one large frame instead of sending separate frames. In this way, the efficiency is improved by reducing the amount of overhead necessary to transmit each individual frame.

- The introduction of new *Modulation and Coding Scheme* (MCS) indexes. These new indexes are obtained by the evolution of the maximum FEC (Forward Error Correction) coding rate of 5/6, the possibility to use a reduced guard interval of 400 $ns$ instead of 800 $ns$ and the increases of the maximum data rate by spatial streams. The achieved highest data rate is 600 Mbps, by using 4 spatial streams in a 40 MHz channel with a 400 $ns$ guard interval.

## 1.3 PHY Layer Characteristics

The physical layer of IEEE 802.11n is the interface between the wireless medium and the MAC layer. As described above, it can operate on both 2.4 GHz and 5 GHz frequency bands with a high varying data rate from 65 Mbps up to 600 Mbps due to the use of MIMO and OFDM.

A summary of the PHY layer specifications is presented in Table 1.1

### 1.3.1 Orthogonal Frequency Division Multiplexing (OFDM)

OFDM is a parallel transmission scheme, where a high-rate serial data stream is split up into a set of N low-rate substreams, each of which are modulated on a separate subcarrier. The subcarrier spacing is denoted by $\Delta f$. To obtain high spectral efficiency, adjacent subcarriers are modulated by selecting orthogonal subcarrier frequencies, i.e., $\Delta f = 1/T_u$, where $T_u$ is the duration of the useful part of the OFDM symbol, as shown in Figure 1.2.

| **Characteristics** | **802.11n** | |
|---|---|---|
| Frequency band | 2.4 GHz | 5 GHz |
| Bandwidth | 20 MHz | 40 MHz |
| Modulation Technique | OFDM | |
| Forward Error Correction (FEC) | BCC, LDPC | |
| Frame Format | HT-Mixed and HT-Greenfield | |
| Coding Rate | 1/2,2/3,3/4,5/6 | |
| Modulation Schemes | BPSK,QPSK, 16QAM, 64QAM | |
| Data Subcarrier | 52 | 108 |
| Pilot Subcarrier | 4 | 6 |
| Total Subcarrier | 56 | 114 |
| IFFT Length | 64 | 128 |
| Guard Interval | 0.8 $\mu s$ / 0.4 $\mu s$ | |
| OFDM Symbol Duration | 4 $\mu s$ / 3.6 $\mu s$ | |
| Minimum data rates (one spatial stream) | 6.5 Mbps / 7.2 Mbps | 13.5 Mbps / 15 Mbps |
| Maximum data rates (one spatial stream) | 65 Mbps / 72.2 Mbps | 135 Mbps / 150 Mbps |
| MIMO Operations | Spatial Multiplexing 4x4, Beamforming, STBC | |
| Subcarrier spacing ( $\Delta f$) | 312.5kHz | |
| Maximum PSDU Length | 65535 Bytes | |

Table 1.1 – PHY layer specifications of the IEEE 802.11$n$ standards [Sta12].

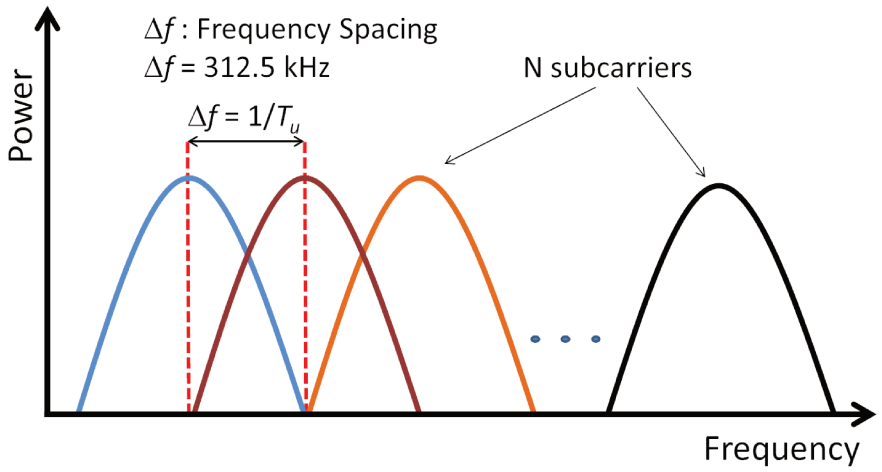



Figure 1.2 – Representation of OFDM subcarriers with a frequency spacing ($\Delta f$) of 312.5 kHz.

This modulation technique is a robust solution to counter the adverse effects of multipath propagation and *Inter-Symbol Interference* (ISI), because the bandwidth of the subcarriers is short compared to the coherence bandwidth of the channel; that is the individual subcarriers experience flat fading. This implies that the symbol period of the substreams is long compared to the delay spread of the time-dispersive radio channel. Besides, a guard interval (GI) is added to the useful part of each OFDM symbol in order to prevent ISI [Ano13, Pra04].

IEEE 802.11n on 20 MHz channel uses an FFT (Fast Fourier Transform) of 64, of which: 56 OFDM subcarriers, 52 are for data and 4 are pilot tones with a carrier separation of $\Delta f = 312.5$ kHz ($\frac{20MHz}{64}$) (3.2 $\mu s$) or 114 subcarriers on a 40 MHz channel. Besides, each of these data subcarriers can be modulated by BPSK, QPSK, 16-QAM or 64-QAM modulations, with a total symbol duration of 3.6 $\mu s$ or 4 $\mu s$, which includes a guard interval of 0.4 $\mu s$ or 0.8 $\mu s$ respectively (see Table 1.1). In any case, the subcarrier spacing is always fixed to $\Delta f = 312.5$ kHz. Note that, as will be seen in chapter 3, this parameter is a key parameter which plays a crucial role in the performance of communication when electromagnetic interferences are present.

Then, depending on the characteristics of the PHY layer, the IEEE 802.11n standard supports multiple transmission rates corresponding to different *Modulation Coding Scheme* (MCS) index values.

### 1.3.2 Modulation Coding Scheme (MCS) index

The MCS is also a key parameter for the interpretation of communication performances in the presence of interferences. Modulation Coding Scheme index is a value that determines the modulation type (e.g., BPSK, QPSK, 16-QAM, 64-QAM), forward error correction (FEC) coding rate (e.g., 1/2, 2/3, 3/4, 5/6) and number of spatial channels, as shown in Table 1.2.

Each MCS index has an associated data rate and the values are given for both 20 MHz and 40MHz channel bandwidths and for both 800 ns and 400 ns GI. 800 ns GI is the legacy mode as well as the default mode for 802.11n devices, and 400 ns GI is an optional mode for 802.11n devices [Lit12].

The table 1.2 gives rate-dependent parameters for MCSs with indices 0 to 76. MCSs with indices 0 to 7 and 32 have a single spatial stream; MCSs with indices 8 to 31 have

multiple spatial streams using equal modulation (EQM) on all the streams; MCSs with indices 33 to 76 have multiple spatial streams using unequal modulation (UEQM) on the spatial streams. MCSs indices 77 to 127 are reserved [Sta12, p.1688].

| **MCS index** | **Spatial streams** | **Modulation type** | **Coding rate** | **Data rate (Mbps)** | | | |
|---|---|---|---|---|---|---|---|
| | | | | **20 MHz channel** | | **40 MHz channel** | |
| | | | | **800 ns GI** | **400 ns GI** | **800 ns GI** | **400 ns GI** |
| 0 | 1 | BPSK | 1/2 | 6.5 | 7.2 | 13.5 | 15 |
| 1 | 1 | QPSK | 1/2 | 13 | 14.4 | 27 | 30 |
| 2 | 1 | QPSK | 3/4 | 19.5 | 21.7 | 40.5 | 45 |
| 3 | 1 | 16-QAM | 1/2 | 26 | 28.9 | 54 | 60 |
| 4 | 1 | 16-QAM | 3/4 | 39 | 43.3 | 81 | 90 |
| 5 | 1 | 64-QAM | 2/3 | 52 | 57.8 | 108 | 120 |
| 6 | 1 | 64-QAM | 3/4 | 58.5 | 65 | 121.5 | 135 |
| 7 | 1 | 64-QAM | 5/6 | 65 | 72.2 | 135 | 150 |
| 8 | 2 | BPSK | 1/2 | 13 | 14.4 | 27 | 30 |
| 9 | 2 | QPSK | 1/2 | 26 | 28.9 | 54 | 60 |
| 10 | 2 | QPSK | 3/4 | 39 | 43.3 | 81 | 90 |
| **11** | **2** | **16-QAM** | **1/2** | **52** | **57.8** | **108** | **120** |
| **12** | **2** | **16-QAM** | **3/4** | **78** | **86.7** | **162** | **180** |
| 13 | 2 | 64-QAM | 2/3 | 104 | 115.6 | 216 | 240 |
| 14 | 2 | 64-QAM | 3/4 | 117 | 130 | 243 | 270 |
| **15** | **2** | **64-QAM** | **5/6** | **130** | **144.4** | **270** | **300** |
| 16 | 3 | BPSK | 1/2 | 19.5 | 21.7 | 40.5 | 45 |
| 17 | 3 | QPSK | 1/2 | 39 | 43.3 | 81 | 90 |
| 18 | 3 | QPSK | 3/4 | 58.5 | 65 | 121.5 | 135 |
| 19 | 3 | 16-QAM | 1/2 | 78 | 86.7 | 162 | 180 |
| 20 | 3 | 16-QAM | 3/4 | 117 | 130 | 243 | 270 |
| 21 | 3 | 64-QAM | 2/3 | 156 | 173.3 | 324 | 360 |
| 22 | 3 | 64-QAM | 3/4 | 175.5 | 195 | 364.5 | 405 |
| 23 | 3 | 64-QAM | 5/6 | 195 | 216.7 | 405 | 450 |
| 24 | 4 | BPSK | 1/2 | 26 | 28.8 | 54 | 60 |
| 25 | 4 | QPSK | 1/2 | 52 | 57.6 | 108 | 120 |
| 26 | 4 | QPSK | 3/4 | 78 | 86.8 | 162 | 180 |
| 27 | 4 | 16-QAM | 1/2 | 104 | 115.6 | 216 | 240 |
| 28 | 4 | 16-QAM | 3/4 | 156 | 173.2 | 324 | 360 |
| 29 | 4 | 64-QAM | 2/3 | 208 | 231.2 | 432 | 480 |
| 30 | 4 | 64-QAM | 3/4 | 234 | 260 | 486 | 540 |
| 31 | 4 | 64-QAM | 5/6 | 260 | 288.8 | 540 | 600 |
| 32 | 1 | BPSK | 1/2 | N/A | N/A | 6 | 6.7 |
| 33-38 | 2 | UEQM | | Depends | Depends | Depends | Depends |
| 39-52 | 3 | UEQM | | Depends | Depends | Depends | Depends |
| 53-76 | 4 | UEQM | | Depends | Depends | Depends | Depends |
| 77-127 | | (reserved) | | | | | |

Table 1.2 – Modulation and coding schemes in single stream for IEEE 802.11n [Sta12, pp.1771-1780].

IEEE 802.11n has the capacity to learn the channel conditions in order to select the right MCS in run-time in order to improve the received signal quality. A continuous decision-making process is applied and based on the feedback from the receiver about the channel conditions. The system has the ability to adjust the modulation system to get the best compromise between data rate and error rate for the payload.

In our study, the test network employs two spatial streams and a 20 MHz channel. Thus, the network supports MCSs indices from 8 up to 15. Depending on the channel conditions the standard changes the modulation type and coding rate in order to reduce the transmission errors.

### 1.3.3 Rate adaptation algorithms

The main rate adaptation algorithms are named *Auto Rate Fallback* (ARF) and *Receiver Based Auto Rate* (RBAR).

- The ARF changes the transmission rate based on the success or failure of previous frame transmissions. The MAC protocol indicates a successful transmission by sending back an ACK (Acknowledgment) to the transmitter and a failed transmission is detected by the absence of an ACK (there is no Negative ACK). So, ACKs are used as implicit feedback. If two consecutive ACKs are not received, the current rate is assumed to be too high and the rate is lowered. If ten consecutive ACKs are received in a row, the transmission rate is increased to a higher data rate. ARF assumes that failure to receive an ACK is due to the rate being too high, even though the failure may have an other cause, such as a collision.

- In RBAR, the RTS (*Request to Send*) frame is used to measure the SNR (*Signal to Noise Ratio*). The receiver then determines the best rate based on this SNR and returns this rate to the transmitter, which uses it to transmit the data [LMT04, KKT+09].

## 1.4 MAC Layer Characteristics

The *Media Access Control* layer manages and maintains the communication between multiple stations in the network. The standard [Sta12] defines the *Distributed Coordina-*

*tion Function* (DCF) as the fundamental access method of the IEEE 802.11 MAC layer which is known as *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA).

### 1.4.1 Distributed Coordination Function (DCF)

The *Distributed Coordination Function* (DCF) is a distributed channel access mechanism. The DCF is designed for asynchronous data transport. It allows medium sharing between compatible WLAN nodes through the use of CSMA/CA.

In CSMA/CA when a station wants to transmit data, it previously senses the channel by the *Carrier Sense* (CS) mechanism over a fixed time duration to determine if another station is transmitting. If the medium is found to be idle, the station may initiate its transmission, otherwise the transmission is deferred, and the station waits for the medium to be idle.

Once the medium remains idle during a *Distributed Inter Frame Space* (DIFS) period, the station has to perform a backoff procedure with a backoff timer and then it can start to send the frames to the receiving (Rx) station.

If the receiving station correctly receives the frame, it sends back an acknowledgement (ACK) frame to the transmitting (Tx) station within the *Short Interframe space* (SIFS) period. The ACK frame indicates a successful reception. In the case that the ACK frame is not received due to frame transmission errors or an ACK frame transmission error, the Tx station assumes that the frame transmission failed and it defers its own transmission for an *Extended Interframe Space* (EIFS) period and schedules a retransmission of the same frame after the backoff procedure [PS13].

### 1.4.2 The backoff procedure

The backoff procedure is invoked by a station in two cases. It can be to transfer a frame once the medium is idle during a DIFS period and following a busy detection by the CS mechanisms. Or, it can be when the transmitting station infers a failed transmission. The random backoff procedure is very useful in a loaded network in order to avoid collision.

Indeed, when several stations are waiting an idle medium to initiate their frame transmissions, each one will select a random time, and as a result, it is unlikely that two

or more stations start transmission at the same time.

The backoff time is calculated using the following equation:

$$BackoffTime = Random() \times SlotTime \tag{1.1}$$

where

- *Slot Time* (ST): is a system parameter that depends on the characteristics of the PHY layer. It is defined as the minimum duration to determine the channel state (CCATime), plus the round-trip time, the propagation time and the processing time of the MAC layer.

- *Random*: refers to the number of slots and it is an integer in the range of [0, CW], where CW is the *Contention Window* and can vary [3] between CWmin and CWmax (Table 1.3)[Cos10, Sta12, TWT+13, MAE07].

### 1.4.3 Inter Frame Space (IFS)

As its name suggests, *Inter Frame Space*(IFS) is the time interval between frames. The CSMA/CA distributed algorithm defines several IFSs as part of channel access rules to provide control and access to the wireless medium at different priority levels as well as to avoid interferences. The length of each IFS interval is determined from attributes specified by the PHY layer. The different IFSs related with the DCF for IEEE 802.11n are presented in Table 1.3 and defined below:

#### Short Inter Frame Space (SIFS)

is the minimum gap between frames in a sequence used by the station to maintain the control of the medium. As soon as the station has accessed to the medium, the station respects the SIFS between the successive frames during the exchange sequence

[3] If the medium is determined busy due to interferences or other transmissions at any time during the backoff time, the backoff procedure is suspended. That means, the backoff timer shall not decrement for that slot. A new independent random backoff value is selected for each new transmission attempt by the exponential backoff algorithm, where the CW value is increased by $(oldCW \times 2 + 1)$, with an upper bound given by CWmax (Table 1.3). The medium must be sensed idle for the duration of a DIFS period or EIFS period, as appropriate, before the backoff procedure is resumed. Once the backoff timer reaches zero, the station can start its transmission.

in progress. It avoids that other stations use the medium.

SIFS is also the time interval between the acknowledgement (ACK) frame and the previous data frame as well as between RTS (*Request To Send*) and CTS (*Clear To Send*) frames exchanges, which will be defined later.

**Reduced Inter Frame Space (RIFS)**

is the shortest IFS defined in 802.11n. RIFS can be used in place of SIFS to separate multiple transmissions from one only transmitting station. [4]

**Distributed Interframe Space(DIFS)**

is used by the stations in a DCF network to transmit a data frame or management frame for the first time if the CS mechanism determines that the medium is idle during the DIFS period. In case the medium is detected as busy, the station has to sense again the medium during the DIFS period of plus the backoff time before occupying the medium.

DIFS period is defined by the following equation:

$$DIFS = SIFS + 2 \times SlotTime \tag{1.2}$$

**Extended Interframe Space (EIFS)**

as mentioned before, must be used instead of DIFS period after an erroneous frame reception. EIFS is used as an inhibitor to prevent serial collisions. EIFS is defined by the sum of SIFS, plus the DIFS and the time that takes an ACK frame transmission (ACKTxTime)[5], as you can see in Equation 1.3:

$$EIFS = SIFS + DIFS + ACKTxTime \tag{1.3}$$

[4]RIFS is used only with Block Acknowledgement (ACK), in this case several data frames can be continuously sent without wait for each ACK frame. At the end of transmission, the Tx station will simply send a request to Rx station of all ACK in block (BAR - BlockACKRequest). The Rx station replies with a only block with all ACK (BA-Block Acknowledgement).

[5]The ACK frame are not transmitted with the same data rate than the data frame.

| | **2.4 GHz band** | **5 GHz band** |
|---|---|---|
| RIFS | 2 $\mu s$ | |
| SIFS | 10 $\mu s$ | 16 $\mu s$ |
| DIFS | 28 $\mu s$ | 34 $\mu s$ |
| Slot Time | 9 $\mu s$ | |
| CWmin | 15 | |
| CWmax | 1023 | |

Table 1.3 – Values of some parameters in DFC of IEEE 802.11n [Sta12, p.1761]

In Figure 1.3, a successful packet transmission and the different IFSs are illustrated. In this example, the frame is transmitted after the DIFS period plus the backoff time formed by a contention window of seven slot times (i.e. $28\mu s + 7 \times 9\mu s = 91\mu s$, for 2.4 GHz band and short preamble).

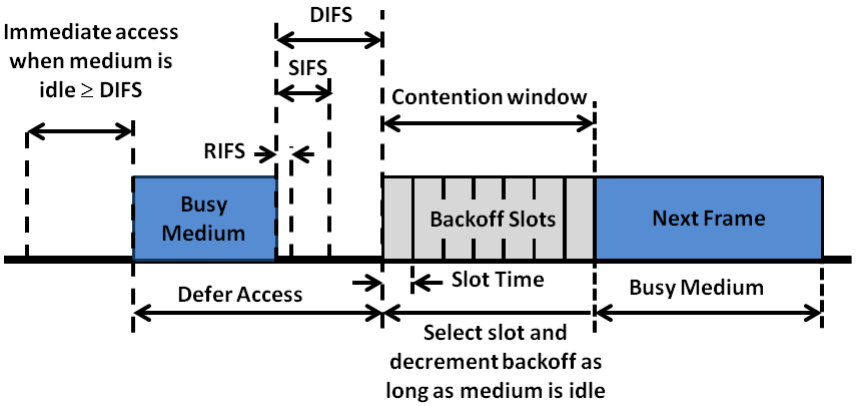



Figure 1.3 – Some IFS relationships [Sta12, p.826.]

Note that the DISF value is the minimum time period during which the channel has to be idle to allow the station to access to the medium. DIFS period is then one of the important parameters of IEEE 802.11n to be considered to analyze the impact of EM interferences on the communication.

### 1.4.4 CSMA/CA with RTS/CTS

The CSMA/CA with RTS/CTS (*Request To Send/Clear To Send*) is another mode more refined than the CSMA/CA method, which can also be used by the DCF. The CSMA/CA with RTS/CTS is used to further minimize collisions and avoid hidden station problems [6].

Once the transmitting (Tx) station determines that the medium has been idle for a DIFS or a EIFS period (plus the backoff times), the transmission and reception stations exchange short control frames (called RTS and CTS frames) before the data transmission.

Figure 1.4 shows the time diagram for a transmission using the IEEE 802.11 CSMA/CA with RTS/CTS scheme. The transmitting station (source) sends a *Request To Send* (RTS) frame once it has observed the medium is idle during the DIFS period. Note that the only case where the backoff procedure is not used is when a station is ready to transmit a data frame and the medium has been idle for a time longer than the DIFS period.

When the receiving station (destination) receives the RTS, it will send back a *Clear To Send* (CTS) frame after a SIFS period if it is available to receive data. Then, the source is enable to send the data after a SIFS period. Once that this procedure is completed and the destination successfully receives the data frame, the destination sends back a positive acknowledgment (ACK frame) after a SIFS period, without considering the state of the medium.

## 1.5 Carrier sense (CS) mechanisms

The CS mechanism is used to determine the state of the medium. The CS can be performed in two ways at the PHY or MAC layers levels. The MAC layer CS is used by other users to abstain from using the medium. Note that since in our experiments,

[6]The hidden station problem is due to the physical obstacles in the environment or the distance between the A and C stations. This problem can do that the CS mechanisms of station A detects the idle channel and station A starts a transmission towards the station B when it is already receiving a frame from the station C. Thus, station B gets both frames from different stations causing a collision.

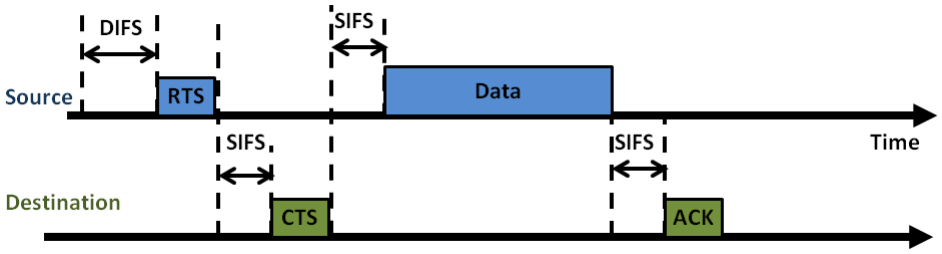



Figure 1.4 – RTS/CTS/data/ACK settings [Sta12].

detailed in chapter 3, only one user is considered, the MAC layer CS will not be investigated in this thesis.

At the PHY layer, the CS mechanism is the physical carrier sense process which is detailed as follows [RR07].

### 1.5.1 Physical carrier sense

PHY CS performs a *Clear Channel Assessment* (CCA) at the physical layer to detect the presence of ongoing transmissions on the wireless medium and indicates the state of medium to the MAC layer. CCA is performed by all stations that are not transmitting or receiving data, in such a way that the sensing station knows if it can transmit. The CCA mechanism can be based on energy detection (ED) or on carrier sense (CS).

#### Clear Channel Assessment-Energy Detect (CCA-ED)

This mechanism verifies the power of the received signal on the operating channel. CCA-ED detects the busy medium if it measures a power greater than the CCA-ED threshold [Sta12, p.1614].

#### Carrier Sense/Clear Channel Assessment (CS/CCA)

The carrier sense/clear channel assessment uses coherent detection. CS/CCA reports a busy medium if it detects a valid frame, by recognizing the preamble. In that case, a power measurement is also performed but only over a specific part of the frame which is called the PLCP (*Physical Layer Convergence Procedure*) header [Sta12, p.1614].

## 1.6 Analysis of the frame types used by IEEE 802.11

As explained above, the IEEE 802.11 standard focuses on PHY and MAC layers. For this reason, this section briefly describes the frame format in each layer.

In IEEE 802.11, the PHY layer is categorized into two sublayers called the *Physical Medium Dependant* (PMD) and the *Physical Layer Convergence Procedure* (PLCP). On the one hand, the PLCP prepare the frame for the transmission by taking the frame from the MAC layer and adding the preamble and PLCP header that permit the interoperability between the PHY and the MAC processes. On the other hand, the PMD describes functional, electrical and radio frequency characteristics for the communication signals. Thus, PMD modulates and transmits the frame.

Each frame as shown in Figure 1.5 at PLCP sublayer starts with a preamble which is used for synchronization and channel estimation [SRS14, SSR15, RHS12], followed by the PLCP header and the MAC Data. The PLCP header contains information required for decoding the data such as date rate and frame length. The MAC data comprises the MAC header, the data to transmit (called the Frame body) and the FCS (*Frame Check Sequence*).

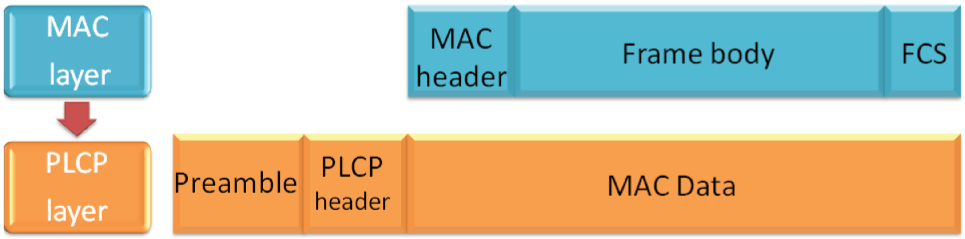



Figure 1.5 – IEEE 802.11 Frame format.

## 1.7 802.11 MAC Frame Format

Figure 1.5 illustrates a general MAC frame which is formed by the MAC header, the frame body and terminated by the *Frame Check Sequence* (FCS). These different parts are described below.

### MAC header

The MAC header notably contains the frame control (FC) which indicates the nature of the data (signaling or information), the duration and the MAC addresses.

### Frame body

The Frame body of variable length contains information specific to the frame type.

### FCS (*Frame Check Sequence*)

The FCS field contains a *Cyclic Redundancy Check* (CRC) of 32 bit used to detect any corruption of data in transit. This value is calculated by the transmitting station from all the data included in the MAC header and the Frame Body field. When the destination station receives the frame, the FCS value is recalculated and compared with the FCS value included at the end of the frame. If the two values are different, an error is assumed and the frame is discarded. Therefore the destination station requests to send again the frame.

In the IEEE 802.11n standard, there are three MAC frame types: data frames, control frames and management frames. These frame types are specified in the MAC header [7]. A brief description of these frames is presented below.

## 1.7.1 Data frame

Data frames are the frames which contain the packets that are transmitted, which come from higher layers. As MAC frames, Data frames include different fields: the MAC header, the frame body (data to transmit) and the FCS.

In the case of the Data frame, the MAC header can contain up to 4 addresses. These addresses correspond to the addresses of the transmitting and receiving stations, the station address which is at the origin of the data and finally, the station address which has to receive the data. The four addresses are specified only if the data has to progress between different networks [Sta12, PS13]. The frame body length is variable, depending on the frame aggregation process.

[7] specifically in the frame control (FC) field

### 1.7.2 Control frame

Control frames are used to control access to the wireless **medium** between stations. The most frequent control frames are RTS, CTS and ACK [Sta12, RR07].

#### The RTS frame.

The Request To Send frame is the first frame transmitted by a station to get the approval to send data.

The RTS frame as shown in Figure 1.6 includes 20 Bytes. The MAC header of the RTS frame includes the frame control, the duration, the transmitting (TA) and receiving (RA) addresses.

The Duration field is the time in microseconds, required to transmit the frame exchange sequence formed by the CTS frames, data frame, and ACK frame, plus three SIFS periods.

The frame body of the RTS frame is empty.

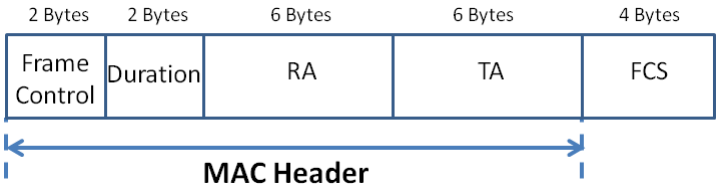



Figure 1.6 – RTS frame [Sta12].

#### The CTS frame.

As explained above, a receiving station replies to a RTS frame by sending a *Clear To Send* (CTS) frame after a SIFS period if the medium is idle. The CTS frame format contains 14 Bytes (see Figure 1.7).

Its length is reduced in comparison to the RTS frame because its MAC header specifies only the receiving station address.

The duration field is obtained from the duration field of previous RTS frame minus the time required to transmit the CTS frame and minus one SIFS period.

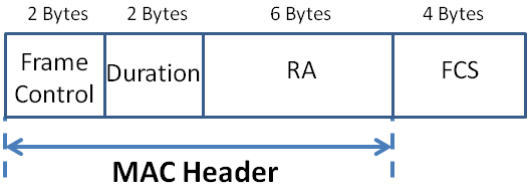



Figure 1.7 – CTS frame [Sta12].

### The ACK frame.

The *Acknowledgement*(ACK) frame is sent by the receiving station to notify to the transmitting station the successful data frame reception. Like CTS frames, ACK frames contain the same fields and have the same 14 Bytes length (see Figure 1.6).

The duration field is the value of the duration field of the previous frame minus the time required to transmit the ACK frame and the SIFS period.

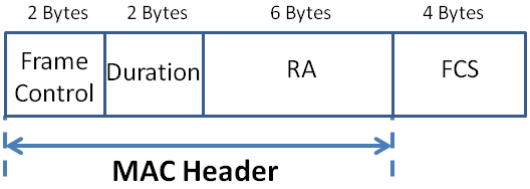



Figure 1.8 – ACK frame [Sta12].

## 1.7.3 Management frames

Management frames are used to manage access to wireless **networks**. They correspond to the frames which permit to inform of the existence of the network and to connect/disconnect the stations to the network (association, deauthentication, authentication, disassociation).

### The Beacon frame

is one of the management frames in IEEE 802.11. It is broadcast periodically to announce the presence of the wireless network by the AP (*Access Point*). The Beacon frame contains all the information about the network, including:

- The channel frequencies (frequency center and bandwidth)
- The time period during which the AP has been active (Time Stamp).
- The time interval between two consecutive beacon frames (Beacon Interval). This interval is a configurable parameter and it is measured in Time Units (TUs), where each TU equals 1024 microseconds. The beacon interval is generally set to 100 TUs, approximately 100 milliseconds.
- The name and address of the wireless network.
- The supported rates by this wireless network.
- The security capabilities to access the network.

The beacon frame can have a variable length, depending on the transmitting status and its transmission rate is a constant of 1 Mbps [PS13, MZM+14].

## 1.8 IEEE 802.11n communication

To end this chapter about the IEEE 802.11n standard, we will provide a general overview of the process of communication between a user and a server connected through an access point (AP), in order to illustrate the main protocols and layers involved during the IEEE 802.11n communication.

Figure 1.9 depicts a connection scheme between a user (from now on called a client) and an access point (AP) connected to a server. It is noted that the connection between the client and the AP goes through an IEEE 802.11n communication network, whereas the AP is connected to the server by IEEE 802.3 network. Taking into account that this research is centered on the IEEE 802.11n vulnerability, we are going to focus on the process of communication between the client and the AP, which is based on CSMA/CA with RTS/CTS.

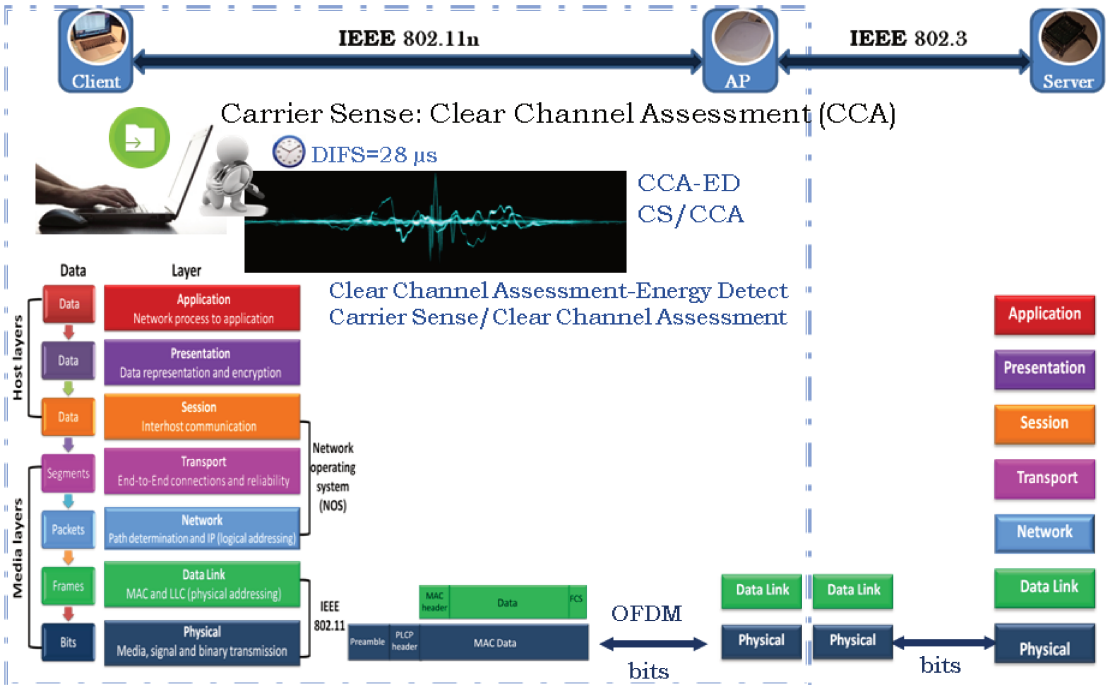



Figure 1.9 – Connection scheme between a client and a server connected through an AP.

As previously explained, when a client wants to start a process of communication, before sending a data (application layer), it must send a request to MAC and PHY layers. At these layer levels, the CS mechanisms (explained in section 1.5) are activated, in order to know if the communication channel is idle or busy.

Once the CS mechanism determines the idle channel, the client is enable to use the channel (PHY layer). Then, it sends a RTS frame created by the MAC layer and sent by the PHY layer as a binary transmission through a wireless channel previously established by the network. Once the AP receives the RTS frame at the MAC layer and if it is able to answer this request, the AP replies to the client with a CTS frame (MAC layer) sent through the same wireless channel. When the client receives the CTS frame, it starts sending the data after the SIFS period,as soon as the AP receives the data, it makes a verification by checking the FCS field and if the data arrives without errors the AP sends an ACK frame to the client after the SIFS period. Figure 1.10 illustrates a representation of the exchanged frames between AP and the client.

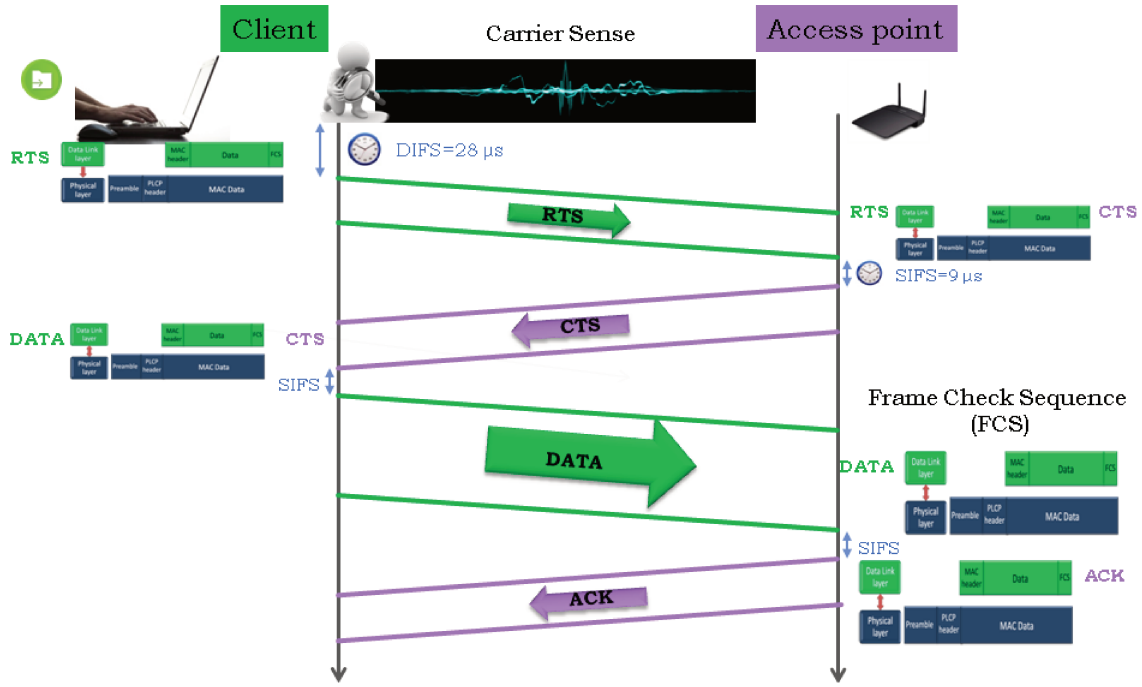



Figure 1.10 – Representations of an IEEE 802.11n communication between AP and client.

Figure 1.11 illustrates a representation of the IEEE 802.11n frames exchange between the AP and the client, measured by a wavemaster 813Zi-B oscilloscope connected to an antenna placed near the client. As a result, the frames coming from the client side were received with greater power than those coming from the AP side.

Figure 1.12 exemplifies another representation of an IEEE 802.11n communication exchange between the AP and the client, measured by an N9030A PXA signal analyzer connected to an antenna placed close to the client. This visualization was captured by a real-time spectrum analyzer, which which allows us to study the signal in more details thanks to the Time-Frequency representation. Note that the headers at the beginning of each frame (RTS, CTS, DATA) are similar and corresponds to the PHY layer header (preamble and PLCP header).

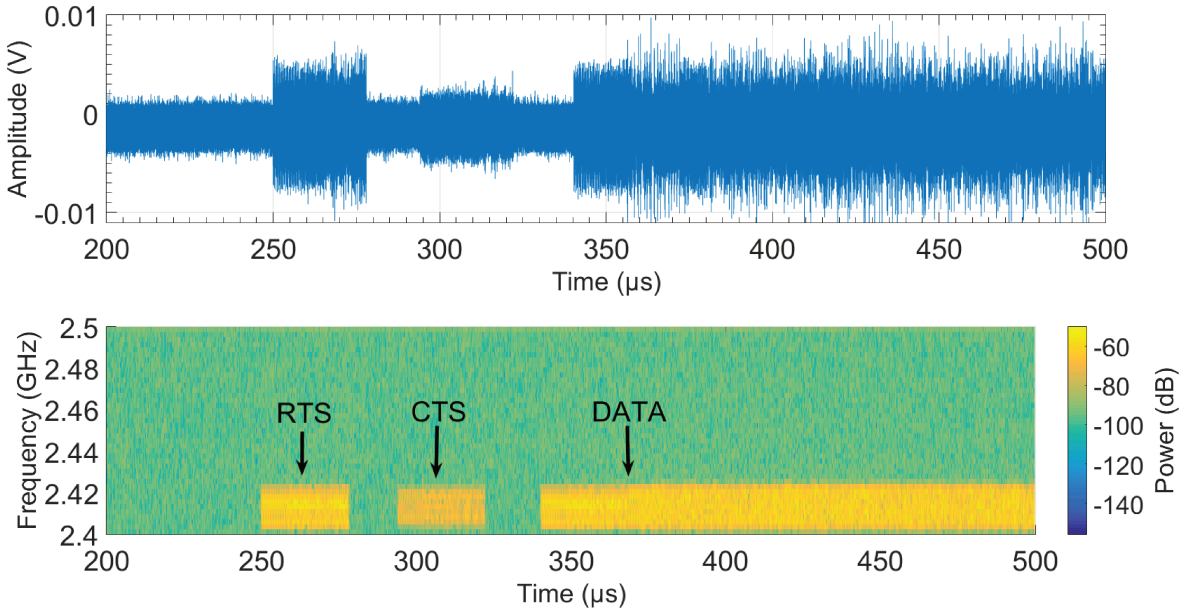



Figure 1.11 – Time domain and Time-Frequency representations of an IEEE 802.11n communication between AP and client by oscilloscope.

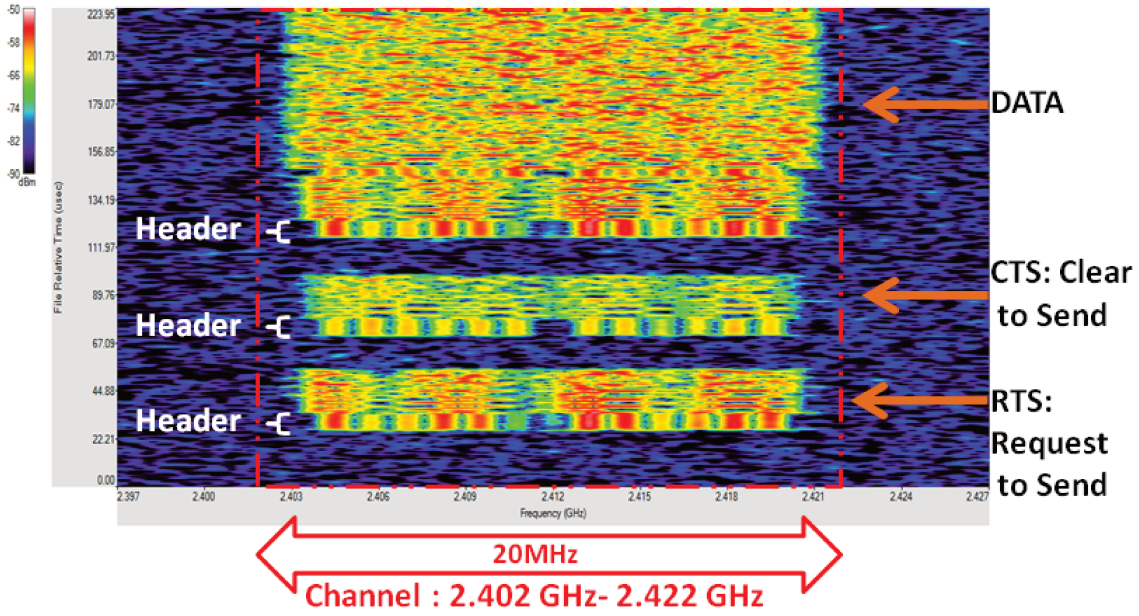



Figure 1.12 – Time-Frequency representation of an IEEE 802.11n communication between AP and client by real-time spectrum analyzer.

## 1.9 Conclusion

We have presented in details all the steps and mechanisms which are involved in the communications based on the 802.11n standard.

Therefore, in the following analysis, this precise description will permit us to understand the exchanges collected during our experiments and to distinguish the messages coming from the AP and the client.

We also introduced the different parameters and mechanisms which characterized the 802.11n standard, at the PHY and MAC layers.

Some of these parameters and mechanisms will have to be taken into account to understand the impact of specific interferences on the degradation of the communication. In particular, in the interpretations, we will highlight the impact of the CS and CCA-ED mechanisms and the MCS adjustment mechanism.

We will also compare the characteristics of the interference signals with the different parameters of the 802.11n standard, such as the symbol duration, the subcarrier frequency spacing and the DIFS period.

Chapter 2

# Electromagnetic interference

The transportation world evolves to improve transport efficiency, the safety, mobility, as well as reduce environmental impacts. New transportation technologies are developed to respond to these requests, including a connected system and electricity highways to fight against air pollution.

However, the implementation of these technologies in the transportation sector could produce electromagnetic (EM) interferences. That are referred to as the electromagnetic compatibility (EMC).

In general, the electromagnetic interferences could be categorized according to several criteria. We can consider the type of source (low and high power electromagnetics [Gir04, TG94]) from natural or industrial origin, their time domain characteristics (transient or continuous signal), their bandwidth (wide band or narrow band) and the type of propagation (conducted or radiated interferences). This work focuses on the radiated electromagnetic interferences from industrial origin that could be intentionally or unintentionally generated. The first section of this chapter is dedicated to unintentional electromagnetic interferences and the second section deals with intentional electromagnetic interferences.

## 2.1 Unintentional electromagnetic interference

Unintentional EM interference could be caused by another type of electronic or electrical equipment present in a transport electromagnetic environment. The diversity of unintentional interferences makes they can be categorized according to different criteria. In the following subsection an overview of two main cases of unintentional EM interference sources in a transport environment powered by electricity is presented: EM interference produced by the catenary-pantograph contact and EM interference generated by ground-level power supply.

### 2.1.1 Introduction to the different kind of emissions in the transport system

This subsection briefly presents some of the different kinds of unintentional electromagnetic interference present in the transport system, including the emissions generated by the electrical networks and the power electronic system, whose interference signals reach high power levels. However, they can not perturb the IEEE 802.11n communications because their interference signals just reach up to a few dozen MHz [Oua11], without generating any kind of impact over IEEE 802.11n communications whose frequency bands are 2.4 GHz or 5 GHz.

On the other hand, radiated interferences generated by sliding contact solutions such as pantograph-catenary systems or the third rail systems (also known as, ground-level power supply) are known to be of short duration and as very wide band signals [RM14].

Nowadays, there are new power supplies for transportation sectors that incorporate these sliding contact solutions mainly known in the railway sector, and now appear in road transport.

One of these solutions, called eHighway system by Siemens [Sie17], is based on a hybrid truck with a conventional combustion engine and an electric motor with battery. Electrical operations include an intelligent pantograph system that unfolds over the truck either manually or automatically connected to a catenary once it has been detected by the sensor. Figure 2.1 shows a road freight transport powered by electricity.

Another solution named APS (*Alimentation Par le Sol*) is developped by Alstom


Figure 2.1 – Road freight transport powered by electricity [Sie17].

[Als17]. It is a ground-level power supply system for tramways through a third rail placed between the running rails, as can be seen in Figure 2.2.

This third rail is formed by two types of segments: powered segments (about 10 meters) and neutral segments (about 3 meters). Each tramway has contact shoes to collect electricity from powered segments which are activated by antennas placed under the tramway when it passes over these segments. Thus, only the segments covered by the tramway are powered while the other segments are not. This system eliminates the use of catenaries, thus preserving the aesthetics of the city.

Another system proposed by Alstom, is a ground-level static charging system, called SRS (*Systeme de Recharge Statique*). The SRS is for tramways, electric buses and hybrid trucks with on board energy storage. This technology makes it possible to recharge the battery by quick high power level transfers at each stop of the vehicle, during the normal dwell time (about 20 seconds). The recharge is performed by contacting the vehicle to the ground based charging slots, which are connected to a compact power supply cabinet integrated into transport stations.

Figure 2.3 illustrates the slots used for fast charging of trams and buses. The coded signal transmitted by an antenna located at the ground-based charging slot allows the


Figure 2.2 – APS system by Alstom [Als17].

buses and the trams arriving at the station to locate the charging slot. Once the batteries are recharged, the transport can run independently until the next stop.

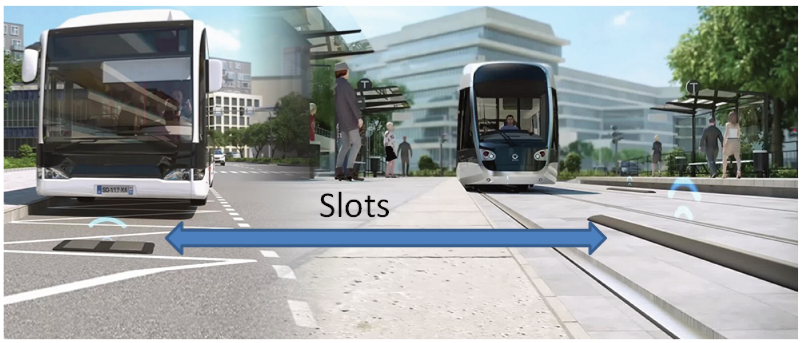



Figure 2.3 – SRS system by Alstom [Als17].

One variation of eHighway, APS and SRS systems is Elways system [Elw17]. Elways system makes it possible to charge the battery of the electric vehicles while driving with-

out the use of catenaries. Elways system is developped for electrical cars, trucks, and buses, as well as hybrid vehicles.

This system is based on the battery recharge via an electric rail placed in the centre of the roadway which is connected to the vehicle through an electric arm, as shown in Figure 2.4. When the vehicle detects the rail, it attaches and detaches automatically by the moving arm. Once it is in contact with the electrical grid, the battery is recharged in short distance and in a minimal charge time.

The rail is built and electrified in sections. In order to be safe and efficient, the voltage section supply shuts off automatically when the arm leaves a section of the road.


Figure 2.4 – Elways system [Elw17]

Therefore, different types of power supply for transport systems are on the market or in development today. This work focuses on the pantograph-catenary system. The impact of the interferences generated by this system needs to be studied because it is used by high-speed trains and the occurrence of electric arcs generated by contact losses generally increases with the train speed [JK17]. The pantograph-catenary system and its interferences have been well studied in the literature [RM14, JK17, Wan09, DPOS$^+$08].

However, to our knowledge, no work dealt with the impact of this kind of interferences on a 802.11n communication.

### 2.1.2 Characteristics of the EM interferences produced by contact losses between the catenary and the pantograph

This subsection presents the main characteristics of EM interferences generated by contact losses between the catenary and the pantograph, in order to study the effect of these transient discontinuities on an IEEE 802.11n communication network.

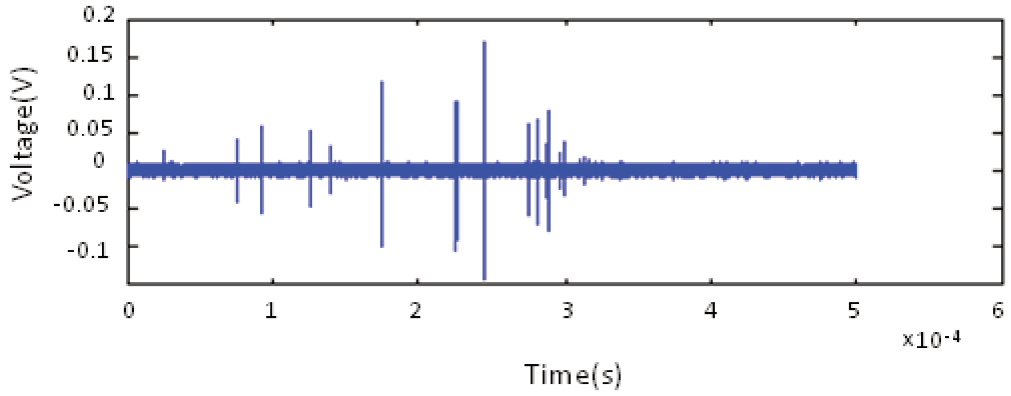
When the contact between catenary and pantograph is lost, important current variations are generated. These fast current variations are broadband transient [RM14]. Moreover, this contact loss will be more frequent as the speed of the railway vehicle increases [JK17].

Experimental results presented in [Wan09] show that the spectrum of these pulses are very wide. Thus, these high and transient interferences may cover the Wi-Fi band, i.e., 2.4 GHz .

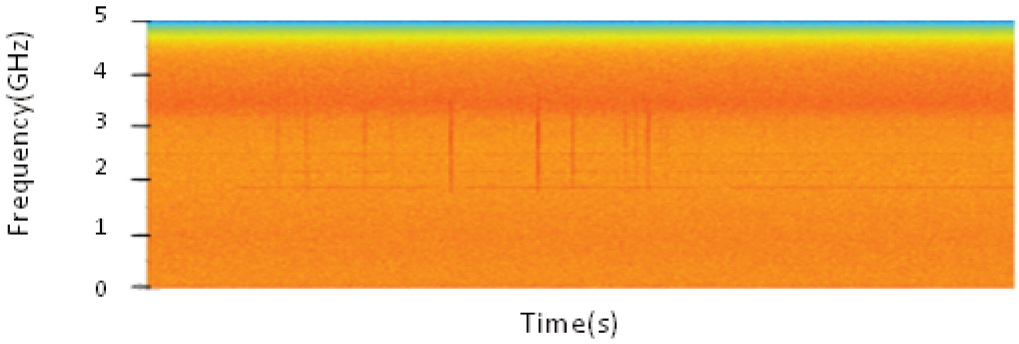
Note that the study of the EM interferences in the railway environment at high frequencies generally requires to filter the low frequency signals. Indeed, the railway environment is characterized by the presence of very high power low frequency signals. Due to the significant difference of powers between the low frequency and high frequency signals, the high frequency signals are generally undetectable in the measurement results. By consequence, the major part of the studies in the literature [DPOS+08], employs measurement methods and sampling rates which do not allow to characterize the interference signals above 1 GHz.

However, within the scope of the ANR Metaphort project [met09], specific measurements were carried out to characterize the high frequency EM noises present on board trains. An 1 GHz - 9 GHz wide frequency band antenna (Model 3181 1 GHz - 9 GHz) was placed on the train roof and the measurements were performed with an oscilloscope (LeCroy WavePro 760Zi). To allow the high frequency signals analysis, a 2 GHz- high pass filter was connected to the oscilloscope input and a 20 Gsamples/s sampling rate was applied.

Figure 2.5 shows some results of these measurements. Figure 2.5(a) represents a measured signal in the time domain. It is composed of transient signals which are very short time duration signals and they occur with variable time intervals. Figure 2.5(b) shows the time-frequency representation of the measured signal obtained through the spectrogram algorithm. The representation shows that the frequency band covered by the transient signals is very wide.




(a)




(b)

Figure 2.5 – Interference signals measured in the railway environment; (a) Time domain representation, (b) Time-Frequency representation.

Finally, these interferences come from electrostatic discharges between the catenary and the pantograph. Electrostatic discharges present very short temporal characteristics

and are naturally able to cover very wide bands, including the Wi-Fi band. Therefore, it is necessary to study their impacts on Wi-Fi communication networks. The next section presents the mathematical model which is defined to represent these transient interferences and which will be used in the experimental tests of chapter 3.

### 2.1.3 Mathematical model of EM interference produced by contact losses between the catenary and the pantograph

In this section, we present the mathematical model that we used to emulate transient EM interferences representative of those observed on board a moving train. According to the results presented in Figure 2.5, the mathematical model of the EM pulse must be of a very short duration, have a variable period and broadband. Based on this, the interference signal model used for the experimental test must have, as characteristic parameters, the time duration (D) and the repetition interval between successive transients (T).

Previous studies [XWZ13, DDA+12] proposed the double exponential function as representative analytical expression. To generate this double exponential function, we selected the approximate mathematical expression proposed by [DDA+12], whose characteristic parameters are the time duration (D) and rise time ($T_{rise}$). The time duration (D) and the rise time ($T_{rise}$) values were estimated from statistical analyses of transient signals collected on board moving trains and are about $ns$ [SDR+09].

Thus, the general expression is defined by:

$$i(t) = A\left(e^{-\frac{t}{D}} - e^{-\frac{t}{T_{rise}}}\right) \tag{2.1}$$

Where $t$ is the time, A is the voltage amplitude. Knowing that we study the impact of such interferences on a Wi-Fi network, the Equation (2.1) must be modulated to concentrate the power in the 2.4 GHz frequency band in order to reproduce the behavior of a reception Wi-Fi antenna. The Equation (2.1) from now on is expressed as:

$$i(t) = A\left(e^{-\frac{t}{D}} - e^{-\frac{t}{T_{rise}}}\right)\sin\left(2\pi f_0 t\right) \tag{2.2}$$

Where $f_0$ is the center frequency of Wi-Fi channel. The Equation (2.2) corresponds to the general expression of one transient (event). Figure 2.6 depicts this mathematical expression with a 10 $ns$ time duration, 0.5 $ns$ rise time and a $f_0 = 2.412$ GHz center

frequency. The interference signal band is centered over the Wi-Fi channel between 2.402 GHz and 2.422 GHz. The variation between its spectral components over the channel are within 3 dB. This implies that the signal has a stable response within the channel, which is essential to have repeatable test results.

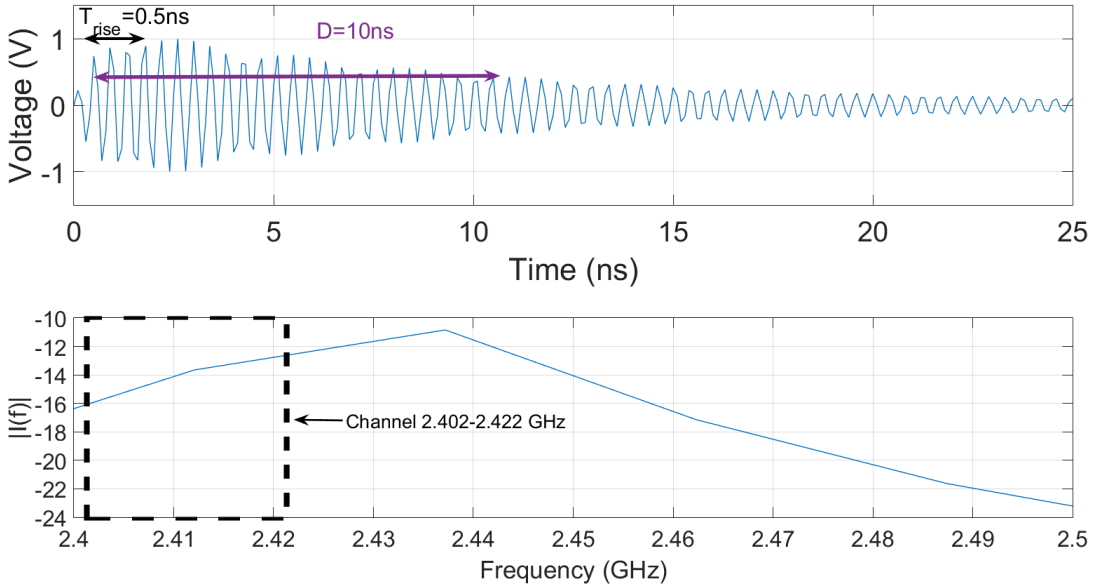



Figure 2.6 – The double exponential signal represented in time domain and frequency domain, applying a 40 $ns$ window.

As mentioned above, another characteristic of the interference signal model is its repetition period (T). Figure 2.7 shows the time domain and frequency domain representations of the double exponential signal with T = 10 $\mu s$ repetition period. In the frequency representation, we can verify that the signal covers the channel from 2.402 GHz to 2.422 GHz with a 3 dB variation.

The mathematical model of transient EM interference is defined with all its parameters. In the next chapter, it will be applied to several experiments to study the vulnerability of the IEEE 802.11n communication in the presence of these transient interferences representative of those produced by the sliding contact between the catenary and the pantograph. In particular, we would like to evaluate whether the performance of an IEEE 802.11n communications network deployed on board a train could be degraded by these interferences and identify solutions to mitigate their impact on the standard.

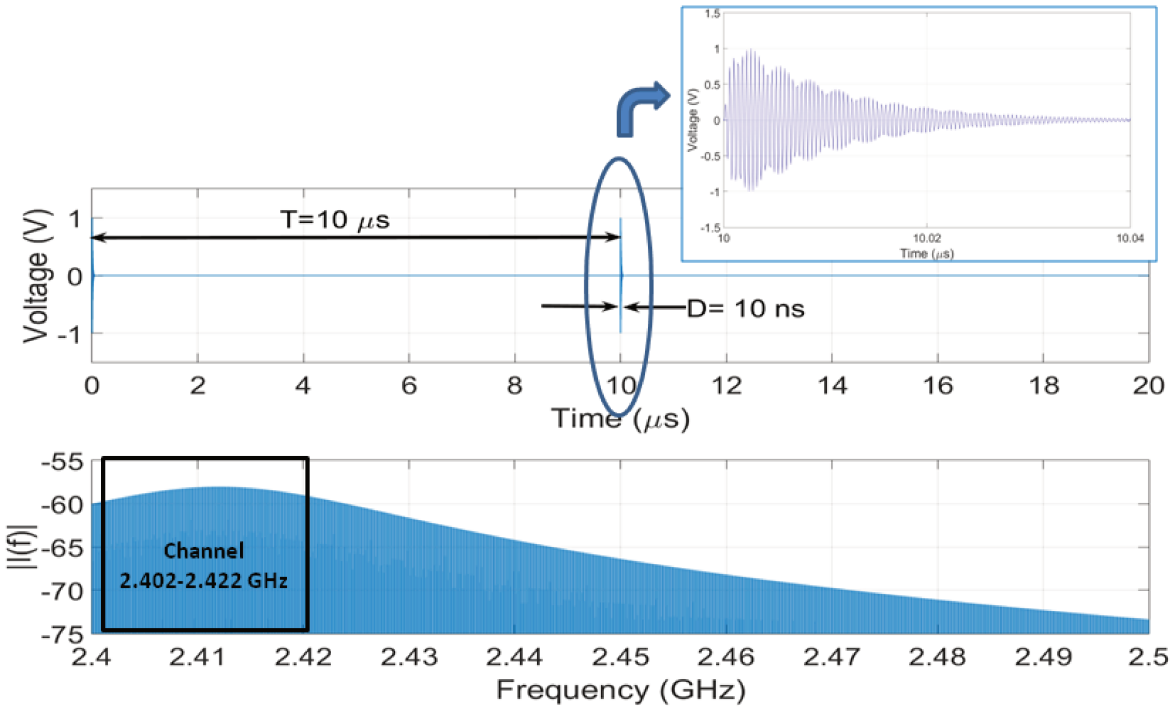



Figure 2.7 – Time and frequency representations of a double exponential signal with D=10 $ns$, $T_{rise}$ = 0.5 $ns$ and T = 10 $\mu s$. The frequency representation is obtained with a 20 $\mu s$ time window.

## 2.2 Intentional electromagnetic interference

This section is dedicated to present intentional electromagnetic interferences (IEMI). These interferences can be generated intentionally for terrorist or malicious purposes. The objectives are to disrupt, confuse or damage electrical and/or electronic systems through the generation of electromagnetic energy to induce interference inside the systems [RS10, Gir04]. However, in our work, we do not study powerful IEMI which can provoke permanent damage. We study IEMI which can be generated to corrupt the communication signals, and which the powers are comparable to those of the communication signals.

### 2.2.1 Classification of jamming

First of all, we define the term *Jamming* which is a technique used for avoiding or limiting the effectiveness of wireless communications. In the literature [SLPL+15, Poi11a], there are a large number of classifications of jamming techniques. Our synthesis is presented below.

- Protocol-Aware Jamming: in this jamming type, the jamming signal is defined according to the prior knowledge of the protocol used for the communication system to exploit its weaknesses in order to increase jamming effectiveness.

  For example, through MAC protocol aware, the jamming signal can send a packet with a valid MAC header, with a long duration in order that other users adjust their NAVs (*Network Allocation Vector*) [1], deferring their transmission attempts. In the case of MAC layers based on CSMA/CA, a protocol-aware jamming can send a pulse interference signal during the SIFS period in such a manner that the CCA (*Clear Channel Assessment*) detection algorithms senses the channel as busy.

- Spoofing Jamming: it consists in sending signals pretending to come from a legitimate communication in order to become a member of the network. Here, the spoofing jamming can take the place of a legitimate user whose the service will be denied.

- Learning Jamming: this kind of jamming tries to disrupt the communication with different jamming signals, and checks if the jamming signal is efficient to corrupt the communication; this means it can adapt its attack techniques according to its own successes and failures.

- Frequency Sweeping Jamming: this is the more frequent jamming technique. It is the simplest to implement and it consists in affecting the PHY layer by covering the frequency channels dedicated to the communication standard. It can cover the frequency bands of the standard partially or totally.

[1] The NAV value indicates the time for which the medium should be busy. This value comes from MAC header specifically in the duration field of previous frames.

Furthermore, each one of these jamming techniques can be implemented with slightly variant versions. For example, we can mention those that permanently transmit or only emit when they detect a communication, as well as those that adapt their output power.

### 2.2.2 Analysis of conventional jammers

We bought several commercial jamming devices and we analyzed them in order to compare and characterize the jamming signals generated by these different devices. Note that from now on, we will use the term jammer for commercial jamming device. This section details the analysis of one jammer and highlights the main differences which can be observed between the interferences produced by different jammers.

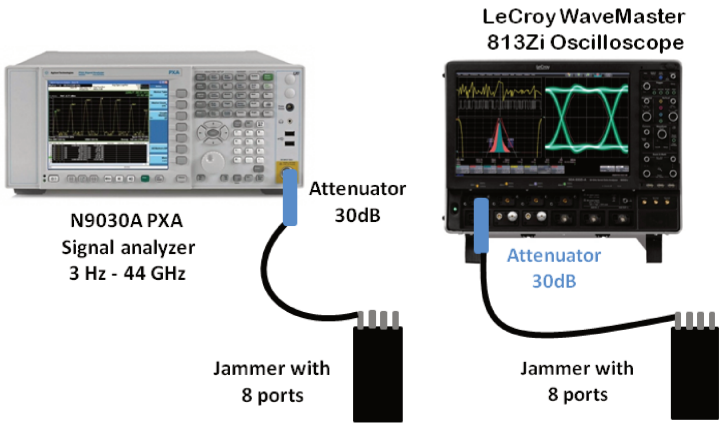
The presented jammer covers eight frequency bands, including the 2.4 GHz Wi-Fi band. Table 2.1 presents its characteristics, including the frequency bands covered by each antenna and the targeted communication system. We noticed that for cellular networks, the jammer covers only the downlink frequency band. That means that it can corrupt the communication signal received by mobile phones. For Wi-Fi networks, it covers the whole 2.4 GHz Wi-Fi band.

| **Jammer with 8 antennas** | | |
|---|---|---|
| **Antenna** | **Band (MHz)** | **Type** |
| 1 | 925-960 | 2G GSM 900 (Download) |
| 2 | 1805-1880 | 2G DSC 1800 (Download) |
| 3 | 2110-2170 | 3G UMTS (Download) |
| 4 | 1570-1580 | GPS (1575.42 MHz) |
| 5 | 2400-2485 | Wi-Fi 802.11 b/g/n |
| 6 | 168-178 | Lojack (173.075 MHz) |
| 7 | 2620-2690 | 4G LTE (Download) |
| 8 | 790-862 | 4G LTE (Upload-Download) |

Table 2.1 – Jammer characteristics.

A set of measurements was performed in a conducted mode in our laboratory. The experimental setup used is shown in Figure 2.8.

In order to identify the exact frequency bands covered by each antenna, each output was successively connected to the spectrum analyzer (N9030A PXA signal analyzer 3




(a) (b)

Figure 2.8 – Experimental setup; (a) with spectrum analyser, (b) with oscilloscope.

Hz - 44 GHz) as shows Figure 2.8(a). An attenuator of 30 dB was connected to the spectrum analyzer input. The measurement results of Max Hold traces are displayed in Figure 2.9. It is observed that the jammer covers all the frequency bands presented in table 2.1.

To obtain the Time-Frequency representation of each jammer output port, each output signal was measured by an oscilloscope (LeCroy WaveMaster 813Zi-B 13 GHz) with 10 Gsamples/s as is shown in Figure 2.8(b), including a 30 dB attenuator at the oscilloscope input. Finally, Time-Frequency representations are obtained through spectrogram algorithms applied to stored data by the oscilloscope.

Figure 2.10 shows Time-Frequency representations of the signals generated by the 8 ports of the jammer. It is noted that all the cases have a similar Time-Frequency representation, whose interference signals do not permanently cover the whole frequency band. This result shows that the jammer is basically a transmitter, whose interference signal is a chirp signal type, and its frequency band is swept in time [Poi11a].

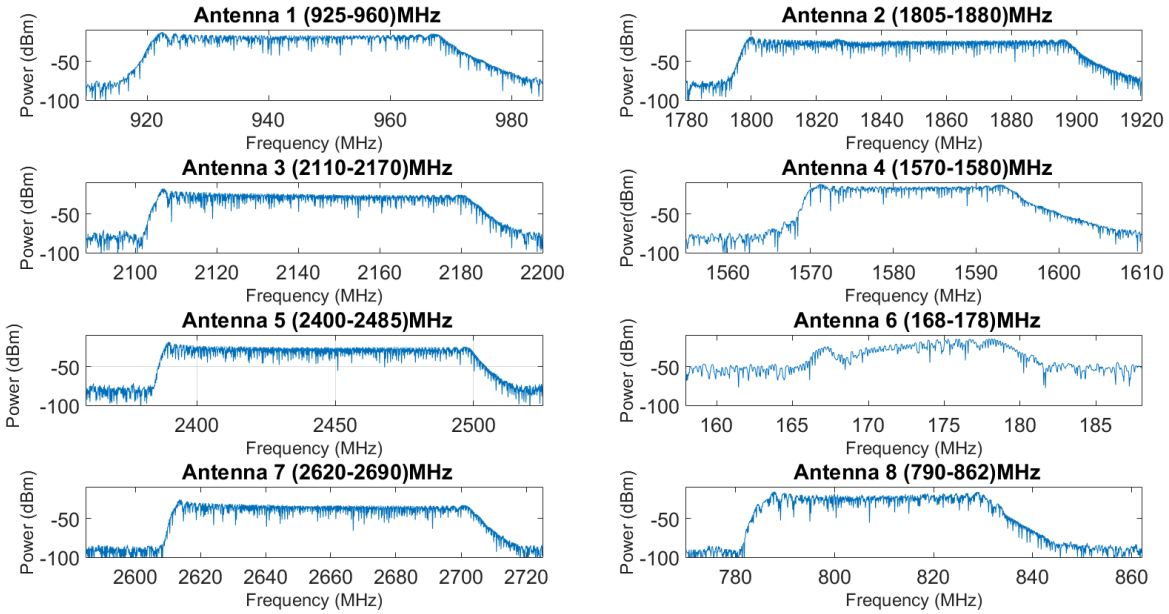



Figure 2.9 – Spectrum representation of each output of the commercial jammer (Table 2.1).

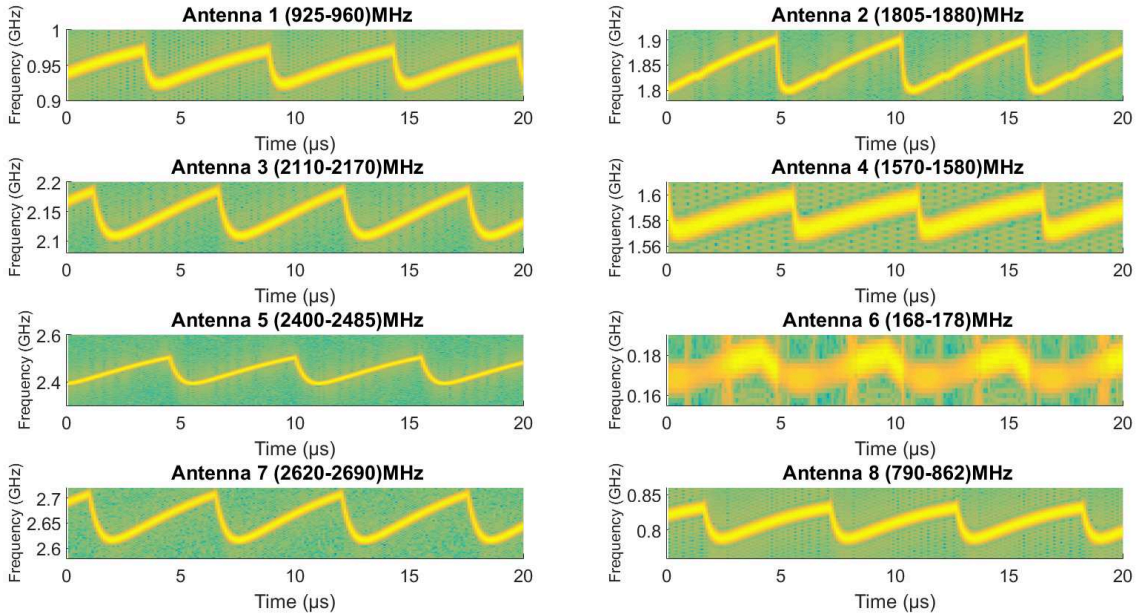



Figure 2.10 – Time-Frequency representation of each output of the commercial jammer (Table 2.1).

We present in Table 2.2 the minimum and maximum frequencies covered by the signal at each jammer output and the *Time Duration* to scan these frequency bands. What is interesting about these results is that the Time Duration for all the outputs was approximately 5.5 $\mu s$ regardless of the band, meaning that the Time Duration represents a key parameter of the jammer.

Furthermore, in characterizing different jammers, we observed that the nature of the jamming signals is similar but the Time Duration to scan the frequency bands can be different from one jammer to an other. Thus, in the following pages we will study the importance of this parameter, which will be called as the *Sweep Period* (SP).

| Output | Fmin (MHz) | Fmax (MHz) | Time Duration (us) |
|---|---|---|---|
| 1 | 922,9 | 966,8 | 5,483 |
| 2 | 1797 | 1899 | 5,425 |
| 3 | 2109 | 2183 | 5,48 |
| 4 | 1572 | 1597 | 5,48 |
| 5 | 2393 | 2500 | 5,53 |
| 6 | 175,8 | 1138 | 5,478 |
| 7 | 2617 | 2705 | 5,48 |
| 8 | 786,1 | 830,1 | 5,579 |

Table 2.2 – Spectrogram measurement results of the commercial jammer with 8 output port

Now, because this work focuses on Wi-Fi communications, Figure 2.11 and Figure 2.12 respectively present spectrogram and spectrum representations of the signal generated by the antenna 5 of the jammer, which covers the 2.4 GHz Wi-Fi band according to Table 2.1. These results evidence that the jammer covers the whole range from 2.4 GHz to 2.5 GHz.

After studying the jamming signal generated by the jammer, the next step will be to digitize our own intentional EM interference signal with similar characteristics to be used in the experimental test. This model will permit us to control the sweep period in order to study its impact on the communication performance. In the following section, we present the mathematical model of the frequency sweeping jamming signal.

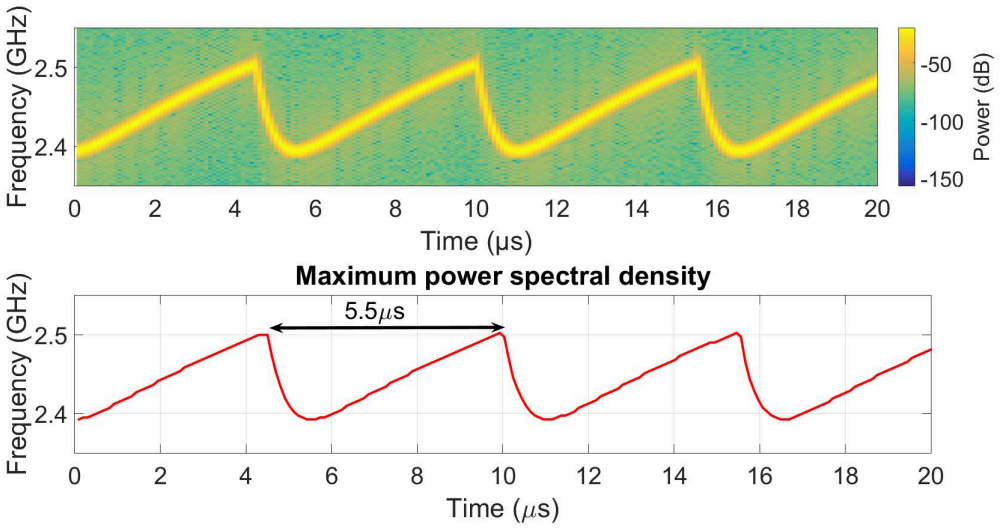



Figure 2.11 – Spectrogram of the antenna 5 of the commercial jammer (Table 2.1).

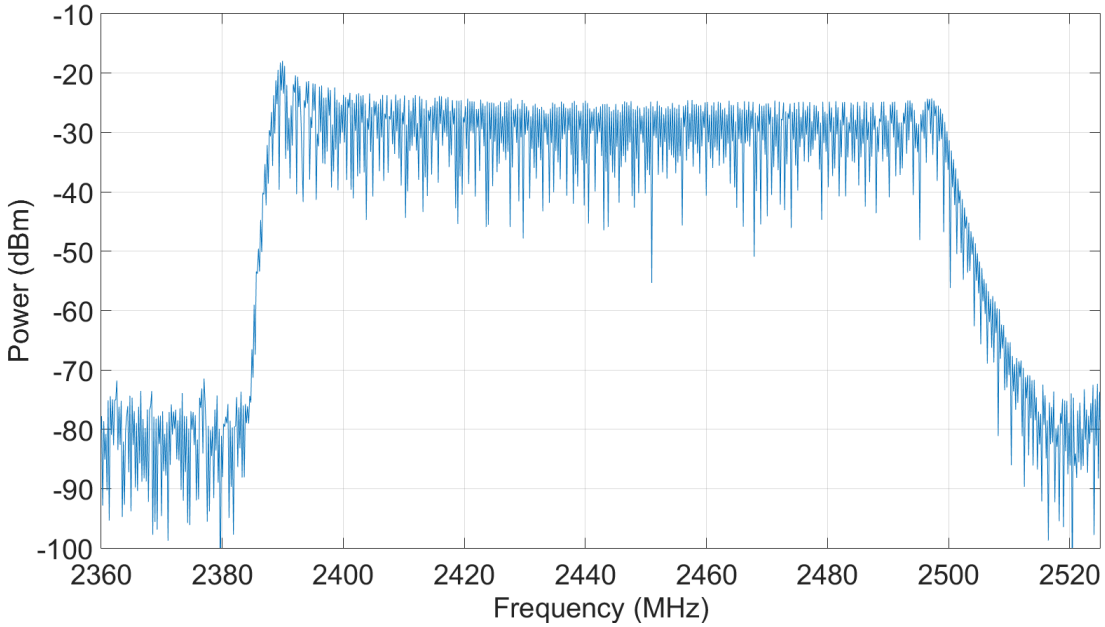



Figure 2.12 – Spectrum representation of the antenna 5 of the commercial jammer (Table 2.1).

### 2.2.3 Mathematical model of the frequency sweeping jamming

This section defines the mathematical expression of intentional EM interference which will be used in experimental tests. This expression will permit us to extract the intentional interference model by Matlab. The model will then be employed to assess the impact of the jamming signal on the performance of IEEE 802.11n communications through tests which will be detailed in the following chapter.

The mathematical model is based on the measurement results obtained in the previous section. The interference waveform must be representative of frequency sweeping jamming signals. Moreover, it is important that the intentional interference covers the entire Wi-Fi band from 2.4 GHz to 2.5 GHz in a homogeneous way.

Our model can be expressed as:

$$i(t) = \mathrm{A}\cos\left(2\pi f(t)t\right), \quad 0 < t < \mathrm{SP}, \tag{2.3}$$

where A is the interference signal amplitude. $f(t)$ is defined from the instantaneous swept frequency $f_i(t)$. SP is the sweep period or time duration to scan the frequency band of interest.

To represent the swept frequency process of the signal, $f_i(t)$ has to vary linearly from $f_1$ at time 0 to $f_2$ for a duration SP, as we can see in Figure 2.13.

$$f_i(t) = \frac{d}{dt}\left[f(t)t\right] = \frac{f_2 - f_1}{SP}t + f_1, \tag{2.4}$$

yielding

$$f(t) = \frac{f_2 - f_1}{2SP}t + f_1. \tag{2.5}$$

Figure 2.13 illustrates the interference signal defined by Equation (2.3) with its key parameters ($f_1$, $f_2$ and SP).

We used Matlab to digitize the interference signal of Equation (2.3). In order to cover the entire 2.4 GHz Wi-Fi band, we set $f_1$ and $f_2$ at 2.4 GHz and 2.5 GHz respectively. Figure 2.14 presents time domain and Time-Frequency representations of our jamming signal with SP of 10 $\mu s$.

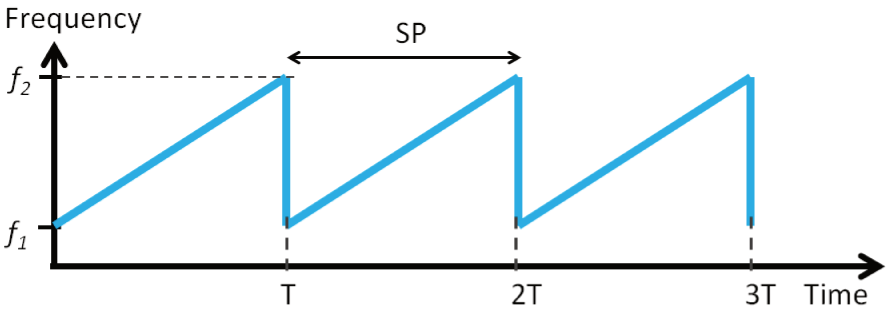



Figure 2.13 – Time-Frequency representation of the frequency sweeping interference signal.

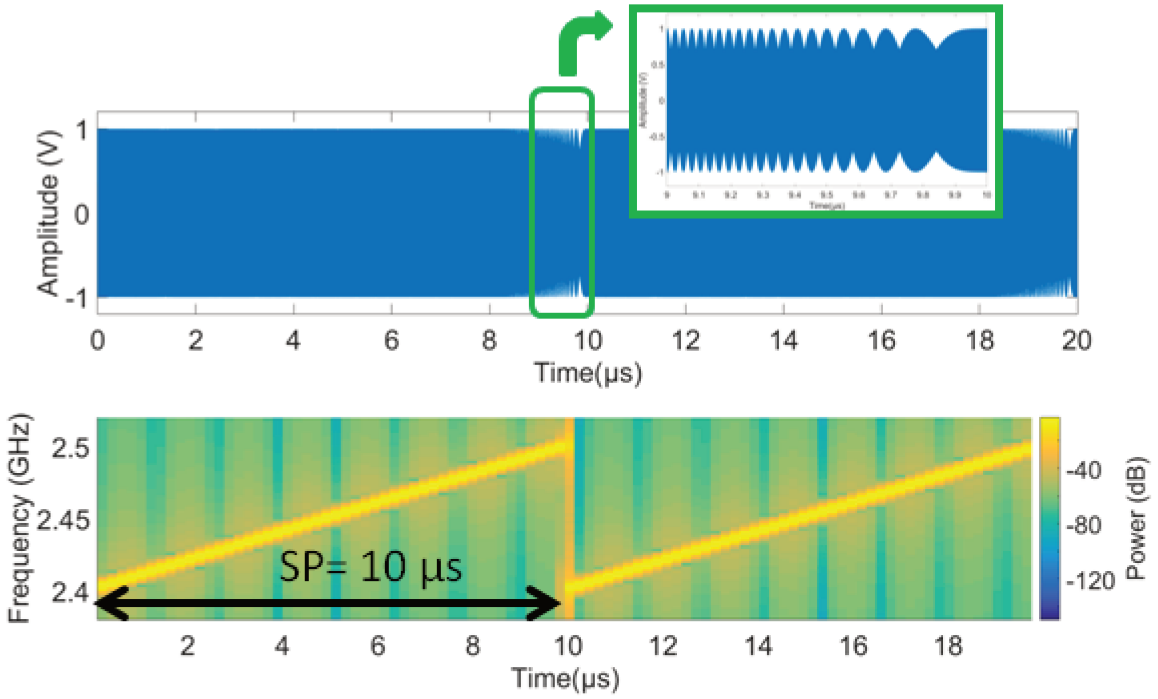



Figure 2.14 – The frequency sweeping interference signal with a sweep period of 10 $\mu s$ in the time domain and Time-Frequency representations.

Chapter 3

# Measurements and interpretations

After having presented the characteristics of the IEEE 802.11n standard and the different types of interference signals that will be used for measurement tests, we describe the experimental approach, including testing tools, the measurement equipment and the general test setup used during this research work. This is followed by the description of experiments carried out to evaluate the vulnerability of the IEEE 802.11n standard to specific intentional and unintentional EM interferences.

The first experiment is based on the interference signal that emulates a jammer (previously presented in section 2.2.3). We varied the main jammer parameters in order to identify which parameter values have more influence on the quality of the IEEE 802.11n communications.

For the second experiment, we used another type of interference signal of short duration and broadband, corresponding to the transient signal generated by contact losses between the catenary and the pantograph (previously presented in section 2.1.3).

Firstly, we introduce the general setup, including the different tools and equipment employed in both experiments. Then, for each experiment, the specificities of the test setup are highlighted and measurement results are presented in detail and analyzed.

## 3.1 Experimental approach

This section begins by explaining the testing tools used to measure the IEEE 802.11n network performance. Next, we describe the measurement equipment, as well as the general scheme of the experimental setup used during the experiments.

### 3.1.1 Testing tools

We chose Iperf and Wireshark as testing tools for measuring the IEEE 802.11n network performance. Both testing tools are free software and they are described below.

#### 3.1.1.1 Iperf

Iperf is a network testing tool used to create TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) data streams. It also measures the throughput of a network in terms of bit rate.

Iperf has been evaluated in [KNNS11] among four different monitoring tools. The results indicate that Iperf shows the highest throughput for a packet size of 1,408 bytes.

To measure the bit rate at the transport layer, the tool uses a client-server architecture where the Iperf client connects to a Iperf server [Ipe, SAS+14].

To assess the IEEE 802.11n network performance, we measured the bit rate through TCP tests. Indeed, TCP detects and retransmits any lost segments whereas UDP packets are sent without any checks. In this case, if a packet is lost, it is not re-transmitted and the measurement of the bit rate is not impacted.

During the tests, the Iperf3 program is run in such a way that the data are continuously exchanged between the client and the server through the access point. Each experiment begins with the Iperf client continuously sending a TCP stream to the Iperf server over the IEEE 802.11n network. We ran the Iperf tool with default settings (e.g. TCP window size, the interval in seconds between periodic bit rate reports) and the test duration time was set to 1000 secs. The bit rate is measured on the client side (from the client to the server).

#### 3.1.1.2 Wireshark

Wireshark is a network protocol analyzer, which allows us to capture and examine packets that are moving over a specific computer network [Wir17].

Once the packets are captured, these could be inspected for the diagnostic of network problems. Wireshark has various features, including color coding, filters, and statistics that help us to analyze the traffic flow over the network.

Wireshark allows us to know the signal power level, noise power level, as well as if the packets are received without errors and retransmission number of data packets. The errors are detected by means of the FCS (Frame Check Sequence) (see section 1.7).

The above-mentioned information will be useful to identify in some cases the effect of interference signals over the network.

### 3.1.2 Measurement equipment

This section presents the equipment used to generate and to transmit the interference signal, as well as the devices needed to perform measurements, including the signal generator, the oscilloscope, the attenuator, the amplifier and the antennas.

#### 3.1.2.1 Tektronix AWG7102 Signal Generator

The generation of the interference signal is carried out with an Arbitrary Waveform Generator (AWG) (Figure 3.1) that can generate any arbitrarily defined waveshape with sample rates of 10 Gsamples/s. The waveform was previously defined with Matlab and recorded in a file that is uploaded in the AWG. The signal can be repeated either indefinitely or over a specific period of time.

Figure 3.1 – Tektronix AWG7102 Signal Generator.

#### 3.1.2.2 LeCroy WaveMaster 813Zi Oscilloscope

This device (Figure 3.2) allows time domain signal measurements, with bandwidth up to 30 GHz and 80 Gsamples/s sampling rate. Applying the spectrogram algorithm on the stored data and according to the defined sampling rate, we obtain its spectrogram representation, which allows us to analyze the time-frequency distribution of the signal.

Figure 3.2 – LeCroy Wave Master 813Zi Oscilloscope.

#### 3.1.2.3 J7211A Attenuation Control Unit

The J211A attenuation control unit was connected to the AWG7102 Signal Generator output in order to vary the power of interference signal step by step. The J211A attenuation (Figure 3.3) can cover from DC to 6 GHz and gives an attenuation up to 121 dB with a 1 dB step size.

Figure 3.3 – J7211A Attenuation Control Unit.

#### 3.1.2.4 GRF5060 RF Power Amplifier

In some tests, we used the GRF5060 RF power amplifier to reach higher power levels. The amplifier (Figure 3.4) provides 40 dB gain and operates from 800 MHz to 4200 MHz.

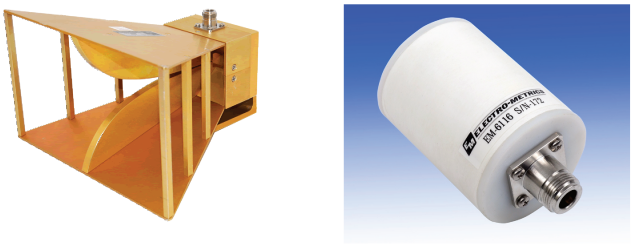
Figure 3.4 – GRF5060 RF Power Amplifier.

#### 3.1.2.5 Antennas

We used two antennas in the experimental tests: one to transmit the interference signal and the second one for the monitoring system.

We selected two different types of antennas for the tests: horn and omnidirectional antennas. Both cover the Wi-Fi frequency bands as described below.

- Double ridge guide horn antenna, SAS-571 model (Figure 3.5a). It is a directional antenna, whose frequency band ranges from 700 MHz to 18 GHz.
- EM-6116 omnidirectional antenna (Figure 3.5b). This omnidirectional antenna has a frequency range from 2 GHz to 10 GHz.



(a) (b)

Figure 3.5 – Types of antennas used; (a) Double ridge guide horn antenna, (b) EM-6116 omnidirectional antenna.

## 3.1.3 Experimental setup

### 3.1.3.1 Equipment setup

The general scheme of the experimental setup is shown in Figure 3.6. It is comprised of a monitoring system, an interference system and an IEEE 802.11n test network.

All the experiments were carried out in a semi-anechoic chamber at the University of Lille 1, which provides a multipath-free and interference-free environment. The semi-anechoic chamber is 7 m x 7 m x 3 m and it is efficient for frequencies from 100 MHz to 10 GHz. Inside the chamber, we placed the test network, the transmitting antenna of the interference signal, the monitoring antenna and another computer. This computer was used in some tests to capture the network traffic by Wireshark.

#### 3.1.3.1.1 The monitoring system

is comprised of an oscilloscope and an antenna in order to measure the IEEE 802.11n communication signal power and the interference signal power. We carried out the acquisition in the time domain with the oscilloscope and a sampling rate of 10 Gsamples/s. The time domain data is used to calculate the average power of the signals together with the spectrogram.

#### 3.1.3.1.2 The interference system

is composed by the AWG signal generator connected to the variable attenuator in order to modify the output power transmitted by the antenna. An antenna was used to

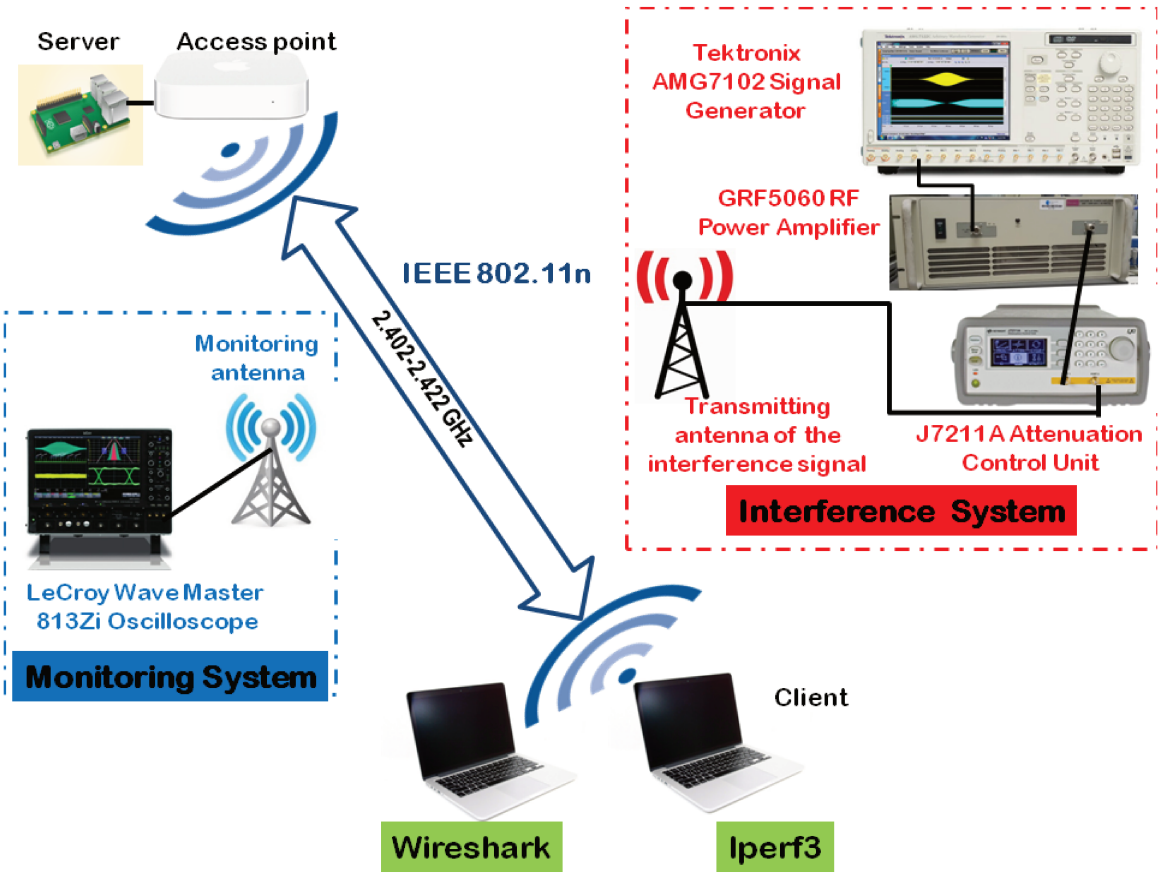



Figure 3.6 – The general scheme of the experimental setup, including the monitoring system, the interference system, and the IEEE 802.11n test network.

radiate the interference signal. One can note, in Figure 3.6, the presence of the power amplifier connected to the attenuator input. However, the amplifier was not used for all the tests.

#### 3.1.3.1.3 The test network

includes: an access point (AirPort Express), a server (Raspberry Pi), and a client (computer Macbook Pro) using TCP/IP protocol (IPv4) with Macintosh network operating system.

The access point uses a wireless connection (IEEE 802.11n) with the computer and an Ethernet connection (IEEE 802.3u) with the server.

The channel used by the IEEE 802.11n test network is centred at 2.412 MHz and the occupied bandwidth of the data is 20 MHz.

The server is a Raspberry Pi 2 Model B quad-core ARM Cortex-A7 900MHz with an Ethernet port. The computer is a Macbook Pro with Intel Core i7 2.9 GHz and 8 GB of memory, using AirPort Extreme Wireless Network Card. The IEEE 802.11n standard can use an MCS index up to 15 in the 2.4 GHz frequency band, according to the standard specifications presented in Table 1.2. The modulation type is 64− QAM with a coding rate of 5/6 and, considering 800 ns guard band interval for the OFDM symbols transmission. It delivers a maximum data rate of 130 Mbps. However, for a short guard band interval (400 ns), the maximum data rate is 144.4 Mbps.

Nevertheless, the Ethernet connection between the server and the access point limits the bit rate to 100 Mbps. As a result, the traffic between the client and server machines generated using the iPerf3 utility will be at 100 Mbps as a maximum bit rate.

#### 3.1.3.2 Measurement Setup

As mentioned before, the objective of the experimental tests is to assess the impact of the interference signal on the communication network performance. Therefore, we selected the interference signal power as a variable parameter in experimental tests. Thus, we defined the *Interference to Signal Power Ratio* (ISR) as one of the measurement parameters.

##### 3.1.3.2.1 Interference to Signal Power Ratio.

Interference to signal power ratio at the receiver mainly determines the degree to which interference will be able to affect the transmission quality [Poi11b]. ISR can be expressed as:

$$\mathrm{ISR} = \frac{\mathrm{P}_I}{\mathrm{P}_S}, \tag{3.1}$$

where $\mathrm{P}_I$ is the interference signal power and $\mathrm{P}_S$ is the IEEE 802.11n communication signal power, which are indicative power values. $\mathrm{P}_I$ and $\mathrm{P}_S$ are obtained from the

oscilloscope measurements, which are performed over 500 $\mu s$ time windows.

In a first step, the Wi-Fi communication is activated and the data of several 500 $\mu s$ time windows are collected. The power contained in each time window is calculated. $P_S$ is the average value between power values obtained from ten time windows. It can be expressed as:

$$P_S = \frac{1}{10} \sum_{j=1}^{10} \frac{1}{N} \sum_{i=1}^{N} \frac{x_j^2(i)}{Z} \tag{3.2}$$

where $x_j$ is the signal of the time window $j$, $i$ is the sample index, $Z$ is the oscilloscope input impedance, and $N$ is the number of samples or length of the vector $x$. This latter parameter is obtained as $N = f_s \times w$; $f_s$ is the sampling rate and $w$ is the duration of the time window.

The same process is applied to measure $P_I$. The interference signal is generated (without communication) and a single 500 $\mu s$ time window is collected to calculate the normalized power $P_I$.

## 3.2 Frequency sweeping jamming

This section presents the first experiment corresponding to the study of the impact of frequency sweeping jamming signals on the performance of IEEE 802.11n communications. The aim is to analyze the susceptibility of *Orthogonal Frequency Division Multiplexing* (OFDM) signals and to understand how some parameters of the frequency sweeping jamming act on the degradation of the achieved bit rate, taking into account the signal processing performed by the OFDM receiver.

### 3.2.1 Signal Parameters

We studied the impact of the frequency sweeping jamming signal on the communication quality degradation according to the interference to signal power ratio (ISR) and the sweep period (SP).

#### 3.2.1.1 Interference to signal power ratio (ISR)

As defined in Equation 3.1, the ISR is determined by the interference signal power and communication signal power. In order to evaluate the effect of different ISR levels on the achieved bit rate, we varied the ISR by modifying the interference signal power by means of the variable attenuator.

#### 3.2.1.2 Sweep Period (SP)

The sweep period was already defined in the previous chapter and it was highlighted as one of the key parameters of the frequency sweeping jamming signals.

We considered several SP values in our study, ranging from 0.5 $\mu s$ to 50 $\mu s$. Moreover, some of them are defined with respect to the parameter $T_u$ which is the duration of the useful part of the OFDM symbol. It is worth reminding that $T_u = \frac{1}{\Delta f} = 3.2\ \mu s$.

Thus, SP values are 50 $\mu s$, 40 $\mu s$, 30 $\mu s$, 20 $\mu s$, 10 $\mu s$, $\frac{1}{0.5\Delta f} = 6.4\ \mu s$, 5.5 $\mu s$, $\frac{1}{2\Delta f} = 1.6\ \mu s$, $\frac{1}{3\Delta f} \approx 1.06\ \mu s$, $\frac{1}{4\Delta f} = 0.8\ \mu s$, $\frac{1}{5\Delta f} = 0.64\ \mu s$, $\frac{1}{6\Delta f} \approx 0.53\ \mu s$, $\frac{1}{7\Delta f} \approx 0.45\ \mu s$.

### 3.2.2 Experimental setup

The experiments were presented in general terms in section 3.1.3. Now, we present the specificities of the experimental setup used to assess the impact of frequency sweeping jamming on the IEEE 802.11n communication network.

The scheme of the experimental setup is presented in Figure 3.7. Note that we employed two horn antennas, one as transmitting antenna of the interference and another as monitoring antenna. Due to their high directivity, both antennas are oriented in the direction of the center of the line of sight between the client and the access point as is shown in Figure 3.8.

Both antennas have been placed on either sides of the axis between the access point and the client (computer). The exact locations of the equipment inside the semi-anechoic chamber are illustrated in Figure 3.9.

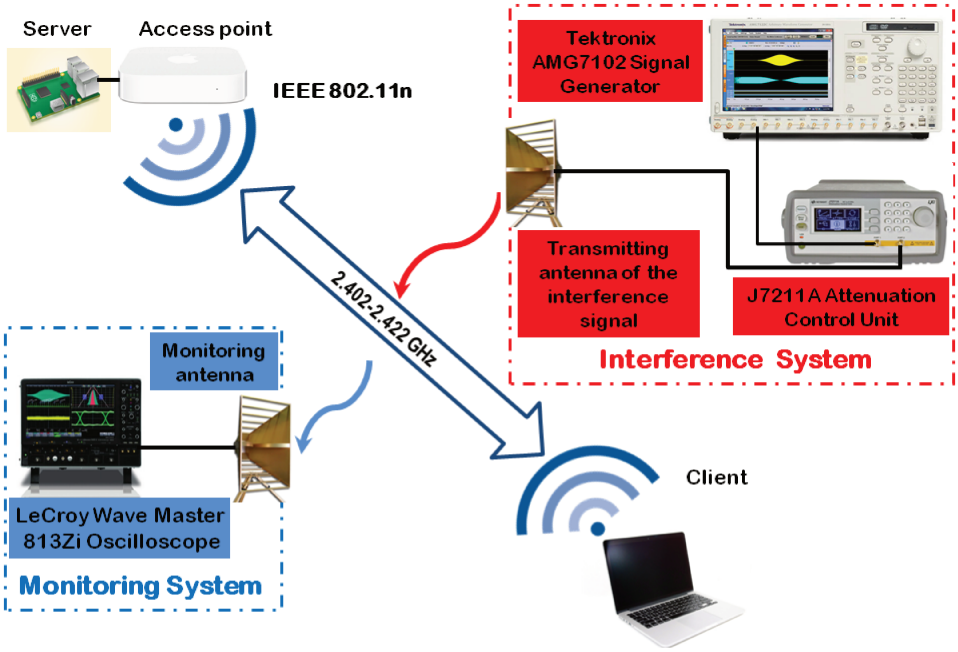



Figure 3.7 – The scheme of the experimental setup, including: the monitoring system, the interference system, and the test network.

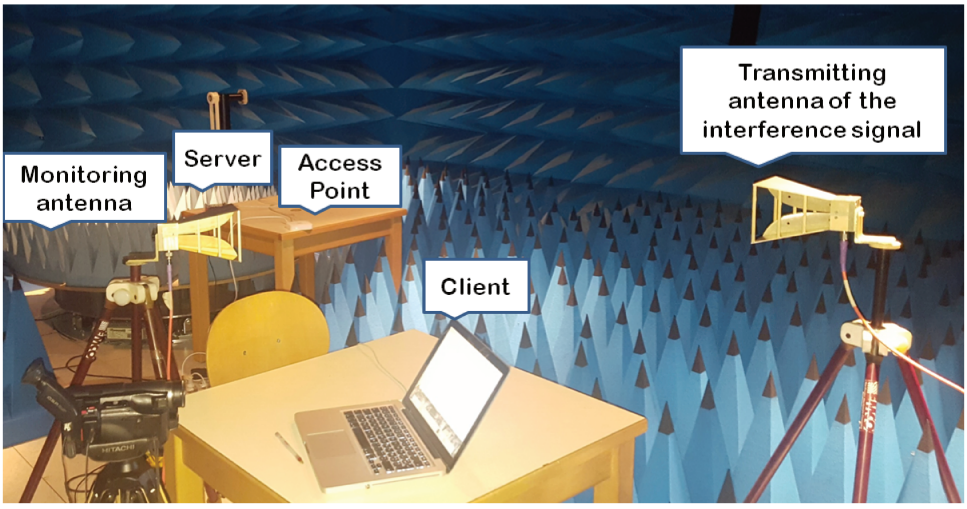



Figure 3.8 – Experimental setup in the semi-anechoic chamber.

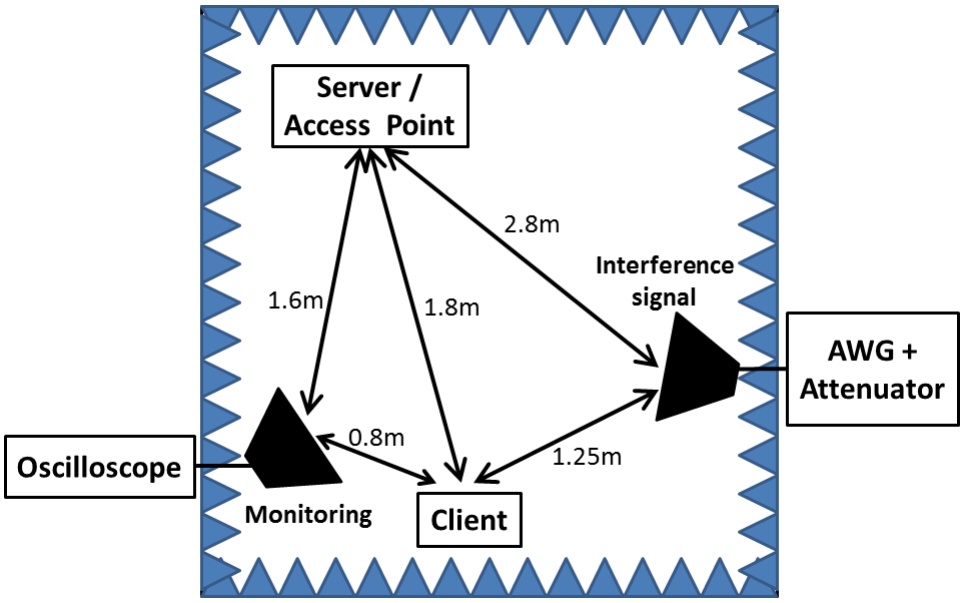



Figure 3.9 – Location diagram of the equipment inside the semi-anechoic chamber.

### 3.2.3 Measurement results

To perform measurements according to the parameters and setups already described, we selected an interference signal with a defined SP and we varied the ISR step by step, by increasing the interference signal power. Starting from a value of -40 dB, the ISR was increased until the communication was interrupted, meaning that the measured bit rate reached zero. For each tested value of the ISR, we measured the average bit rate resulting from ten outcomes, by means of the iPerf3 program. This procedure was repeated for each SP.

The bit rate measurements obtained for the 13 different SP values specified in section 3.2.1.2 are reported in Figure 3.10. For each applied SP, the achieved bit rate is given as a function of the ISR. We observed a varying impact of the ISR on the system performance.

For instance, for an ISR lower than -26 dB and whatever the SP value, we observed that the system performance is not affected (i.e., the bit rate is nearly 95 Mbps). However, for an ISR bigger than -26 dB, the bit rate is affected and the loss depends on the SP of the interference signal. For instance, at an ISR of -20 dB, the bit rate can be 0

bps for a SP of 20 $\mu s$ or can reach the maximum rate for a SP of 0.45 $\mu s$.

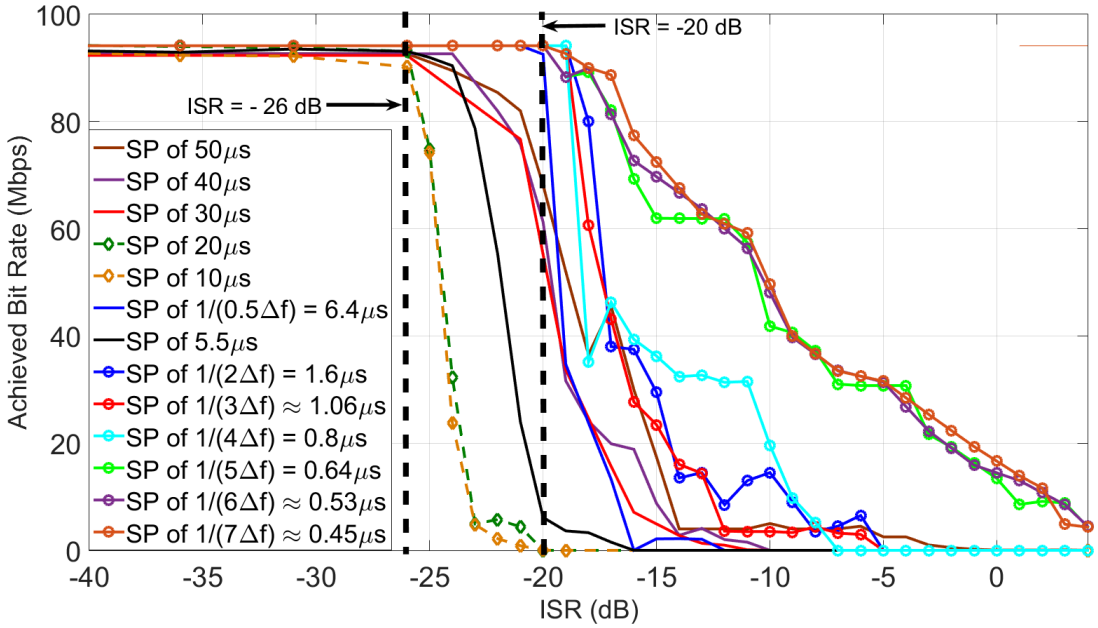



Figure 3.10 – Bit Rate measurements, as a function of the ISR.

To further assess the results obtained in Figure 3.10, we present, in Figure3.11, the minimum level of ISR required to lose the communication (i.e., the achieved bit rate is 0 bps), as a function of the SP.

We distinguish three areas in Figure 3.11. For areas A and B, the impact of the interference signal is weak, i.e., a high level of ISR is necessary to interrupt the communication. Area A concerns small SP values, ranging from 0.45 $\mu s$ to 6.4 $\mu s$, whereas area B concerns higher SP values, ranging from 20 $\mu s$ to 50 $\mu s$. Between these two value ranges, we find area C where the interference signal is the most efficient to corrupt the communication. The interpretation of these observations will be provided in the following section.

Finally, we can observe, in Figure 3.11, that, depending on the SP, the ISR value permitting the communication interruption can vary by around 30 dB.

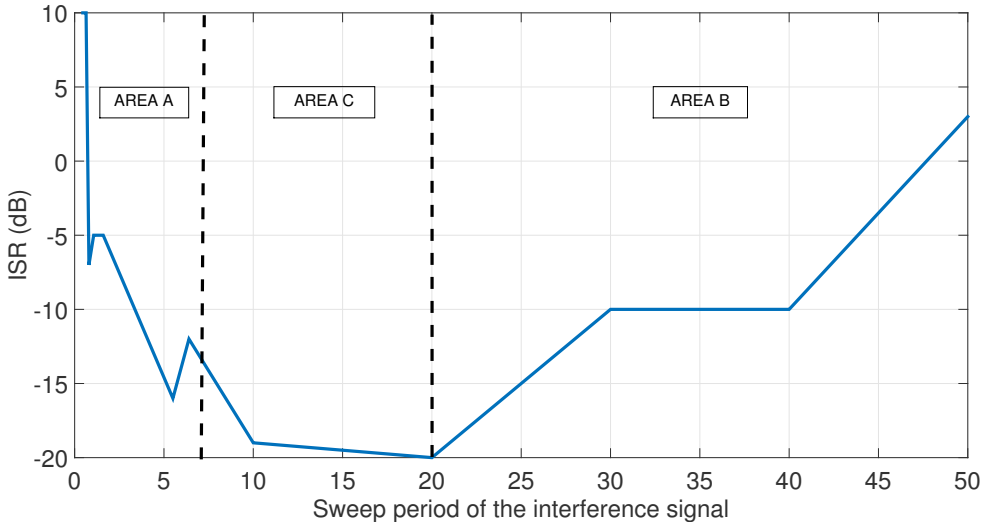



Figure 3.11 – Required value of the ISR to completely interrupt the communication, as a function of the SP.

### 3.2.4 Interpretation of the measurements

This section presents the interpretation of the results of Figure 3.10 and Figure 3.11. We analyzed the results based on the spectrum of the interference signal obtained at the receiver stage and on the *Clear Channel Assessment* (CCA) induced by the interference signal.

#### 3.2.4.1 Observations based on the spectrum

**Interpretation for area A.**

This area corresponds to SP values below 6 $\mu s$. Figure 3.12 presents the achieved bit rate as a function of the ISR for some interference signals with SP values corresponding to area A.

It is worth reminding the structure of an OFDM receiver. After filtering and down-conversion, the guard interval (GI) is removed and an FFT operation is performed on the 64 samples of the useful part of the received signal as is mentioned in the section corresponding to OFDM in the first chapter of this work.

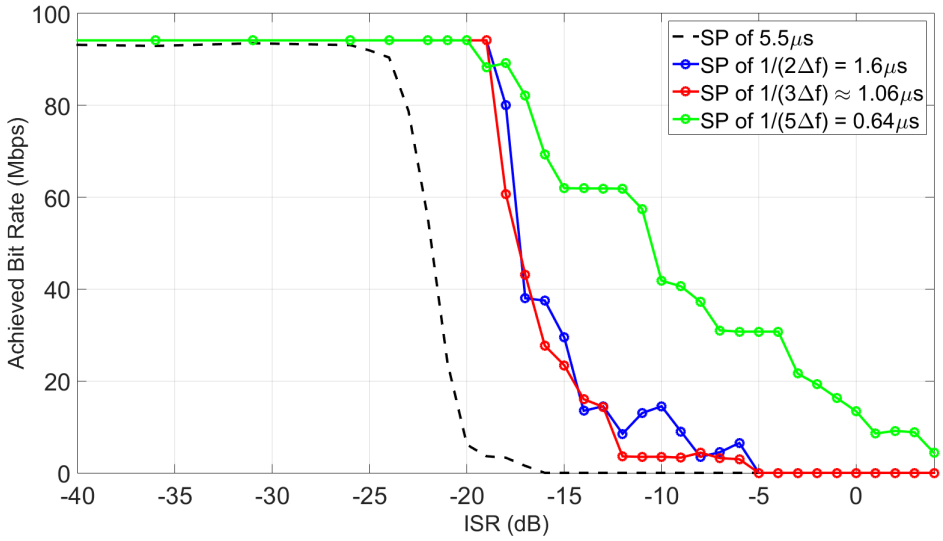



Figure 3.12 – Bit Rate measurements, as a function of the ISR for SP = 0.64, 1.06, 1.6 and 5.5 $\mu s$.

According to the OFDM receiver sampling characteristics, the 64 samples correspond to an observation time window of $T_u = 3.2\ \mu s$. At the output of the FFT, we recover a version of the transmitted data symbols on each subcarrier, corrupted by additive thermal noise as well as the interference signal. Here, the effect of the thermal noise on the achieved bit rate is negligible with respect to the frequency sweeping interference signal contribution. Afterwards, an M-ary to binary conversion is carried out, and the bits obtained are fed to the channel decoder.

Now, we will proceed in two steps for the interpretation of the results.

Firstly, we will analyze how the interference signal is transformed by the FFT operation, in order to assess its impact on the data symbols transmitted over the subcarriers.

Secondly, the effect of the interference signal on the channel decoder behavior will be analyzed.

The interference signal is generated by Matlab at a sampling of 10 Gsamples/s.

To observe the frequency sweeping interference signal in a similar way as the OFDM receiver, the FFT has to be applied on a number of samples which corresponds to a $T_u = 3.2\ \mu s$-observation time window. With a 10 GHz sampling frequency, this corresponds to 32000 samples. Then, a 32768-point FFT is applied.

Figure 3.13 shows the FFT results for the SP of $\frac{1}{5\Delta f} = 0.64\ \mu s$, $\frac{1}{3\Delta f} \approx 1.06\ \mu s$, $\frac{1}{2\Delta f} = 1.6\ \mu s$, and $5.5\ \mu s$.

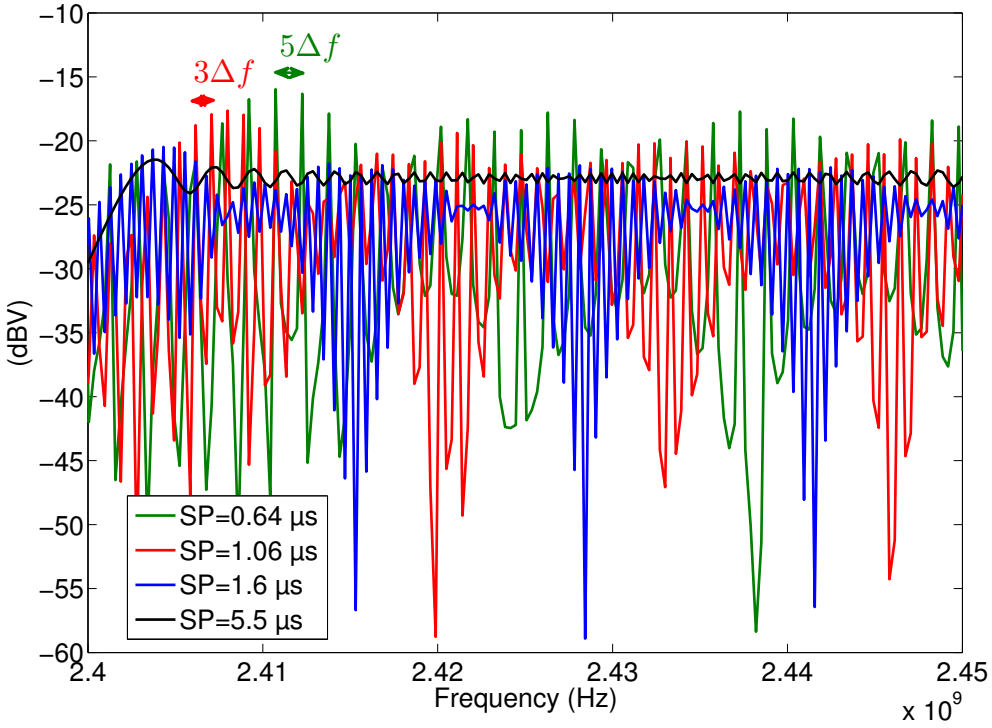



Figure 3.13 – Spectra of the frequency sweeping interference signals obtained by FFT over a 3.2 $\mu s$ window, for SP = 0.64, 1.06, 1.6 and 5.5 $\mu s$, between 2.4 GHz and 2.45 GHz.

Let us recall that the interference signal $i(t)$ (Equation 2.3) is a periodic signal with a period of SP . This means that its frequency representation is a train of impulses spaced by $\frac{1}{SP}$ and convolved by a sinc function with a main lobe width of $\frac{1}{T_u} = \Delta f$.

The impulsive structure clearly appears for the SP of $\frac{1}{5\Delta f}$ and $\frac{1}{3\Delta f}$. When the SP increases, the impulses are closer, and the convolution with the sinc flattens the curve, thus attenuating the impulsive structure, as observed in Figure 3.13.

This impulsive structure explains the general trend for the left side of area A: the interference signal is less efficient when the SP decreases. Indeed, for an SP of $\frac{1}{5\Delta f}$, only one subcarrier out of 5 can be struck by the interference, whereas for an SP of $\frac{1}{3\Delta f}$, only one subcarrier out of 3 can be struck by the interference. Hence, when the SP decreases, fewer OFDM subcarriers are struck. Let us now explain the impact on the channel decoder.

From the error-correction decoding standpoint, the channel encoder in IEEE 802.11n is either a Binary Convolutional Code (BCC) or a Low Density Parity Check (LDPC) code. It is known that channel decoders in general, and especially the Viterbi algorithm [Ber10] used for the decoding of convolutional codes, yield better error-rate decoding performances when detection errors are isolated at the input of the decoder, compared to concatenated or burst errors. This is due to the inherent trellis-tracing nature of this algorithm that can better correct isolated errors, in contrast to burst errors that make the algorithm diverge from the optimal code-word path.

For the same overall interference power, when SP decreases, the number of corrupted OFDM subcarriers is lowered, which in turn increases the average time spacing between bit errors at the input of the Viterbi decoder. The same reasoning applies for the Sum-Product algorithm [Hay09] used for LDPC decoding. More insight on the influence of errors' proximity on the performance of error-decoding algorithms can be found in [Hay09] with practical examples.

When the impulsive structure of the interference signal is attenuated, i.e., from SP = 1.6 $\mu s$, every subcarrier is struck by the interference signal. What explains the stronger impact for SP = 5.5 $\mu s$ compared to 1.6 $\mu s$ is the spectrum amplitude level which is 3 dB higher. Thus, the system behavior corresponding to the left side of area A is explained by the difference in ISR level per subcarrier.

**Interpretation for area B.**

This area corresponds to SP values greater than 20 $\mu s$. Figure 3.14 presents the achieved bit rate as a function of the ISR for the interference signals with SP corre-

sponding to area B.

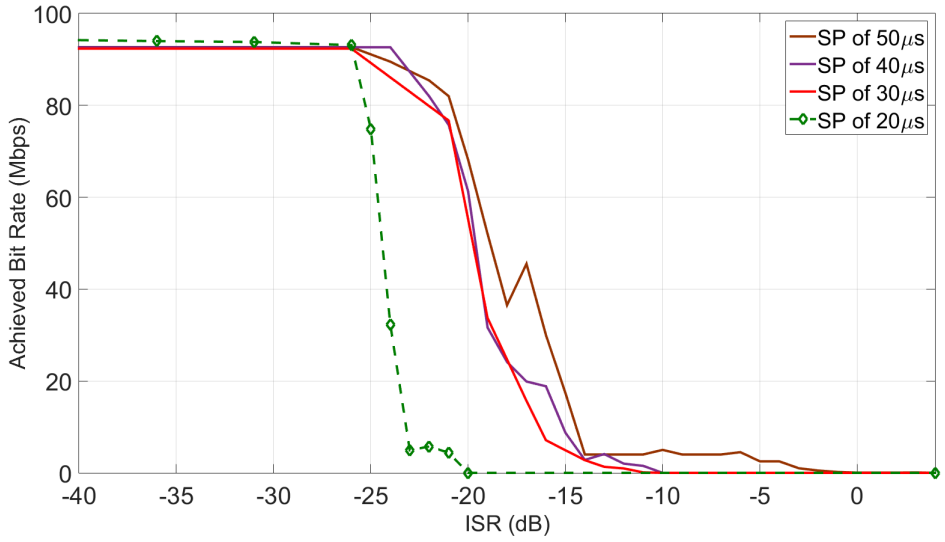



Figure 3.14 – Bit Rate measurements, as a function of the ISR for SP = 20, 30, 40 and 50$\mu s$.

In area B, the impact of the interference on the communication quality degradation decreases with the SP increase. To understand this evolution, we applied an FFT to the interference signal, for SP values varying between 20 $\mu s$ and 50 $\mu s$. We also applied a 32,768-point FFT, corresponding approximately to a window of 3.2 $\mu s = \frac{1}{\Delta f}$, to be in agreement with the post-processing performed at the reception stage. The results are presented in Figure 3.15. The 3.2 $\mu s$ time window being inferior to the SP, the spectrum obtained by the FFT covers only a portion of the 2.4 GHz - 2.5 GHz frequency band.

When we compare the frequency band covered by the frequency sweeping interference signal in a 3.2 $\mu s$ time window, with the bandwidth of the Wi-Fi channel, we notice that the interference signal can affect only a portion of the Wi-Fi channel.

A Wi-Fi channel is composed of 64 subcarriers, including 52 active subcarriers and 6 guard subcarriers. Knowing that they are spaced by 312.5 kHz, the real bandwidth of a channel is 17.5 MHz. So, only the 20 $\mu s$-frequency sweeping signal is able to disturb the communication significantly. In the case of perfect time and frequency superpositions of

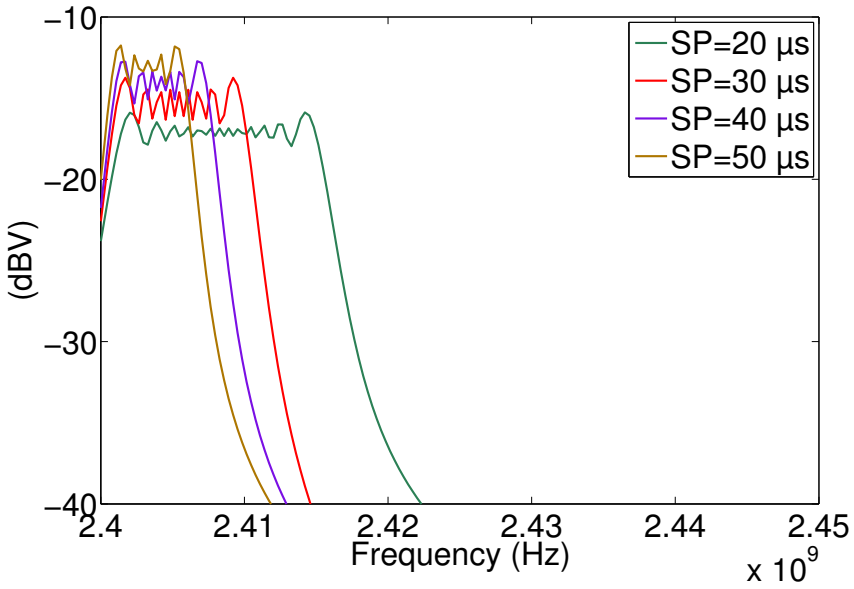



Figure 3.15 – Spectra of the frequency sweeping signals obtained by FFT over a 3.2 $\mu s$ window, for SP = 20, 30, 40 and 50$\mu s$.

the communication signal with the interference signal, nearly all the active subcarriers can be corrupted and a full OFDM symbol can be lost.

Nevertheless, for higher SP values, only a part of the OFDM symbol can be disturbed. As a consequence, the more the SP increases, the more errors are isolated at the channel decoder input, since they are spread all over the sequence by the channel interleaver, and a better error-rate decoding performance can be achieved.

Finally, due to the interference signal scanning a 100 MHz frequency band and the instantaneous frequency bandwidth of the interference signal decreasing with the SP, the probability that the interference covers the used Wi-Fi channel decreases when the SP increases. We can then understand the increase in the ISR curve when the SP increases in area B in Figure 3.11.

**Interpretation for area C.**

Now, to understand the results observed in area C, we focus on the case with SP between 6.4 $\mu s$ and 30 $\mu s$ that is shown in Figure 3.16.

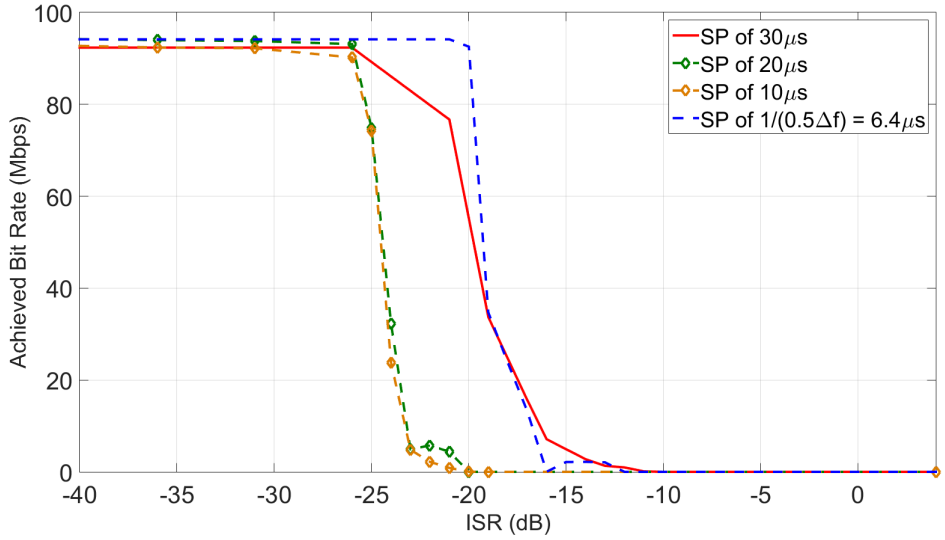



Figure 3.16 – Bit Rate measurements, as a function of the ISR for SP = 6.4, 10, 20 and 30 $\mu s$.

To assess the results observed in area C, we applied again an FFT with a 3.2 $\mu s$ time window on different interference signals, for SP between 6.4 $\mu s$ and 30 $\mu s$.

Figure 3.17 presents the bandwidth covered by the different interference signals, for a 3.2 $\mu s$-observation time window. Note that the bandwidth covered decreases when the SP increases, as in area B. Therefore, the quickest SP insures a higher probability to cover the Wi-Fi channel used.

Nevertheless, according to Figure 3.11, the more disturbing signals in the overall SP range from 0 $\mu s$ up to 50 $\mu s$, are obtained for SP of 10 $\mu s$ and 20 $\mu s$. This means that another factor acts on the degradation of the communication quality. Therefore, we have also to take into consideration the level of the interference signal, which also depends on the digital signal processing involved at the reception [Gro14].

Indeed, Figure 3.17 shows how the power level significantly increases in the area of

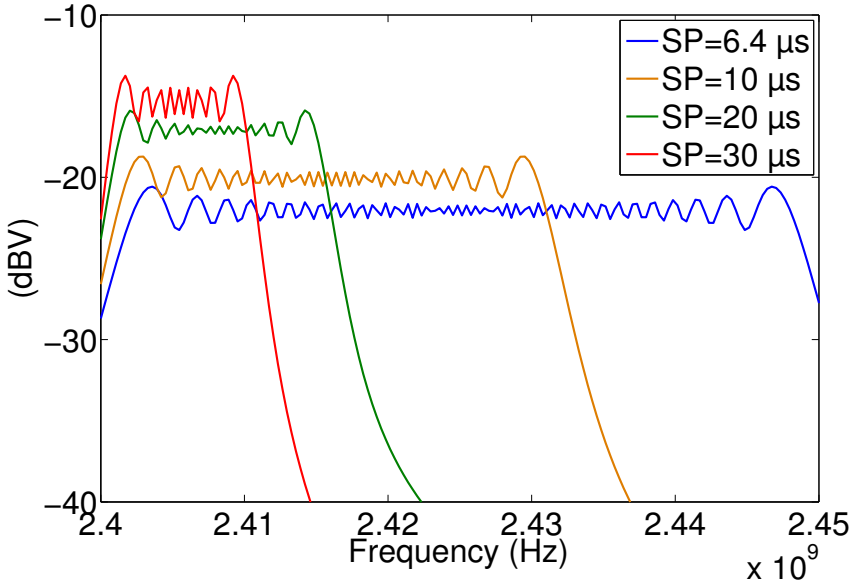



Figure 3.17 – Spectra of the frequency sweeping signals obtained by FFT over a 3.2 $\mu s$ window, for SP = 6.4, 10, 20 and 30 $\mu s$.

concern when the SP increases. The power level for a 6.4 $\mu s$ sweep period is respectively 3 and 6 dB inferior to the power levels for 10 $\mu s$ and 20 $\mu s$ sweep periods. Hence, the capacity to corrupt the communication is a combination of the covered frequency band and the power level obtained by the signal processing at the reception.

#### 3.2.4.2 Observations based on the CCA

As explained in the section 1.5 in the first chapter, a station needs to enable the CS mechanisms to determine the state of the medium over the DIFS period, before being able to use the channel. The CS mechanisms performed by the PHY layer measure the energy observed at the antenna through CCA (*Clear Channel Assessment*); either through the energy measurement of the PLCP preamble (CS/CCA) or by the energy detection (CCA-ED).

The energy measured during the reception of the PLCP preamble (CS/CCA) is specified as RSSI (*Received Signal Strength Indicator*). Thus, RSSI is a parameter that indicates the RF energy received by the OFDM PHY.

When the CCA reaches a given level [Sta12, p. 1746], the station considers the channel as being occupied. The algorithm to obtain the CCA is not well detailed in the standard. However, the CCA is specified as the average power measured on the 20 MHz channel of interest and with a maximum time window of 4 $\mu s$ [Sta12, p. 1623], which corresponds to an OFDM symbol duration plus the guard period.

After applying the frequency sweeping jamming signal in the absence of the Wi-Fi signal, we measured the interference signal for different SP values by using the monitoring antenna and the oscilloscope and then we calculated the evolution of the average power over the channel. For this purpose, we performed a *Short Time Fourier Transform* (STFT) with a rectangular window which allows us to exactly apply a 4 $\mu s$ time window:

$$X(i,f) = \sum_{n=-\infty}^{+\infty} s(n)w(n-iR)\exp\left[-j2\pi fn/F_s\right], \tag{3.3}$$

where $f$ is the frequency in Hz, $w(n)$ is a windowing function of length $W$, $R$ is the hop size, in samples, of the window $w(n)$, for the successive estimations of the STFT. The signal measured by the oscilloscope, with a sampling frequency $F_s = 10$ Gsamples/s, is called $s(n)$, where $n$ is the index of the samples. $s(n)$ is the measured signal, comprising the interference signal and the additive noise. Equation 3.3 is applied as follow. First, the DFT (Discrete Fourier Transform) of the signal is calculated using Equation 3.4:

$$\bar{x}(n,f) = \exp\left[-j2\pi fn/F_s\right] s(n). \tag{3.4}$$

Then, the application of a 4 $\mu s$ rectangular time window is carried out using:

$$X(i,f) = \frac{\sum_{n=iR}^{iR+W-1} \bar{x}(n,f)}{W}, \tag{3.5}$$

where $W = 40000$ is the number of samples in the 4 $\mu s$ time window.

Finally, Equation 3.6 allows us to calculate $P_{avg}$, the average power over the channel, as a function of the window shift:

$$P_{avg}(i) = \frac{\sum_{f=f_{start}}^{f_{stop}} |X(i,f)|^2}{N_f \cdot Z}, \tag{3.6}$$

where $f_{start} = 2.402$ GHz and $f_{stop} = 2.422$ GHz are respectively the start and end frequencies of the channel, $Z$ is the oscilloscope input impedance and $N_f$ is the number of frequency steps.

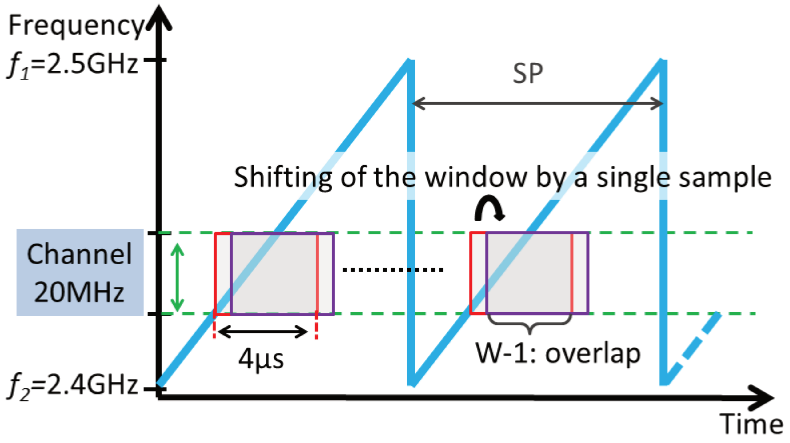



Figure 3.18 – Illustration of the STFT processing.

Figure 3.18 shows how the time evolution of the average power over the channel is calculated with a shifting window. A maximum overlap of $(W-1)$ samples between the successive 4 $\mu s$ time windows is applied, i.e., $R = 1$ in Equation 3.3.

The window is shifted over a 100 $\mu s$ duration of the $s(n)$ signal. The highest value of the average power obtained over the 100 $\mu s$ duration is plotted in Figure 3.19 as a function of the SP.

Figure 3.19 shows that the highest value of the average power increases with the SP until the value of 20 $\mu s$ is reached, starting from which this power becomes constant.

Therefore, the highest value of this power is obtained with a SP superior or equal to 20 $\mu s$. Consequently, the CCA threshold defining an occupied channel is more easily reached with a 20 $\mu s$ sweep period due to the induced average power and to the more frequent passage of the interference signal on the channel in relation to the superior SP. This justifies the fact that a 20 $\mu s$ sweep period corresponds to the worst case in Figure 3.11.

In a more concrete environment, a similar curve to the one given in Figure 3.19 would be obtained, with the same behavior, but with different power values due to multipath interferences, additive background noise, and different transmission parameters related to the receiving antenna gain.

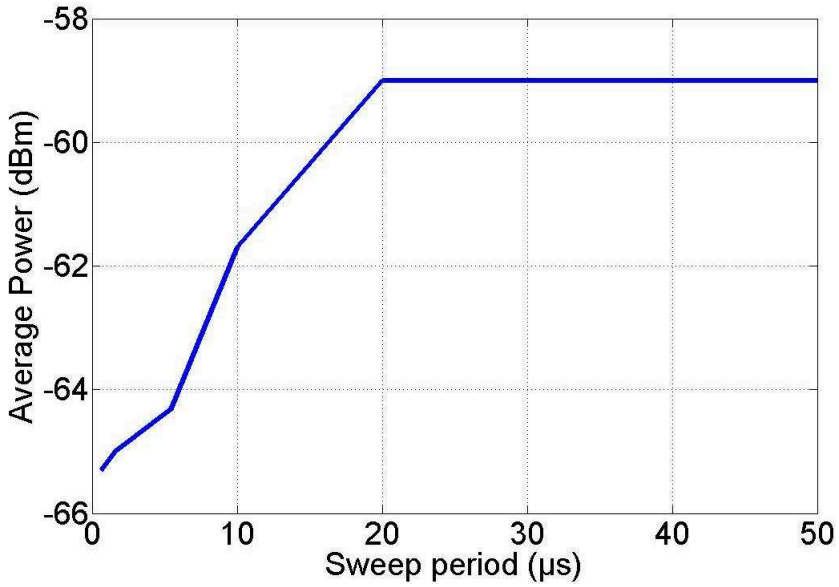



Figure 3.19 – Highest average power over the 20 MHz communication channel for different sweep periods.

Finally, it should be noted that the average power simultaneously depends on the SP and the time window duration applied at the receiver stage. Indeed, a 20 $\mu s$ sweep period is the worst case that corresponds to the particular case of a 4 $\mu s$ time window at the reception signal processing stage. This is further illustrated by Figure 3.20.

In Figure 3.20, we observe that, with a SP smaller than 20 $\mu s$, the interference signal does not cover the whole 4 $\mu s$ time window when the 20 MHz channel bandwidth is considered. For example, if SP = 10 $\mu s$ (green curve), the interference signal lies within the 20 MHz channel bandwidth only during 2 $\mu s$. This means that half the interference power is lost. This 3 dB power loss can also be observed in Figure 3.19 for a SP of 10 $\mu s$ compared to SP $>$ 20 $\mu s$.

Moreover, while we focused our analysis on the Physical layer, it should be noted that the MAC layer characteristics can also contribute to the justification of the most aggressive SP. Indeed, for the 802.11n, the minimum medium idle time, or DIFS, is 28 $\mu s$. WLAN stations can access the medium if the 20 MHz channel is free for a time

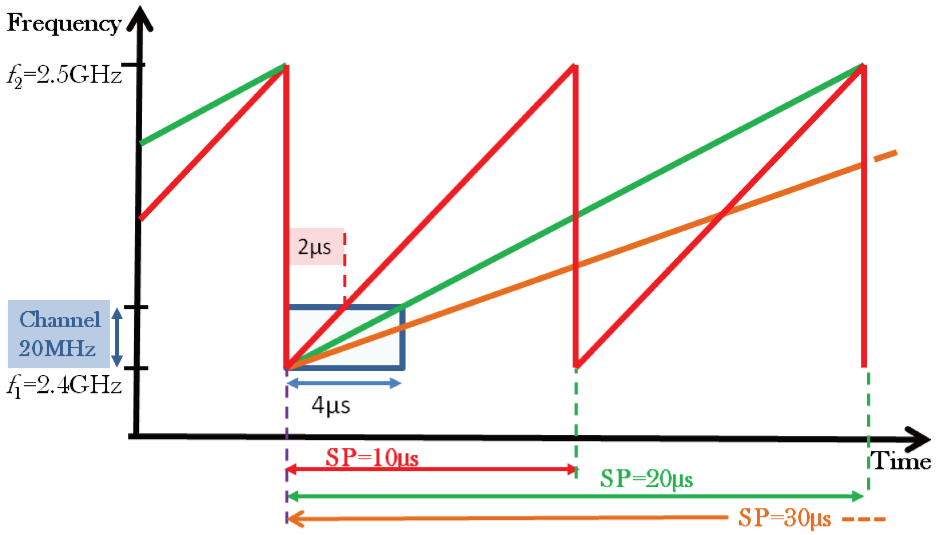



Figure 3.20 – Illustration of the relationship between the sweep period and the signal processing time window used for average power measurement at the reception.

period longer than the DIFS value. Consequently, the channels' access can be more problematic for a SP lower than the DIFS [PIK11, LPA+16]. Besides, with a 20 $\mu s$ sweep period, the DIFS period is systematically affected, but with an interference power level superior to those induced by smaller values of the SP. This can further explain the worst system behavior with a SP of 20 $\mu s$.

### 3.2.5 Conclusions on frequency sweeping jamming

This research presented a study of a frequency sweeping interference signal in order to analyze its impact on a IEEE 802.11n communication, using a practical experimental setup. As a perturbation strategy, we varied the sweep period and ISR values. The experimental results were analyzed from different perspectives: signal processing at the reception stage, error-correcting coding and network access.

The study aims at identifying the most harmful interference factors on the Wi-Fi communication, with the goal of paving the way for the design of a receiver able to adapt itself in such a way to become resilient to this kind of interference.

We particularly noticed that the impact of the interfering signal greatly depends on

the relationship between its sweep period and the time window duration of the receiver signal process.

When the observation time window of the receiver is significantly superior to the sweep period of the interfering signal, the perceived interference appears as a train of impulses that can only affect some subcarriers and, thus, the degradation of the communication is reduced. This means that, by adapting the width of the observation time windows of the reception stage, we could reduce the impact of the interference signal.

We also demonstrated that the most disturbing interference signal is the one which induces the highest value of the average power for the 20 MHz channel with the minimum sweep period. This average power also depends on the time window of the receiver processing. These observations can also constitute the design basis of resource allocation techniques for wireless communication systems, in such a way to allocate subcarriers to users so as to enhance their robustness to intentional interferences, by efficiently exploiting frequency diversity.

## 3.3 Transient EM interferences

This section presents the second experiment corresponding to the study of the impact of the transient EM interferences generated by contact losses between the catenary and the pantograph on the performance of an IEEE 802.11n communication. The goal is to study the relation between the DIFS period and the repetition period of these transient signals on the degradation of the achieved bit rate.

### 3.3.1 Signal Parameters

For this experiment, we studied two transient EM interference signal parameters: its repetition period and power level.

#### 3.3.1.1 Repetition period (T)

The repetition period (T) is one characteristic of the transient EM interference signal, as defined in section 2.1.3. T indicates the repetition interval between successive transients. According to [JK17], the occurrence of transient interferences increases with

the train speed.

In order to study the repetition interval between successive transients over the IEEE 802.11n performance, we varied the repetition period T by the AWG.

The values of T were defined in taking into account the values presented in [SDR+09].

#### 3.3.1.2 Interference to signal power ratio (ISR)

To calculate Interference to Signal ratio, the powers of the interference and communication signals are obtained by Equation 3.2.

Because the interference signals are transient, the power obtained for the interference signal varies with the repetition period. Indeed, the number of transient signals inside a 500 $\mu s$ time window depends on T. For example, when T decreases, the number of transients in the 500 $\mu s$ time window increases, leading to an increase in the interference power.

Thus, in this second experiment, we sometimes present the results as a function of the attenuation level instead of the ISR.

### 3.3.2 Experimental setup

Figure 3.21 presents the experimental setup employed in this experiment. We located the monitoring antenna near the client in order to assess the received power similarly to those received by the client.

We used the EM-6116 omnidirectional antenna as a monitoring antenna to receive with the same gain the interference signal and the IEEE 802.11n communication signal. We employed identical antennas to monitor and to emit the interference signal, and placed it at the same height as shown in Figure 3.22.

To reach higher interference power levels, we connected the GRF5060 RF power amplifier to the generator output.

The exact locations of the equipment inside the semi-anechoic chamber are illustrated in Figure 3.23.

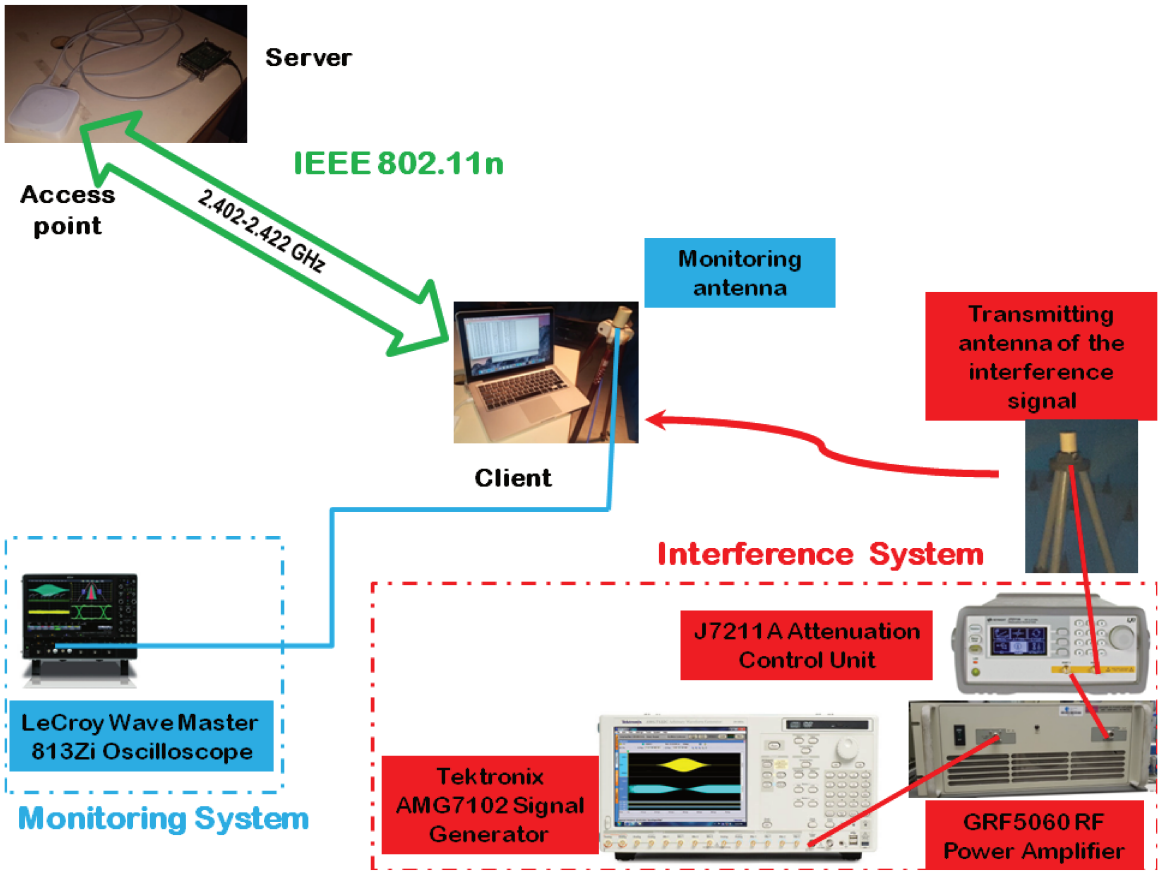



Figure 3.21 – The scheme of the experimental setup, including: the monitoring system, the interference system, and the test network.

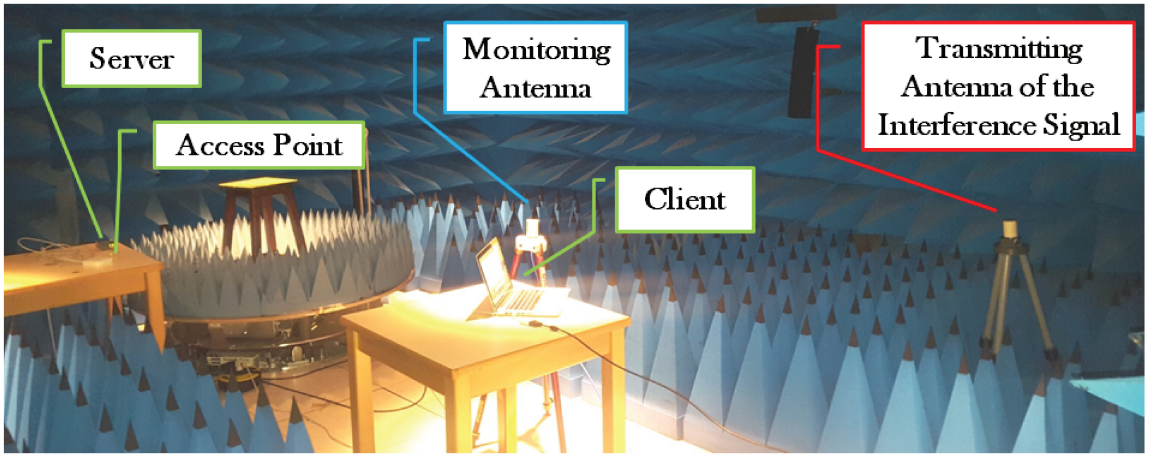



Figure 3.22 – Experimental setup in the semi-anechoic chamber.

The transmitting antenna of the interference signal has been placed on either side of the access point, while the client is in the middle. The exact locations of the equipment inside the semi-anechoic chamber are illustrated in Figure 3.9.

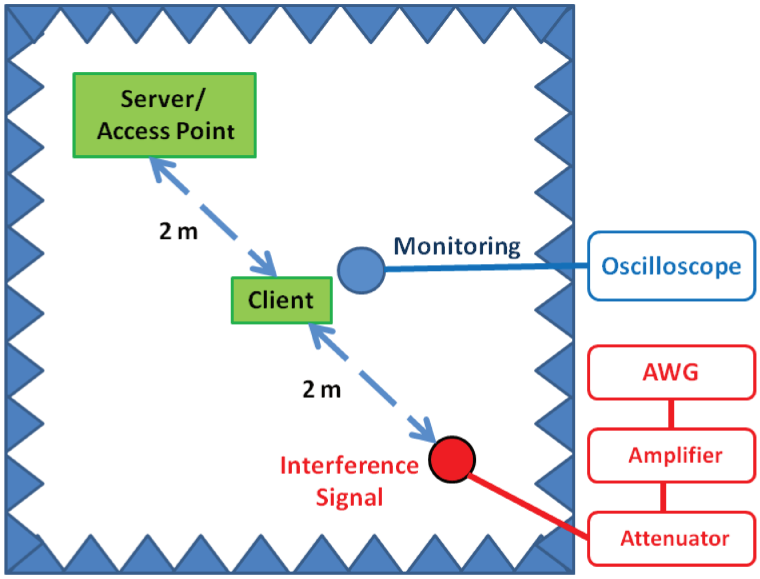



Figure 3.23 – Location diagram of the equipment inside the semi-anechoic chamber.

### 3.3.3 Measurement results

In order to study the impact of transient EM interference signals on the IEEE 802.11n communication performance, we carried out three different tests.

**For the first test**, we used an interference signal defined in section 2.1.3 (Equation 2.2), with a 10 $ns$ duration (D), 1 V voltage amplitude (A), 0.5 $ns$ and a rise time ($T_{rise}$). The repetition period (T) was decreased step by step, starting from 1000 $\mu s$ until the measurement of the bit rate reached zero, implying that the communication was interrupted.

For each applied T, we measured the maximum, mean and minimum bit rates resulting from twenty outcomes, by means of the Iperf program [Ipe] which was run on

the client side.

Figure 3.24 shows the maximum, mean and minimum bit rate measurements obtained for transient EM interference signals for each T. We observed a varying impact of T on the achieved bit rate. For T greater than 600 $\mu s$, the bit rate is not affected, the bit rate reached the maximum nearly 95 Mbps no matter the T values. When T decreases between 500 $\mu s$ and 24 $\mu s$, the achieved bit rate progressively decreased. For T = 50 $\mu s$, we observed a punctual interruption of the communication. For T = 24 $\mu s$, the communication was suddenly and definitely interrupted.

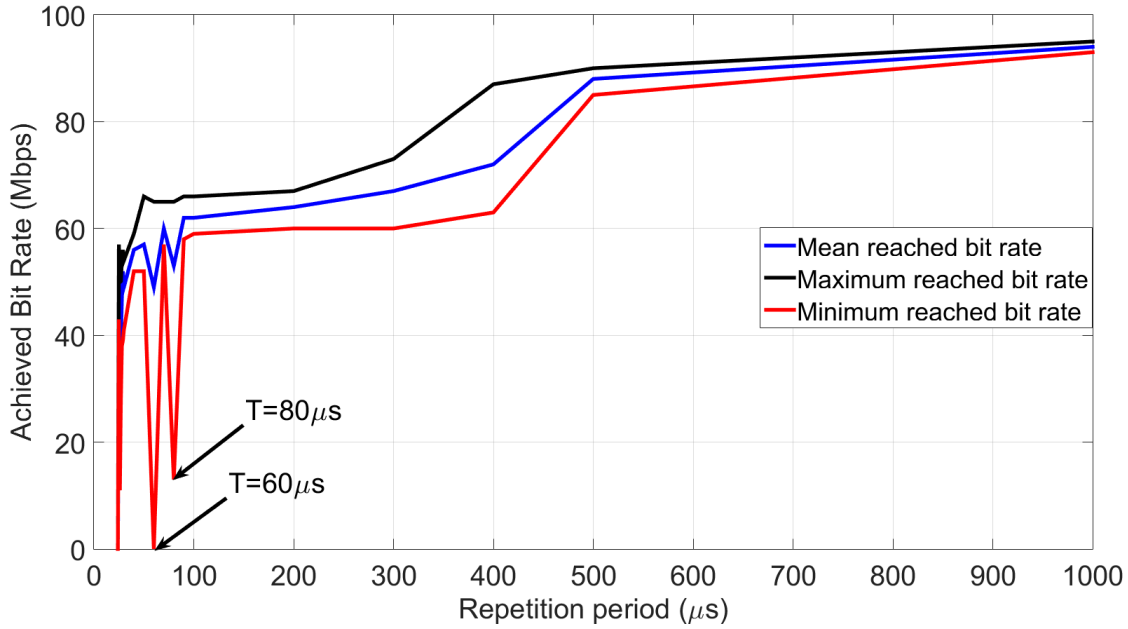



Figure 3.24 – Bit Rate measurements, as a function of the T for A = 1 V.

**For the second test**, we increased the voltage amplitude (A) and the above procedure was repeated. Figure 3.25 presents the mean bit rate achieved for transient EM interference signals for both A values (A = 1 V and A = 10 V), as a function of T. In both cases, the communication was suddenly interrupted for T = 24 $\mu s$.

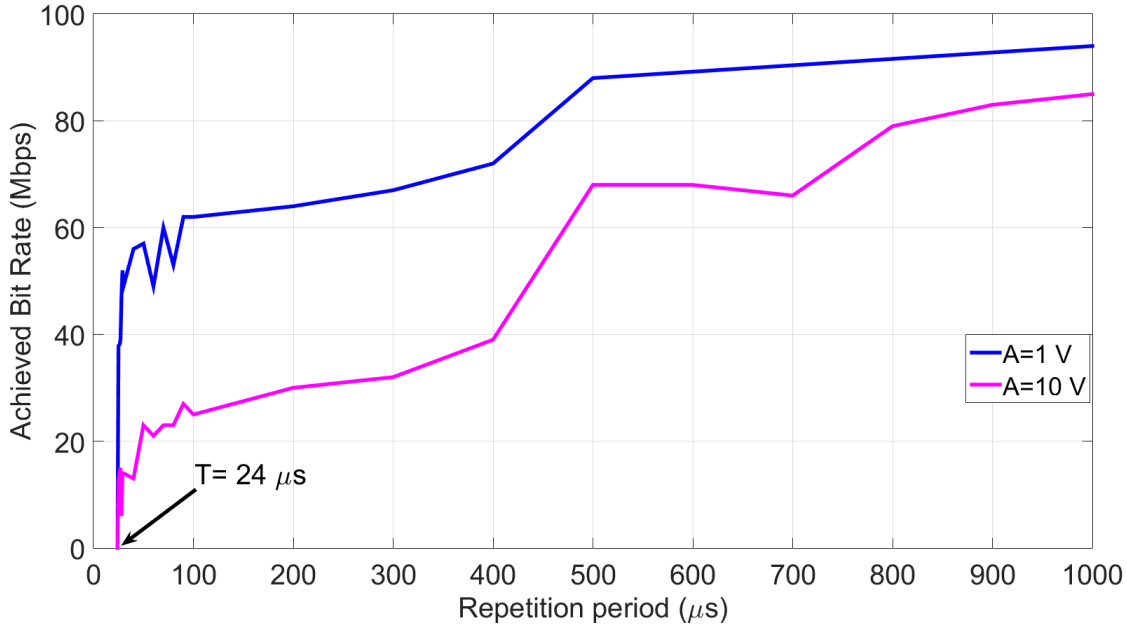



Figure 3.25 – Bit Rate measurements, as a function of the T for A = 1 V and 10 V.

**In the third test**, the mean bit rate measurements were repeated by varying the interference to signal power ratio (ISR) thanks to the variable attenuation control unit. First, we used an interference signal with a defined repetition period (T). Then, the interference signal power was increased until the bit rate reached zero. This procedure was repeated for each repetition period of 27 $\mu s$, 25 $\mu s$ and 24 $\mu s$.

Figure 3.26 presents the results. We observed a varying impact of the ISR on the communication performance. For instance, for a T equal to 25 and 27 $\mu s$, the communication was never interrupted. However, for T = 24 $\mu s$, the bit rate reached zero for ISR = -33 dB.

To study this behavior, we repeated the last test for different repetition periods starting from 25 $\mu s$ until 1 $\mu s$ that is the minimum interval permitted by AWG.

Knowing that the interference signal power varies as a function of T, the ISR also depends on T. In order to use a common metric to compare the impact of the different interference signals, we present the bit rate measurements as a function of the attenuation level applied to the interference signal.

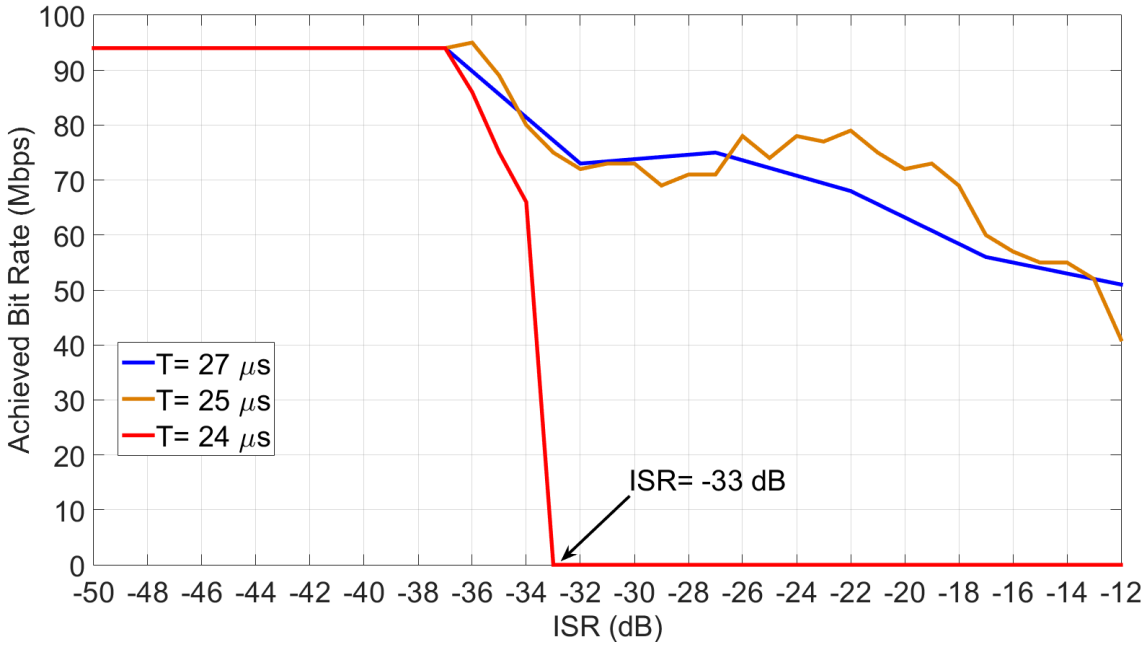



Figure 3.26 – Bit Rate measurements, as a function of ISR for A = 1 V and T= 27 $\mu s$, 25 $\mu s$ and 24 $\mu s$.

Figure 3.27 presents the results corresponding to T= 25 $\mu s$, 20 $\mu s$, 15 $\mu s$, 10 $\mu s$, 9 $\mu s$, 8$\mu s$, 7$\mu s$, 6 $\mu s$, 5 $\mu s$, 4$\mu s$, 3 $\mu s$, 2 $\mu s$ and 1 $\mu s$. Here, for all interference signals with T inferior to 24 $\mu s$, the interference signal suddenly interrupted the communication. However, this happens at different attenuation levels.

Figure 3.28 shows the same results but as a function of the ISR. We observe that the interference signal with T = 1 or 2 $\mu s$ required ISRs significantly inferior than for the other cases to interrupt the communication.

In order to analyze this behavior, Figure 3.29 presents the attenuation required to lose the communication as a function of the T and Figure 3.30 presents the ISR corresponding to the attenuation for the different T values.

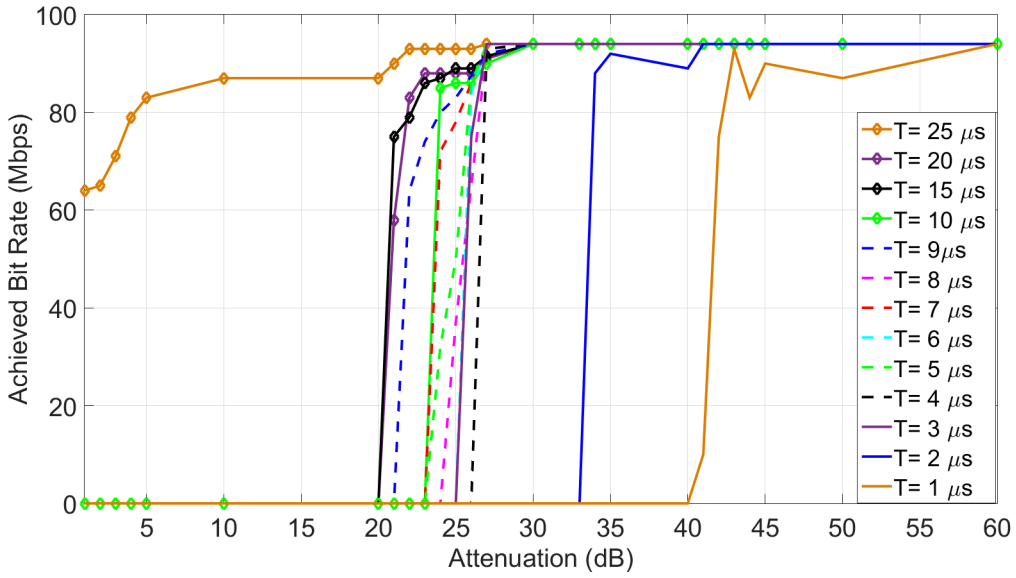



Figure 3.27 – Bit Rate measurements, as a function of the attenuation levels, for A = 1 V and different T values.

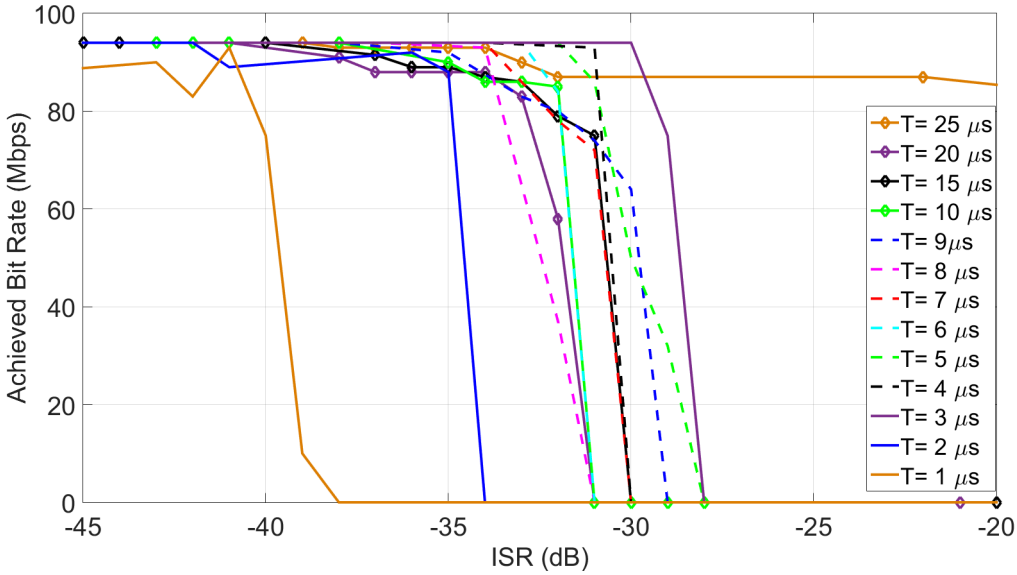



Figure 3.28 – Bit Rate measurements, as a function of the ISR for A = 1 V and different T values.

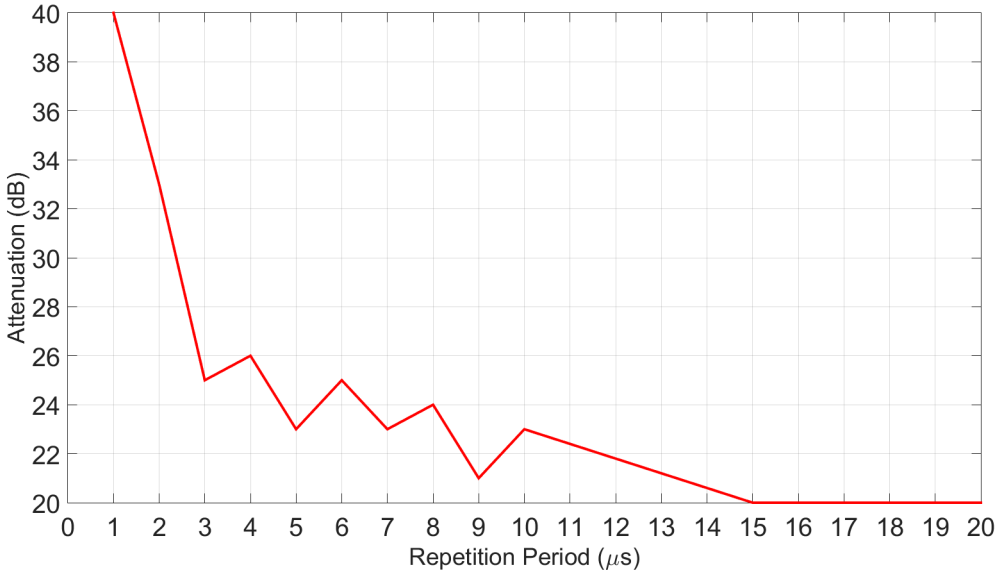



Figure 3.29 – Attenuation value required to completely interrupt the communication, as a function of the T

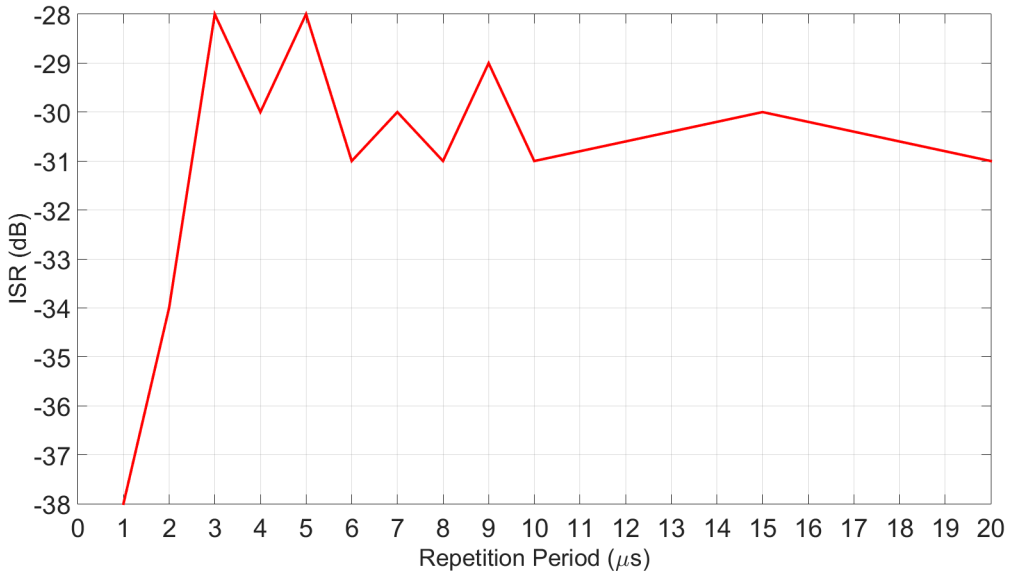



Figure 3.30 – ISR value required to completely interrupt the communication, as a function of the T

On the one hand, we observe that for T superior or equal to 3 $\mu s$, the ISR required to corrupt the communication is quasi constant, around -30 dB. On the other hand, for T inferior to 3 $\mu s$, the ISR required to lose the communication is significantly lower (-34 dB for T = 2 $\mu s$ and -38 dB for T=1 $\mu s$).

### 3.3.4 Interpretation of the measurements

Figures 3.24 and 3.25 show the interruption of the communication for T = 24 $\mu s$ regardless of the interference power level. This can be explained by the MAC layer characteristics.

As explained in section 1.4.1, the channel has to be free during a minimum duration called the *DCF Interframe Space* (DIFS) period (28 $\mu s$) to allow the WLAN station to access the medium and transmit the data. Thus, as soon as the interference signal is systematically repeated with a T period inferior or equal to 24 $\mu s$, the results seem to show that the channel is considered busy.

However, in figure 3.26, we notice that the communication is not interrupted for T = 25 $\mu s$ and 27 $\mu s$, whereas these periods are inferior to the DIFS period.

This can be partially explained by the time window employed at the receiver stage to control the occupation of the resources.

In the first chapter, we briefly described the mechanism applied to sense the medium at the PHY layer, called the *Clear Channel Assessment* (CCA). According to [Sta12] and as indicated in section 1.5.1, it consists in measuring the *highest average power* over the channel during the DIFS period.

However, the acquisition method of the *highest average power* is not precisely described in the standard. Indeed, the standard only states that the CCA indicator should report that the medium is busy within a 4 $\mu s$ maximum time [Sta12, p. 1623]. Note that 4 $\mu s$ corresponds to the duration of one OFDM symbol plus the guard interval.

We can then assume that this delay of 4 $\mu s$ plays a role in the value of 24 $\mu s$. But, without knowing precisely the CCA mechanism, we are not able to provide a precise interpretation.

Figure 3.31 is a zoom of Figure 3.26. In this figure, we present the bite rate for T = 25 $\mu s$ and 27 $\mu s$ according to the ISR.

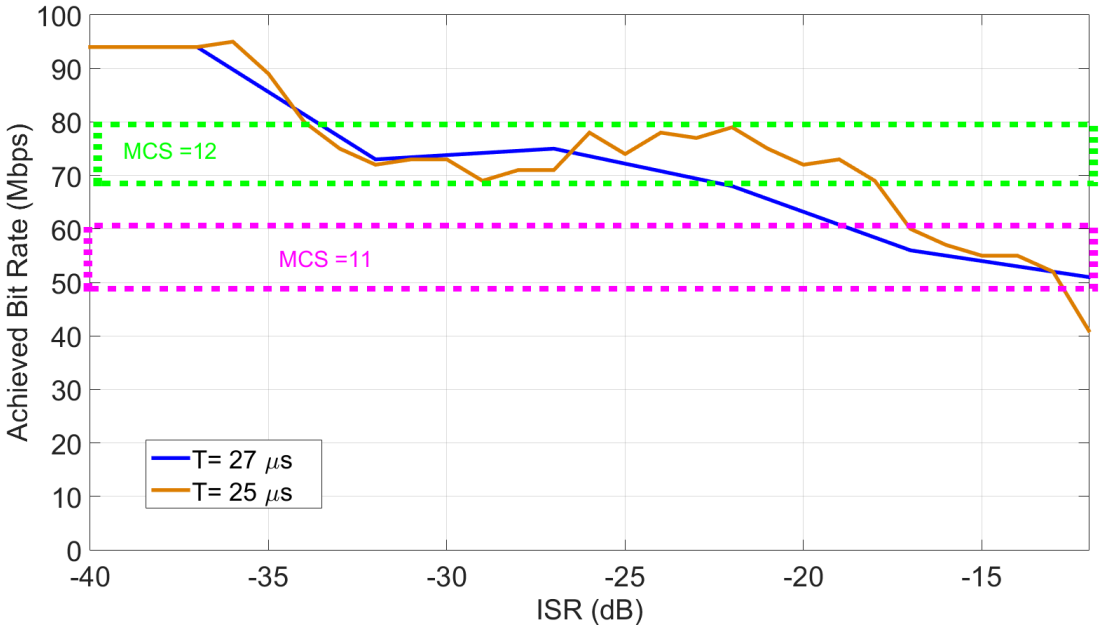
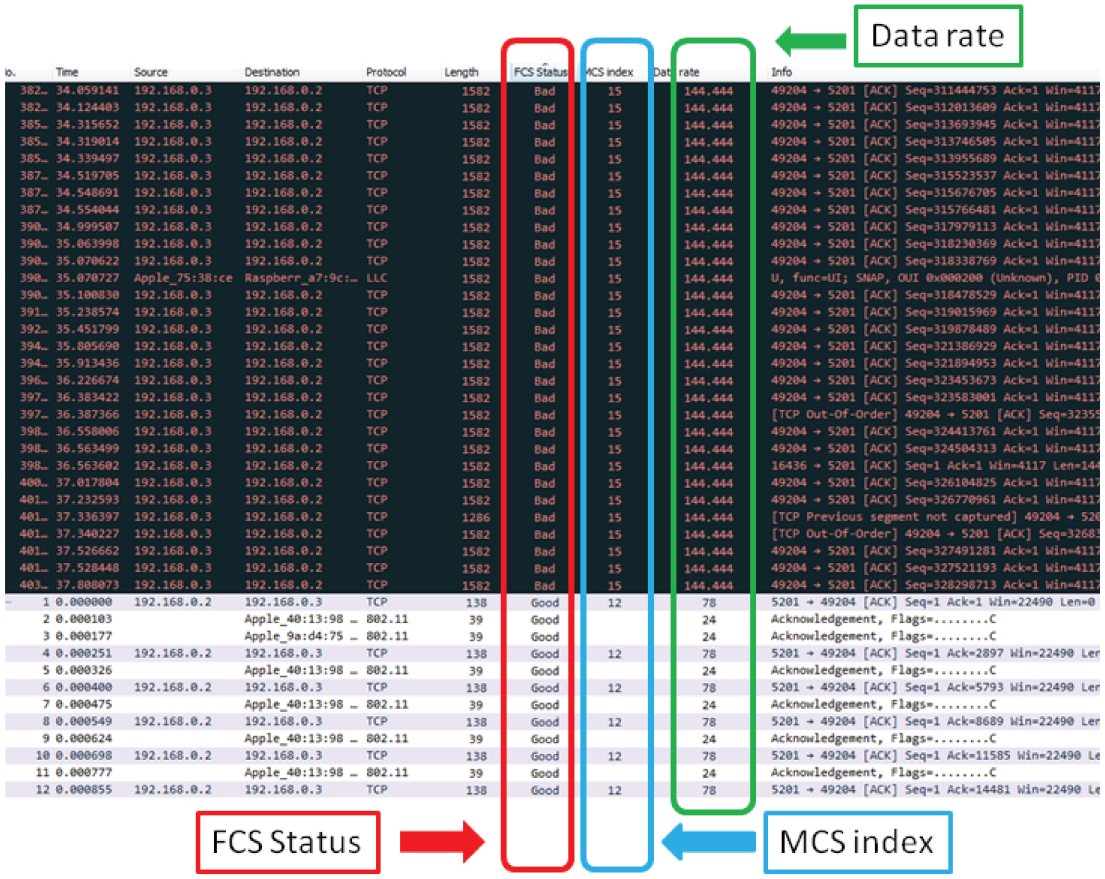



Figure 3.31 – Bit Rate measurements, as a function of ISR for A = 1 V and T= 27 $\mu s$ and 25 $\mu s$.

As previously observed, the CCA mechanism does not consider the medium as busy. Then, we simply observe a diminution of the bit rate with an increase in the ISR. This diminution illustrates the MCS adaptation mechanism. The interference affects the transmitted data and the receiving station is informed of this degradation through the FCS mechanism described in chapter 1.

To be able to observe this mechanism, we employed Wireshark. Figure 3.32 shows captured packets of traffic flow over the network in the presence of an interference signal.

There, we can verify that if the FCS status is bad for several successive frames, the MCS index is adapted from 15 to 12 in this capture. In case of bad FCS, the receiving station does not send the corresponding ACK to the transmitting station. Indeed, the




| No. | Time | Source | Destination | Protocol | Length | FCS Status | MCS index | Data rate | Info |
|---|---|---|---|---|---|---|---|---|---|
| 382… | 34.059141 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=311444753 Ack=1 Win=4117 |
| 382… | 34.124403 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=312013609 Ack=1 Win=4117 |
| 385… | 34.315652 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=313693945 Ack=1 Win=4117 |
| 385… | 34.319014 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=313746505 Ack=1 Win=4117 |
| 385… | 34.339497 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=313955689 Ack=1 Win=4117 |
| 387… | 34.519705 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=315523537 Ack=1 Win=4117 |
| 387… | 34.548691 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=315676705 Ack=1 Win=4117 |
| 387… | 34.554044 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=315766481 Ack=1 Win=4117 |
| 390… | 34.999507 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=317979113 Ack=1 Win=4117 |
| 390… | 35.063998 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=318230369 Ack=1 Win=4117 |
| 390… | 35.070622 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=318338769 Ack=1 Win=4117 |
| 390… | 35.070727 | Apple_75:38:ce | Raspberr_a7:9c:… | LLC | 1582 | Bad | 15 | 144.444 | U, func=UI; SNAP, OUI 0x000200 (Unknown), PID 6 |
| 390… | 35.100830 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=318478529 Ack=1 Win=4117 |
| 391… | 35.238574 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=319015969 Ack=1 Win=4117 |
| 392… | 35.451799 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=319878489 Ack=1 Win=4117 |
| 394… | 35.805690 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=321386929 Ack=1 Win=4117 |
| 394… | 35.913436 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=321894953 Ack=1 Win=4117 |
| 396… | 36.226674 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=323453673 Ack=1 Win=4117 |
| 397… | 36.383422 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=323583001 Ack=1 Win=4117 |
| 397… | 36.387366 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | [TCP Out-Of-Order] 49204 → 5201 [ACK] Seq=3235 |
| 398… | 36.558006 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=324413761 Ack=1 Win=4117 |
| 398… | 36.563499 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=324504313 Ack=1 Win=4117 |
| 398… | 36.563602 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 16436 → 5201 [ACK] Seq=1 Ack=1 Win=4117 Len=144 |
| 400… | 37.017804 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=326104825 Ack=1 Win=4117 |
| 401… | 37.232593 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=326770961 Ack=1 Win=4117 |
| 401… | 37.336397 | 192.168.0.3 | 192.168.0.2 | TCP | 1286 | Bad | 15 | 144.444 | [TCP Previous segment not captured] 49204 → 520 |
| 401… | 37.340227 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | [TCP Out-Of-Order] 49204 → 5201 [ACK] Seq=3268 |
| 401… | 37.526662 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=327491281 Ack=1 Win=4117 |
| 401… | 37.528448 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=327521193 Ack=1 Win=4117 |
| 403… | 37.808073 | 192.168.0.3 | 192.168.0.2 | TCP | 1582 | Bad | 15 | 144.444 | 49204 → 5201 [ACK] Seq=328298713 Ack=1 Win=4117 |
| 1 | 0.000000 | 192.168.0.2 | 192.168.0.3 | TCP | 138 | Good | 12 | 78 | 5201 → 49204 [ACK] Seq=1 Ack=1 Win=22490 Len=0 |
| 2 | 0.000103 | | Apple_40:13:98 … | 802.11 | 39 | Good | | 24 | Acknowledgement, Flags=........C |
| 3 | 0.000177 | | Apple_9a:d4:75 … | 802.11 | 39 | Good | | 24 | Acknowledgement, Flags=........C |
| 4 | 0.000251 | 192.168.0.2 | 192.168.0.3 | TCP | 138 | Good | 12 | 78 | 5201 → 49204 [ACK] Seq=1 Ack=2897 Win=22490 Len |
| 5 | 0.000326 | | Apple_40:13:98 … | 802.11 | 39 | Good | | 24 | Acknowledgement, Flags=........C |
| 6 | 0.000400 | 192.168.0.2 | 192.168.0.3 | TCP | 138 | Good | 12 | 78 | 5201 → 49204 [ACK] Seq=1 Ack=5793 Win=22490 Len |
| 7 | 0.000475 | | Apple_40:13:98 … | 802.11 | 39 | Good | | 24 | Acknowledgement, Flags=........C |
| 8 | 0.000549 | 192.168.0.2 | 192.168.0.3 | TCP | 138 | Good | 12 | 78 | 5201 → 49204 [ACK] Seq=1 Ack=8689 Win=22490 Len |
| 9 | 0.000624 | | Apple_40:13:98 … | 802.11 | 39 | Good | | 24 | Acknowledgement, Flags=........C |
| 10 | 0.000698 | 192.168.0.2 | 192.168.0.3 | TCP | 138 | Good | 12 | 78 | 5201 → 49204 [ACK] Seq=1 Ack=11585 Win=22490 Le |
| 11 | 0.000777 | | Apple_40:13:98 … | 802.11 | 39 | Good | | 24 | Acknowledgement, Flags=........C |
| 12 | 0.000855 | 192.168.0.2 | 192.168.0.3 | TCP | 138 | Good | 12 | 78 | 5201 → 49204 [ACK] Seq=1 Ack=14481 Win=22490 Le |

Figure 3.32 – Example of capturing packets with Wiresharkof traffic flow over the network in the presence of a interference signal.

absence of two consecutive ACKs indicates the necessity to slow down the data rate by adapting the MCS index. This reduces the bit rate but permits to recover a good FCS which guarantees correct transmitted data.

### 3.3.5 Conclusion on the transient EM interferences

This experiment presents a study of the performances of IEEE 802.11n communication network under transient EM interferences, which are representative of those present in the railway environment.

The analysis considered a transient EM signal which is a double exponential signal. We studied the impact of the time interval between consecutive transients and the impact of the amplitude of the transients.

The experimental results allowed us to show that from a given ISR, when the time interval is inferior to 24 $\mu s$, the communication system systematically considers the channel busy and the communication is lost. Thus, if the ISR inside the train coaches reaches a sufficient level, the performance of such standard in the railway environment can significantly depend on the repetition rate of the transient produced by the catenary-pantograph sliding contact.

The DIFS period which is imposed by the MAC layer to sense the channel can be a limitation for applications in the railway environment if the repetition rate of transient interferences is inferior to the DIFS period. In parallel, the CCA process applied to sense the channel also consists in measuring the *highest average power* over the channel and this value depends on the interference power.

To complete this study, it would be necessary to measure the interference power present inside the coaches. Indeed, to our knowledge, the state of the art is limited to measurements performed on the train's roof. According to the interference power level measured inside coaches, it could be necessary to reduce the coupling between the interferences produced by the catenary-pantograph contact and the antennas of the OFDM receivers to permit WLAN station accessing the medium.

# Conclusions and Perspectives

We have carried out a detailed study of a Wireless Local Area Network (WLAN), the IEEE 802.11n network facing electromagnetic interferences. Two kind of interferences have been considered in this work: the intentional electromagnetic interferences (IEMI) in section 2.2 and the unintentional electromagnetic interferences (EMI) in section 2.1.

In the case of IEMI, we used interference signals such as those generated by commercial jammers (section 2.2.3). For EMI we used interference signals such as transient EM interference signals produced by contact losses between the catenary and the pantograph (section 2.1.3).

By doing a detailed analysis of the 802.11n standard, we identified distinctive features of IEEE 802.11n network. These features show that every user must find its own resources, this involves the existence of medium access mechanisms like Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). This can represent a weakness regarding the IEMI, because our experiments show that with an ISR of -20 dB the communication can be interrupted, compared to an ISR between -6 dB and 0 dB for cellular communications [MDS+15].

As soon as the channel access mechanisms are known, the jamming can be configured efficiently with very low power in order to consider the channel as busy for instance, with interference power between 10 dB and 20 dB below the signal power. This aspect makes this protocol vulnerable, because the jamming does not need to degrade the data, which would require more power.

By varying the parameters of the jamming signal, we have noticed that the sweep

period (SP) of the frequency band is an important parameter in the 802.11n network performance. For a sweep period lower than the duration of an OFDM symbol, i.e., 4 $\mu s$, the jamming is less aggressive with an equivalent power. In fact, this interference signal affects only a part of the subcarriers.

When the sweep period is very high, above 30 $\mu s$, the jamming covers only part of the channel. The most harmful sweep period is between the two cases mentioned above.

In perspective, if the aim is to improve the robustness of the IEEE 802.11n network facing this interference type, the CSMA/CA mechanism should be improved.

More broadly, it would be necessary to introduce monitoring solutions dedicated to the characterization of environmental conditions, including the detection of intentional interferences.

Otherwise, taking into account the current effort of leading European railway companies to offer Internet connection aboard trains [Int16], we have also studied 802.11n communications against the transient EM interferences produced by contact losses between the catenary and the pantograph .

We have based our work on interference models from a previous experimental work carried out on trains. We have studied the effect of the repetition interval between successive transients (T). As in the previous case, we have confirmed that the medium access mechanism plays a key role. Indeed, from a certain interference power level and as soon as T is lower than 24 $\mu s$, the communication is systematically interrupted. This figure is of the same order of magnitude as the DCF (Distributed coordination function) Interframe Space (DIFS) period. For lower power levels, the communication performance decreases with the occurrence frequency of the transient interferences. In particular, we observe a greater susceptibility when the occurrence intervals are less than 3 $\mu s$.

In perspective, for a Wi-Fi application aboard trains, it is necessary to study the power of interference signals inside coaches where the Wi-Fi antennas of access points are located. Therefore, a measurement campaign should be carried out to know the actual interference power levels, in order to verify that the power does not reach the threshold required to consider the medium as busy. In this case, it would be necessary to work on the attenuation of these transmitted interferences towards the coaches.

It must also be mentioned that we have worked with constant repetition intervals, whereas in practice they vary a lot. Indeed, these transient interferences can appear with repetition intervals in the order of some microseconds and then in other areas they disappear. With regard to the variation of the repetition intervals, one can also wonder if there is a risk that the modulation and coding scheme (MCS) mechanism will not adapt and what may be the consequences.

Note also that in the case of the aboard Internet, mobile networks are also part of the final solution the solution passes through an LTE link between the base station and the train, then switches to the Wi-Fi network on board the train. In this case, the LTE antennas are located on the train's roof. These antennas may receive interferences which cover a very broad spectrum. Thus, a susceptibility study of the global link will be necessary.

# Bibliography

[Als17] Alstom, urban infrastructure, 2017.

[Ano13] Anonymous. Wi-Fi: Overview of the 802.11 physical layer and transmitter measurements,primer. techreport, Tektronix, 2013.

[Ber10] Claude Berrou. *Codes and Turbo-codes*. Springer, 2010.

[Cos10] Robson Costa. Technical report no: 1. Technical report, Engineering faculty, University of Porto, 2010.

[DDA+12] Stephen Dudoyer, Virginie Deniau, Ricardo Adriano, M Nedim Ben Slimen, Jean Rioult, Benoît Meyniel, and Marion Berbineau. Study of the susceptibility of the GSM-R communications face to the electromagnetic interferences of the rail environment. *IEEE Transactions on electromagnetic compatibility*, 54(3):667–676, 2012.

[DPOS+08] Jon Del Portillo, Mikel Osinalde, Eluska Sukia, Inaki Sancho, Jaizki Mendizabal, and Juan Melendez. Characterization of the em environment of railway spot communication systems. In *Electromagnetic Compatibility, 2008. EMC 2008. IEEE International Symposium on*, pages 1–6. IEEE, 2008.

[Elw17] Elways solutions, 2017.

[Gir04] DV Giri. *High-power electromagnetic radiators: nonlethal weapons and other applications*. Harvard University Press, 2004.

[Gro14] F. Gronwald. On advanced transmitter and receiver models for the EMC analysis of modern communication systems. In *General Assembly and Scientific Symposium (URSI GASS), 2014 XXXIth URSI*, pages 1–4, Aug 2014.

[Hay09] S. Haykin. *Communication systems*. Wiley, 2009.

[Ins] National Instruments. *Introduction to Wireless LAN Measurements from 802.11a to 802.11ac*. National Instruments Corporation. Application Notes.

[Int16] SNCF launches free Wi-Fi on TGVs, December 2016.

[Ipe] iPerf, the ultimate speed test tool for tcp, udp and sctp.

[JK17] No-Geon Jung and Jae-Moon Kim. Contact loss simulator to analyze the contact loss of a rigid catenary system. *Journal of Electrical Engineering & Technology*, 12(3):1320–1327, 2017.

[KKT+09] Wonsoo Kim, Owais Khan, Kien T Truong, S-H Choi, Robert Grant, Hyrum K Wright, Ketan Mandke, Robert C Daniels, Robert W Heath Jr, and Scott M Nettles. An experimental evaluation of rate adaptation for multi-antenna systems. In *INFOCOM 2009, IEEE*, pages 2313–2321. IEEE, 2009.

[KNNS11] Samad S Kolahi, Shaneel Narayan, Du DT Nguyen, and Yonathan Sunarto. Performance monitoring of various network traffic generators. In *Computer Modelling and Simulation (UKSim), 2011 UkSim 13th International Conference on*, pages 501–506. IEEE, 2011.

[Lit12] Practical manufacturing testing of 802.11 OFDM wireless devices. Technical report, LitePoint Corporation, 2012.

[LMT04] Mathieu Lacage, Mohammad Hossein Manshaei, and Thierry Turletti. IEEE 802.11 rate adaptation: a practical approach. In *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems*, pages 126–134. ACM, 2004.

[LPA+16] Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer, and Jeffrey H. Reed. A Communications Jamming Taxonomy. *IEEE Security & Privacy*, 14(1):47–54, jan 2016.

[MAE07] Saida Maaroufi, Wessam Ajib, and Halima Elbiaze. Performance evaluation of new mac mechanisms for IEEE 802.11n. In *Global Information Infrastructure Symposium, 2007. GIIS 2007. First International*, pages 39–45. IEEE, 2007.

[MDS+15] S Mili, V Deniau, D Sodoyer, M Heddebaut, and S Ambellouis. Jamming detection methods to protect railway radio communication. *methods*, 4(7), 2015.

[met09] Rapport sur la methodologie de caracterisation et les distributions de bruits em extraites constitution d'une base de donnees - partie III - mesures temporelles a bord. 2009.

[MZM+14] Yun Mo, Zhongzhao Zhang, Weixiao Meng, Lin Ma, and Yao Wang. A spatial division clustering method and low dimensional feature extraction technique based indoor positioning system. *Sensors*, 14(1):1850–1876, 2014.

[Oua11] Hamid Ouaddi. *Contribution a la modelisation HF du comportement electromagnetique de l infrastructure d alimentation ferroviaire.* Phd thesis, Universite de Lille 1, 2011.

[PIK11] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy. Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys Tutorials*, 13(2):245–257, Second 2011.

[Poi11a] Richard Poisel. *Modern communications jamming principles and techniques.* Artech House, 2011.

[Poi11b] Richard A. Poisel. *Modern Communications Jamming, Principles and Techniques.* Artech House, second edition, 2011.

[Pra04] Ramjee Prasad. *OFDM for wireless communications systems.* Artech House, 2004.

[PS13] Eldad Perahia and Robert Stacey. *Next generation wireless LANs: 802.11n and 802.11ac.* Cambridge university press, 2013.

[RHS12] Laurent Ros, Hussein Hijazi, and Eric Simon. Complex amplitudes tracking loop for multipath slow fading channel estimation in ofdm systems. 2012.

[RM14] Emilio Rodriguez Martinez. *Track circuits robustness: modeling, measurement and simulation.* Licentiate thesis, Lulea University of Technology, 2014.

[RR07] Iyappan Ramachandran and Sumit Roy. Clear channel assessment in energyconstrained wideband wireless networks. *IEEE Wireless Communications*, 14(3), 2007.

[RS10] William Radasky and Edward Savage. Intentional electromagnetic interference (IEMI) and its impact on the US power grid. *Meta*, pages 1–3, 2010.

[SAS+14] Sanjeev Srivastava, Sweta Anmulwar, AM Sapkal, Tushar Batra, Amit Kumar Gupta, and Vipin Kumar. Comparative study of various traffic generator tools. In *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in*, pages 1–6. IEEE, 2014.

[SDR+09] N Ben Slimen, V Deniau, J Rioult, S Dudoyer, and S Baranowski. Statistical characterisation of the EM interferences acting on GSM-R antennas fixed above moving trains. *The European Physical Journal Applied Physics*, 48(2):21202, 2009.

[Sie17] eHighway electrification of road freight transport, 2017.

[SLPL+15] Chowdhury Shahriar, Matt La Pan, Marc Lichtman, T Charles Clancy, Robert McGwier, Ravi Tandon, Shabnam Sodagari, and Jeffrey H Reed. PHY-layer resiliency in OFDM communications: A tutorial. *IEEE Communications Surveys & Tutorials*, 17(1):292–314, 2015.

[SRS14] Huaqiang Shu, Laurent Ros, and Eric Pierre Simon. Simplified random-walk-model-based kalman filter for slow to moderate fading channel estimation in ofdm systems. *IEEE transactions on signal processing*, 62(15):4006–4017, 2014.

[SSR15] Huaqiang Shu, Eric Pierre Simon, and Laurent Ros. On the use of tracking loops for low-complexity multi-path channel estimation in ofdm systems. *Signal Processing*, 117:174–187, 2015.

[Sta12] IEEE standard for information technology–telecommunications and information exchange between systems local and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications - redline. *IEEE Std 802.11-2012 (Revision of IEEE Std 802.11-2007) - Redline*, pages 1–5229, March 2012.

[TG94] Clayborne D Taylor and DV Giri. *High-power microwave systems and effects*. Taylor & Francis, 1994.

[TWT+13] Kuo-Chang Ting, Hwang-Cheng Wang, Chih-Cheng Tseng, Fang-Chang Kuo, and Feipei Lai. An accurate power analysis model based on MAC layer for the DCF of 802.11n. *Journal of the Chinese Institute of Engineers*, 36(1):17–26, 2013.

[Wan09] Guodong Wang. Characteristics of radio frequency interference from pantograph arcing in car of traction stock. In *Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2009 3rd IEEE International Symposium on*, pages 207–210. IEEE, 2009.

[Wi-17] Wi-Fi alliance, 2017.

[Wir17] Wireshark user's guide, 2017.

[XWZ13] Fei Xu, Guodong Wang, and Jinbao Zhang. Research on the radiation characteristics of pantograph and catenaries offline noise. In *Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications (MAPE), 2013 IEEE 5th International Symposium on*, pages 724–727. IEEE, 2013.