UNIVERSITY OF PALERMO

DOCTORAL THESIS

Architectures and Protocols for Flexible Physical Layers in Wireless Networks

Ph.D. Candidate:
Ing. Alice LO VALVO

Tutor:
Prof. Ilenia TINNIRELLO

Cotutor:
Prof. Giuseppe
Costantino GIACONIA

Cotutor:
Dr. Vincent LENDERS

A thesis submitted in fulfillment of the requirements
for the degree of Doctor of Philosophy
in the

DEIM - Dipartimento di Energia, Ingegneria dell'Informazione
e modelli Matematici

XXXI CYCLE - ACADEMIC YEAR 2017-2018

"Imagination is more important than knowledge..."

Albert Einstein

UNIVERSITY OF PALERMO

Abstract

Faculty of Engineering

DEIM - Dipartimento di Energia, Ingegneria dell'Informazione e modelli Matematici

Doctor of Philosophy

Architectures and Protocols for Flexible Physical Layers in Wireless Networks

by Ing. Alice LO VALVO

Emerging wireless technologies are characterized by an increasing level of flexibility and programmability, not only in terms of core network functionalities, with the consolidated paradigms of software-defined-networks and function virtualization, but also in terms of radio access functionalities. Although the concept of software-defined PHY and MAC protocols is not new, exploiting flexibility at the lower layers of the protocol stack is not an easy task, because of complexity and performance constraints. Indeed, dealing with software-defined implementations of the radio implies managing complex software routines, often tightly inter-dependent and difficult to reuse, and poses some performance limitations because software implementations are inevitably less efficient than hardware ones.

In this thesis, we focus on the theme of PHY flexibility, by proposing innovative architectures of the radio, in which a limited set of parameters and functionalities is programmable, in order to achieve a trade-off between the complexity of the hardware and software architecture of the receiver, and the performance improvements that can be enabled in different network scenarios, characterized by specific topologies or interference conditions. More specifically, by considering that most modern communication systems are based on Orthogonal Frequency Division Multiplexing (OFDM), we decided to focus on the generalization of a typical OFDM transceiver, in which we introduced different levels of programmability: i) the possibility of dynamically adjusting the total bandwidth, for a given number of subcarriers, even on a per-packet basis, and without an explicit control channel between the transmitter and the receiver; ii) the possibility of mapping dynamically pilot and data symbols, with a symbol-level resolution, in order to increase robustness to interference and jammers; iii) the possibility of transmitting special tone signals, on desired sub-carriers, for coding simple control messages to be exploited for network-wide coordination.

The first capability has been designed in order to add more granularity to PHY adaptations (usually limited to the tuning of the transmission power or per-carrier modulation format).

The second capability has been conceived in order to improve physical layer robustness to intentional attacks. The are different jammer types, but some kind of their are more disruptive than others. Indeed, in an OFDM-based communication, estimation and equalization of the channel's frequency response is crucial for a correct decoding of the packet at the receiver side. Estimation and equalization are done by the insertion of equal power and equally spaced pilot tones in the signal. Some types of jammers attack pilot tones in order to destroy information used by the equalization algorithm. For this reason, we designed and implemented some mechanisms in order to mitigate as much as possible some of the jamming strategies that are very problematic in an OFDM-based communication.

Finally, the last capability has been exploited for designing an efficient contention mechanism based on the concept of Repeated Contentions, called ReCo. We demonstrate that running multiple contention rounds in random access networks in the frequency domain improves the channel utilization efficiency. Ultimately, thanks to advantages of flexibility of the physical layer, we provide a robust medium access control (MAC) protocol, which is not depending on the number of the contending stations.

All the proposed extensions to a reference OFDM transceiver have been validated with real implementations and experiments. For the prototyping activities, we worked on two different platforms: the well known WARP software-defined board and the USRP platform. Experiments have been planned and analyzed by focusing on reproducibility of the results and by providing comparisons with benchmark scenarios.

Acknowledgements

First, I would like to express my authentic gratitude to my advisor, Ilenia Tinnirello, for trusting me and giving me the opportunity to work in her lab. I think that the satisfaction experienced during the Ph.D. years largely depends on the relationship between the student and the advisor. She is a mentor to me and it was an honor working under her expert guidance.

I am thankful to all my friends and colleagues at University of Palermo; Michele, Domenico, Daniele, Pippo, Giovanni, Fabrizio and all the others. Several of them have become close friends over the years, and I'm very happy to have spent this time with them.

Of course, the Ph.D. years would not have been as nice as they were without my precious friends from the outside world: Arianna, Roberta, Stella, Vittoria, Giuseppe and all others.

Finally, I would like to express my deep gratitude to my family, in particular to my parents Mario and Bianca, for giving me the opportunity to go to the university and for their unconditional love and support. It means a lot to me. A special gratitude to my dog, Spillo. He is definitely in paradise...

Contents

List of Figures

List of Tables

List of Abbreviations

3GPP	Third **G**eneration **P**artnership **P**roject
ACK	**ACK**nowledge
AWGN	**A**dditive **W**hite **G**aussian **N**oise
BBJ	**B**road-**B**and **J**ammer
BEB	**B**inary **E**xponential **B**ackoff
BER	**B**it **E**rror **R**ate
BPSK	**B**inary **P**hase **S**hift **K**eying
CSMA	**C**arrier **S**ense **M**ultiple **A**ccess
CTS	**C**lear **T**o **S**end
CW	**C**ontention **W**indow
DCF	**D**istributed **C**oordination **F**unction
DIFS	**D**CF **I**nter**f**rame **S**pace
DSSS	**D**irect **S**equence **S**pread **S**pectrum
FEC	**F**orward **E**rror **C**orrection
FFT	**F**ast **F**ourier **T**ransform
FHSS	**F**requency **H**opping **S**pread **S**pectrum
FPGA	**F**ield **P**rogrammable **G**ate **A**rray
ICI	**I**nter**c**arrier **I**nterference
IEEE	**I**nstitute of **E**lectrical and **E**lectronic **E**ngineers
IFFT	**I**nverse **F**ast **F**ourier **T**ransform
ISI	**I**nter**s**ymbol **I**nterference
ISM	**I**ndustrial **S**cientific and **M**edical
LTE	**L**ong **T**erm **E**volution
LTS	**L**ong **T**raining **S**ymbol
MAC	**M**edia **A**ccess **C**ontrol
MIMO	**M**ultiple **I**nput **M**ultiple **O**utput
MPDU	**M**AC **P**rotocol **D**ata **U**nit
NAV	**N**etwork **A**llocation **V**ector
OFDM	**O**rthogonal **F**requency **D**ivision **M**ultiplexing
PBJ	**P**artial-**B**and **J**ammer
PDU	**P**rotocol **D**ata **U**nit
PHY	**Ph**ysical **l**ayer
PNJ	**P**ilot **N**ulling **J**ammer
PRJ	**P**ilot **R**andom-phase **J**ammer

PTJ	**P**ilot **T**ones **J**ammer
QAM	**Q**uadrature **A**mplitude **M**odulation
QPSK	**Q**uadrature **P**hase **S**hift **K**eying
ReCo	**Re**peated **Co**ntention
RTS	**R**equest **T**o **S**end
RX	**R**eceiver
SDR	**S**oftware **D**efined **R**adio
SISO	**S**ingle **I**nput **S**ingle **O**utput
SJR	**S**ignal-to-**J**ammer **R**atio
SNR	**S**ignal-to-**N**oise **R**atio
STS	**S**hort **T**raining **S**ymbol
TDMA	**T**ime **D**ivision **M**ultiple **A**ccess
TX	**T**ransmitter
UDP	**U**ser **D**atagram **P**rotocol
USRP	**U**niversal **S**oftware **R**adio **P**eripherical
WARP	**W**ireless open-**A**ccess **R**esearch **P**latform
WLAN	**W**ireless **L**ocal **A**rea **N**etwork
WMAN	**W**ireless **M**etropolitan **A**rea **N**etwork
WMP	**W**ireless **M**AC **P**rocessor

Chapter 1

Introduction

IN the last few years, we have assisted to an incredible proliferation of radio technologies to answer to very different scenarios and applications: cellular technologies for mobile access to internet applications, local technologies for sensor networks, home automation and industrial applications, entertainment, etc. Moreover, most of these services are and will be based on much higher bit rates. The new services (video streaming, video broadcasting, high-speed Internet, etc.) will demand much higher bit rates/bandwidths and will have strict QoS requirements, such as the received BER. The lack of a solution for responding efficiently to all possible usage scenarios is the reason of development of heterogeneous technologies. Despite all modern standard being characterized by a high level of complexity for the definition of multiple operating conditions, new extensions are released for new usage cases. The new and emerging standards (i.e. IEEE 802.11ax for IEEE 802.11 technology) will have to measure up to the ones based on wired communications and overtake the difficulty posed by the wireless medium to provide coverage and communication without interruption. In the current state, we have many 'monolithic' technologies for specific applications. Therefore, there might also be cases in which the user equipment has to follow the rapid development of new wireless standards by providing enough flexibility and agility to be easily upgradeable (with perhaps the modification/addition of specific software code but no other intervention in hardware). A solution could be to resort to radio programmable platforms, where the radio, medium access and network capabilities can be reprogrammed via software according to usage scenarios.

1.1 PHY Flexibility

The notion of flexibility in a radio is an useful concept in the physical layer (PHY) of transmission systems. The main features of a flexible radio are adaptivity, reconfigurability, modularity, scalability, and so on. The presence of any subset of these properties is enough to attribute the term flexible to any particular radio system [1]. For instance, reconfigurability can be defined as the ability to reorganize changeable modules at a structural or architectural level, while adaptivity can be defined as the radio system response to changes by properly altering the numerical value of a set of transmission parameter[2, 3], such as frequency, channel bandwidth, etc..

A flexible PHY design is particularly beneficial considering the various applications recommended for 5G [4]. In fact, these applications typically have strict requirements. For instance, broadband communication are important for video streaming services with high resolution for TV and smartphones; the Internet of Things (IoT) is aimed at connecting a massive amount of devices; wireless sensor networks need to provide monitoring at low cost and with a long battery life; smart vehicles improve safety and avoid accidents by exchanging their driving status, such as position, breaking, acceleration, and speed. Hence, for the imminent fifth generation (5G) mobile networks, software-defined networking (SDN), software-defined radio (SDR) and cognitive radio (CR) are all important concepts. In fact, SDN can facilitate network management by enabling anything as a service; SDR allows to virtualize the radio, where many radio components are implemented in software; finally, CR uses a software-based decision to change some values of SDR parameters optimizing the use of communication resources. A new innovation will be performed when all these software paradigms are applied to the physical layer, in which its functionalities are defined and controlled by software as well.

The goal of this thesis is to focus on the flexibility of the physical layer. More specifically, we studied how this flexibility can be a contribution in various situations. Starting from a design of an enhanced receiver in order to have a dynamic adaptation of the channel bandwidth, then we focused on the security aspect of a particular communication system studying and proposing a new model in order to avoid some types of disrupting jammers. Finally, we studied and implemented a generalized contention mechanism for for wireless network WLAN technologies. This was possible thanks to the flexibility of the PHY layer and SDR is a powerful platform that allows this type of study.

1.2 Software Defined Radio

A radio is any kind of device that using radio waves to transmit or receive signals in the radio frequency (RF) part of the electromagnetic spectrum to

facilitate the transfer of information. It carries information by systematically modulating properties of electromagnetic energy waves transmitted through space, such as their amplitude, frequency, phase, or pulse width. A radio communication system requires a transmitter and a receiver, each having an antenna and appropriate terminal equipment. In today's world, presence of radio systems is in various devices such as cell phones, computers, vehicles, and televisions. Traditional hardware-based radio devices can only be modified through physical intervention. This results in minimal flexibility.

For this reason, in the early 90s Joseph Mitola defined *Software Radio* as an identifier of a class of radios that could be reprogrammed and reconfigured through software [5]. Mitola imaged an ideal Software-Defined Radio, in which physical components were only an antenna and an Analog Digital Converter (ADC) on the receiver side. Similarly, the transmitter would have a Digital Analog Converter (DAC) and a transmitting antenna. The rest of the functions would be managed by software. SDR provides software control of the most radio functions, including modulation, multiplexing, amplification, multiple access. The idea of SDR is simple: to replace as much as possible specialized electronics, used to manage the radio signal, by programmable devices controlled by software. In other words, SDR is a radio communication system where components that commonly implemented on hardware are implemented by software[6, 7, 8]. SDR defines a collection of hardware and software technologies where some or all of the radio functions are implemented through modifiable software or firmware operating on programmable processing technologies. These devices include field programmable gate arrays (FPGA), digital signal processors (DSP), general purpose processors (GPP), programmable System on Chip (SoC) or other application specific programmable processors. The use of these technologies allows new wireless features and capabilities to be added to existing radio systems without requiring new hardware.

As mentioned before, flexibility concept is considered as the strength of SDR. This approach allows for ease of adaptability, shortens development effort and greatly reduces cost and complexity [9].

1.3 Outline and Contributions

We give an overview of the outline of the thesis and summarize the main contribution of each chapter.

- **Chapter 2:** We demonstrate that a possible powerful solution for extending physical layer flexibility in technologies based on Orthogonal Frequency Division Multiplexing (OFDM) is the dynamic adaptation of the channel width. Although some standards already define the possibility of utilizing multiple channel widths (e.g. 20MHz, 10MHz, 5MHz for IEEE 802.11a standards), such an utilization is limited to a static configuration of a value defined during the network set-up. Conversely,

we demonstrate that channel width adaptations can be performed in real-time during network operation, even on a per-packet basis. To this purpose, we propose an innovative and efficient receiver design, which allows the transmitter to take decisions about the channel width without explicitly informing the receiver.

Main contribution: New physical layer capabilities have been envisioned and demonstrated in a real prototype for adapting the channel bandwidth at each transmission attempt within a predefined operating channel *without signalling*.

- **Chapter 3:** We evaluate signal randomization techniques which aim at making the OFDM signal less predictable, and thus more robust to adversarial interference. In fact, OFDM-based wireless communications are particularly vulnerable to jamming attacks. Jammers which have knowledge of the OFDM system parameters can effectively disrupt the communications with matched signals that are much weaker than the legitimate ones. To break this asymmetry, we consider techniques which randomize the location of the pilot tones used for receiver synchronization and the number of active sub-carriers for the actual transmission of the data. Our evaluation based on simulations and experiments with software-defined radios reveal that, in combination, these techniques manage to improve the jamming resistance up to 15dB, forcing the jammer to jam with signals that are significantly stronger than the legitimate signals in order to block the communication. We further propose an adaptive sub-carrier randomization algorithm which optimizes the throughput for different levels of jamming.

  Main contribution: We show that our adaptive algorithm is able to achieve the maximum data throughput in various jamming scenarios while classical OFDM systems fail to deliver any data.

- **Chapter 4:** We propose a generalized contention mechanism for wireless networks based on the concept of Repeated Contentions (ReCo), whose efficiency is not very sensitive to the number of contending stations. The idea is selecting the contention winner in consecutive elimination rounds that guarantee an arbitrary low collision probability. Elimination rounds can be performed in the time or frequency domain (with different overheads) according to the physical capabilities of the nodes. Closed analytical formulas are given to dimension the number of contention rounds. Contention in the frequency domain can be based on the simultaneous transmission and reception of short tones, which is feasible on top of OFDM PHY layers with minor modifications, as demonstrated by our implementation.

  Main contribution: ReCo offers stable and close-to-ideal throughput performance. It can be dimensioned with reliable and simple formulas and it does not require fine tuning or complex adaptive algorithms, e.g., as the number of stations varies. The protocol is also robust to imperfect carrier sensing results.

Chapter 2

Agile Receiver

In this chapter, we present a novel design of a IEEE 802.11-based receiver capable to "understand" the incoming packet bandwidth and to change its internal logic in order to demodulate the information in the correct way. This kind of receiver could be used for various applications, especially for spectrum agility. In this context, the PHY layer flexibility is a key for an intelligent dynamic adaptation based on the spectrum occupancy.

2.1 Introduction

Wi-Fi devices operates using different channels, which correspond to different parts of the total available spectrum. The channels are determined by their carrier frequency and their bandwidth, which we also call channel width. For the older 802.11b/g/a standards, the channel bandwidth is fixed and set to 20 MHz. The newer 802.11n, 802.11ac and 802.11ax standards can use a variable channel bandwidth. More specifically, 802.11n can operate on the 2.4 or 5 GHz bands, and use the legacy 20 MHz bandwidth, as well as a 40 MHz bandwidth, which is obtained by bonding two 20 MHz channels together. 802.11ax also operate on the 2.4 or 5 GHz bands, and it can use widths of 20 MHz, 40 MHz ($2 \cdot 20MHz$), 80 MHz ($2 \cdot 40MHz$) and 160 MHz ($2 \cdot 80MHz$), as well as 802.11ac that can operate only in the 5 GHz band. Fig. 2.1 and Fig. 2.2 show the Wi-Fi standards progression and the comparison between IEEE 802.11ac and 802.11ax.

When two or more 802.11 transmitters overlap parts of the spectrum at the same time an interference occurs. In this case, one (or more) of the receivers might be unable to decode in a right way the signal transmitted by the transmitter(s). If the interfering signal is strong enough, it might cause an incorrect demodulation of some of the symbols at the receiver side(s). Moreover, if too many symbols are corrupted, there is a collision and the frame is lost. The

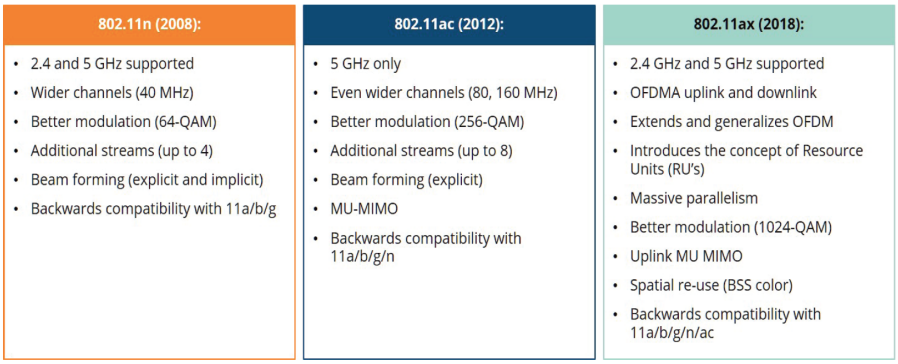


FIGURE 2.1: Wi-Fi Standards progression.

	802.11ac	802.11ax
Bands	5 GHz only	2.4 GHz and 5 GHz
Channels	20, 40, 80, 80+80, 160 MHz	20, 40, 80, 80+80, 160 MHz
FFT Sizes	64, 128, 256, 512	256, 512, 1024, 2048
Subcarrier spacing	312.5 kHz	78.125 kHz
OFDM symbols	3.2 usec	12.8 usec
OFDM symbol cyclic prefix	0.8 or 0.4 usec	0.8 or 1.6 or 3.2 usec
Highest modulation	256 QAM	1024 QAM
Spatial streams	1-8 (not implemented beyond 4)	1-8 (may be implemented)

FIGURE 2.2: Comparison between 802.11ac and 802.11ax IEEE standards.

amount of interference depends on the amount of spectrum overlap. This behaviour is obvious, since the amount of overlap determines the amount of the interference and the probability of corrupting symbols increases. Considering previous observations, we can state: **networks should use configurations that minimize spectrum overlap**.

Spectrum agility has been traditionally considered as the capability to set up a wireless communication link over different spectrum blocks, by shifting from one central frequency to another. This capability is of primary importance for cognitive radio systems or for systems working in ISM bands, which are usually unplanned and characterized by significant spatial variations of spectrum availability. Available spectrum portions can differ in size. Therefore, another desirable capability of spectrum-agile technologies is the possibility of adapting the channel width to the available spectrum bandwidth and/or aggregating independent (non-contiguous) spectrum portions into a single logical link. In [10], they designed and implemented some algorithms in order to find an interference-versus-capacity tradeoff and a utility-optimal for the joint allocation of center frequency, bandwidth and transmit power. In all of these cases, channel width adaptations are implemented through a signalling mechanism between access points (APs) and clients or forcing the transmitter to indicate the channel bandwidth used by each frame in its

preamble. Instead, in our work bandwidth adaptations are performed without any type of signalling. The receiver is so smart to sense on-the-fly the channel bandwidth of the incoming packet in order to properly decode the transmitted packet.

As mentioned before, this work concerns channel width adaptations for OFDM-based systems. As a reference technology, wireless nodes based on the IEEE 802.11a OFDM PHY and medium access control (MAC) specifications are considerate. As mentioned before, the PHY of legacy 802.11a nodes includes the possibility of working with 5 MHz and 10 MHz channel widths, in addition to the usual 20 MHz configuration. This work do not focus on the logic for selecting the channel width, but rather on the receiver architecture which enables the possibility of implementing different decision logics at the transmitter side. Although the logic could in principle benefits on context information signaled by the receiver, our architecture allows the transmitter to take decisions about channel widths, without explicitly signaling the decision to the intended receiver. As in [11], channel width adaptations are implemented by changing the clock of the OFDM transmitter. The receiver architecture has been implemented on the well-known Wireless Open-Access Research Platform (WARP) [12] research board, which is a FPGA-based SDR platform, for which it is available a reference implementation of legacy 802.11 PHY (including 802.11a/g OFDM modulations).

It has proven that a spectral analysis of the preamble of each incoming frame can be performed on time for reconfiguring the internal clock of the receiver consistently to the transmitter one.

We organize the remainder of this chapter as follows. After a literature review presented in Section 2.2, in Section 2.4 we present the main aspects of our innovative transceiver design, also called *Agile Receiver*, and the validation and performance tests that have been carried out for demonstrating the feasibility of spectrum agility on the well-known WARP [12] research board.

2.2 Related Work

2.2.1 Channel width modulation

The possibility of adapting the channel width has been demonstrated to be beneficial for different performance figures, such as energy consumption, link reliability, throughput and fairness [11], by generalizing the concept of *rate adaptation*. Differently from usual rate adaptation, where modulation formats are specified in the PHY fields of each frame, requests for channel width adaptation are transmitted in special control frames which require a confirmation by the intended receiver. A similar adaptation of modulation formats and channel widths is proposed in [13] for OFDM systems. Rather than changing the transmitter clock as in [11], in this work bandwidth adaptations are supported by selecting a set of sub-carrier groups for each frame

transmission. The sub-carrier group ordering is piggybacked by the receiver to the sender in each acknowledgment. Randomized hopping between different channel widths have been proved to increase robustness against jamming attacks of fixed bandwidths [14]. In this case, the hopping sequence used by the transmitter is known to the receiver, which recovers the per-packet channel width by means of a synchronization mechanism with the transmitter hopping sequence. In [15] the benefits of heterogeneous channel widths are achieved by configuring multiple coexisting networks working with different (static) channel widths. To speed-up the scanning of networks working on multiple channel widths, the authors propose to passively perform a temporal analysis of typical channel timings that can be related to the transmission bandwidth employed in each network (such as the duration of acknowledgment transmissions or the DIFS interval).

2.2.2 Bandwidth aggregation/disaggregation

Another form of channel width modulation is represented by the possibility of dynamically aggregating multiple channels or splitting a channel into sub-channels. Channel aggregation is obviously very promising for increasing the available data rates, especially with the recent 802.11ac extensions which allow to aggregate up to 160 MHz of spectrum, but it suffers of severe interference problems caused by the coexisting networks working on each of the elementary channel under aggregation. Several research papers have considered how to ensure fair and efficient access to the non-contiguous spectrum [16], as well as how exploiting channel bonding in multi-hop environments [17]. Coordination between stations working on potentially overlapping channels is performed by using a primary channel for contention, by means of the so called dynamic channel access [16], or by explicitly notifying spectrum occupancy information to the intended receiver and transmitter in extended RTS/CTS frames [18]. Unlike these solutions, we do not require explicit signaling mechanisms between the contending nodes or each couple of transmitters and receivers.

Recently, the attention for channel disaggregation has been motivated by the possibility of achieving better spectrum utilization, whenever multiple narrow channels can be used independently at the same time. A pioneering work in this direction is WiFi-NC [19], where the concept of abstracting a single wideband radio into multiple narrow band sub-radios, called *radiolets*, has been demonstrated in a real prototype. Obviously, the possibility of performing independent carrier sensing as well as transmission and reception operations in each sub-radios is enabled by an increased complexity of the radio architecture. A similar approach, organizing a single OFDM channel into narrower sub-channels is proposed in [20]. However, in this work sub-channels are not completely independent, because carrier sensing works on the entire bandwidth and a contention phase is performed in parallel on multiple sub-channels, after an idle DIFS time, by means of special RTS/CTS signals. The result of the contention phase is a schedule of nodes that are

allowed to simultaneously transmit on each sub-channel, notified by the Access Point. Also in our work, carrier sensing works on the entire bandwidth, but transmissions on each possible sub-channels are not necessarily synchronized in time, nor coordinated by a common Access Point.

Finally, another mechanism for OFDM-based bandwidth disaggregation has been proposed in [21] for improving the coexistence of wide-band nodes with narrow-band interfering signals. In this work, the authors design a special radio able to split the spectrum in chunks, detecting chunks interfered by narrow-band transmissions, and then weaving together the unused (non-contiguous) bands by transmitting data bits only on the unoccupied frequencies. This approach is very different from ours because nodes still use the entire available, and potentially wide, band as a single channel.

2.3 Motivating Examples

Apart from the obvious benefits of improving link-level performance, the possibility of supporting in-band spectrum agility can lead to many others network-level benefits. In this section, we present some interesting, non exhaustive, use cases in three exemplary scenarios: a fully-connected network, in which in-band spectrum agility can be exploited for enabling parallel link operations; a multi-hop network, in which in-band spectrum agility can significantly reduce collisions due to hidden nodes and flow starvation; a multi-technology network, in which in-band spectrum agility can improve the coexistence with heterogeneous technologies.

In all these scenarios, we argue that the utilization of agile nodes can boost the network performance. According to the sampling rate and digital processing capabilities of the nodes, multiple channels can be obtained by partitioning a traditional 20 MHz channel into a few sub-channels, or by aggregating contiguous channels in a consecutive spectrum portion to be continuously monitored. Within the configured spectrum portion, agile receivers are able to work on the whole bandwidth or to switch from one sub-channel to another, as a result of the spectral analysis of each received preamble and different decision logics exploited by the access protocols.

2.3.1 Fully-connected networks

The adoption of multiple channels in fully connected networks can be effective for increasing the network capacity in case different links can work concurrently, and for reducing the collision rate in case of high-density networks. Consider first a simple ad-hoc network of 4 nodes. Being the network fully connected, in normal conditions only one link can be active at a given time instant, even if traffic flows exist between independent node pairs. By configuring each pair of nodes on a different channel (e.g. blue and red channels in Fig. 2.3(a)), the capacity can be doubled. However, for achieving this

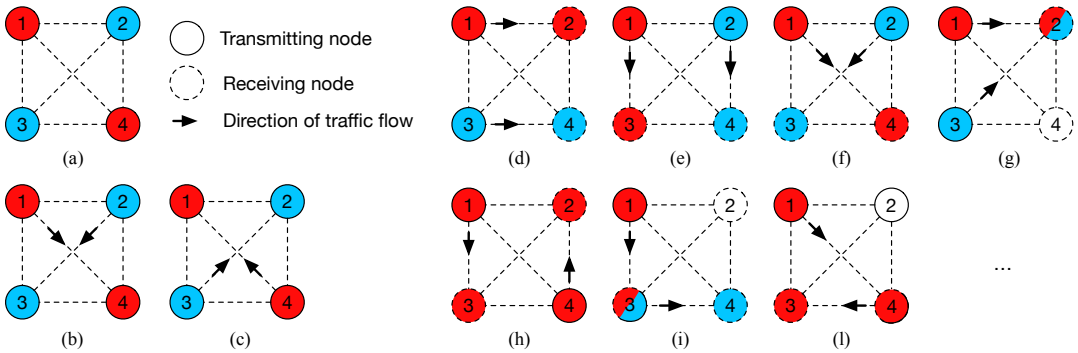


FIGURE 2.3: Topology flexibility in a fully-connected reference scenario coloring scheme on transmissions (a), the two possible flow layouts in case this fixed color scheme is also static at the receiver (b) and (c), and a selection of the possible traffic flows in case of fixed coloring at the transmitters and dynamic coloring at receivers (d)-(l).

configuration, a common control channel and configuration protocol has to be adopted. Once the nodes are colored as shown in the figure, only traffic flows between nodes 1 and 4 or nodes 2 and 3 can be accommodated in the network, unless a new coloring is performed. Being traffic flows highly dynamic, reconfigurations can be frequent and consume significant network capacity. Conversely, if nodes are based on our agile architecture, channel allocations at the transmitter nodes do not prevent receivers from automatically switching from one channel to another. In other words, after an initial coloring of transmitter nodes, receivers can dynamically adapt their colors to follow the time-varying traffic flows sent by the transmitters, as shown in some representative examples of Fig. 2.3(d)-(l).

Note that, in case two nodes transmit with different colors to the same receiver as shown in Fig. 2.3(g), the network continues to work properly: when the frames do not overlap, the receiver will hop from one channel to another during the preamble reception. In case of collisions, the first preamble will force the receiver to switch to a given sub-channel, thus resulting in a *"capture effect"*, regardless of the power ratio of the colliding frames. During the reception of the frame, other preambles can still be detected, but the receiver will continue to demodulate the ongoing frame.

Although our current implementation does not allow the simultaneous reception on multiple sub-channels, in principle it is possible to make some nodes (e.g. the Access Points) more complex, by adding multiple receiver chains to be activated at each preamble detection (similarly to [19]). In these conditions, the agile architecture can be effective for reducing the collision probability in high-density node scenarios. Rather than dividing the channel in sub-intervals to be allocated to different node groups [22], nodes could pick randomly one sub-channel after experiencing high collision rates, without following any pre-defined schedule of access intervals permitted to each node.

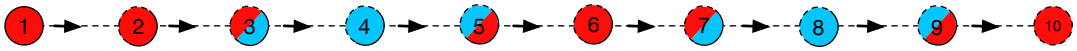


FIGURE 2.4: Multi-hop chained linear topology. Static coloring of transmissions according to the red-red-blue-blue pattern and the corresponding dynamic coloring scheme for dynamic reception.

2.3.2 Multi-hop networks

The use of multiple channels is also beneficial for multi-hop networks, whose performance are generally impaired by hidden node phenomena. Multiple channels permit to split collision domains and reduce collision probability. As an exemplary multi-hop network, we consider the linear chain topology shown in Fig. 2.4, which is composed by ten nodes in a row. For sake of presentation, the figure shows only flows oriented from left-to-right (although most of the considerations can be generalized to other types of traffic flows). Assuming that carrier sense range and transmission range coincide and are equal to one hop between consecutive nodes, the best coloring solution with two channels only is given by the regular pattern shown in the figure. Indeed, with this coloring, hidden nodes, whose distance is two hops (e.g. nodes 1 and 3), always employ different colors. The adoption of the agile transceiver allows to implement such a coloring without using multi-radio nodes. Indeed, nodes can receive on multiple channels, although not concurrently, and forward the frames using a different color. For example, node 3 will tune on the blue channel for receiving the frames transmitted by node 2. In case a reception from node 4 is active on channel red, node 3 is still able to detect a preamble sent on channel blue and decide to stop or not the ongoing reception, switching to the new channel.

2.3.3 Coexistence of multiple technologies

Bandwidth adaptations are very well consolidated in the context of cognitive networks, where multiple unplanned networks can coexist. Similarly, in ISM bands, they can be very useful, especially in the emerging scenarios of spectrum overcrowding and new incumbent technologies, such as LTE in unlicensed bands (LTE-U), which may pose serious coexistence problems with WiFi. In fact, it has been shown that LTE-U communications working on small bands[1] may harm WiFi communications on 20 MHz bands, if they overlap as shown in Fig. 2.5(a). Additionally, it has been demonstrated that WiFi transmissions are impaired by LTE frames, even when the listen-before-talk functionality is adopted, because of the intrinsic differences in sensing capability and access timings of the two standards [23]. Therefore, reducing the bandwidth of WiFi for avoiding the interference with a coexisting LTE-U network could be more effective than inter-technology contention on the

[1] LTE-U uses bandwidths of 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz, and 20 MHz

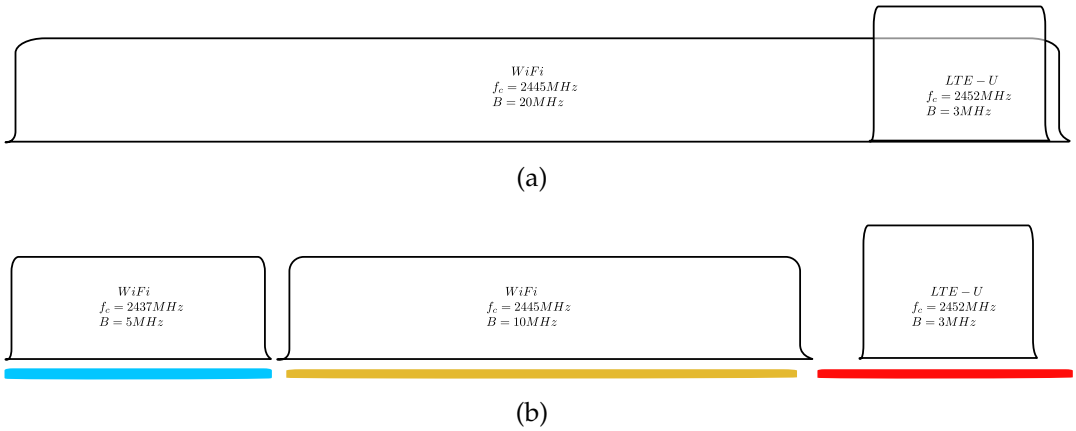


FIGURE 2.5: WiFi is killed by LTE-U when they coexist on the same 20 MHz channel (a) Two WiFi transmissions and one LTE-U peacefully coexist because of the band split (b).

whole bandwidth. Fig. 2.5(b) shows a possible solution of spectrum allocations, assuming to organize a traditional 20 MHz channel into 4 sub-channels (blue, red, yellow and green) of 5 MHz each.

2.4 Transceiver Architecture

In this section, we present an innovative transceiver architecture, obtained with minimal modifications on a WiFi OFDM transceiver, devised to support spectrum agility within a pre-defined WiFi channel. The architecture has been prototyped on top of the well known WARP research board. Because of the board hardware constraints, in our implementation the total bandwidth available for spectrum agility is 20 MHz.

At the transmitter side, channel width adaptations are implemented by simply scaling the basic clock of the system (80 MHz for the WARP board) to a desired output clock by means of a dynamic reconfiguration port, responsible of mapping a selection signal received by an external decision logic into the parameters required for scaling the clock. An optional shift of +/-5 MHz from the central frequency can be performed by opportunistically reconfiguring the register responsible of tuning the carrier frequency. At the receiver side, we considered more general extensions of a typical OFDM receiver, devised to enable the correct identification of the channel width and central frequency of an incoming frame within the reception of the short OFDM preamble. As we will explain shortly, we modified the peak detection block of an OFDM receiver working with fixed channel width, for taking into account that the preamble duration is not known, and we added an FFT block for performing a preliminary spectral analysis of the received signal when a preamble is detected.

2.4.1 Main Functional Blocks

The fundamental difference from non-agile transceivers is given by the possibility of dynamically tuning the system clock. The tuning of this parameter, implemented by writing opportunistically on some hardware registers, is decided as a function of the outputs of some correlation blocks and FFT analysis of the preamble.

Peak detection. The legacy 802.11 short preamble has a periodic structure with 10 identical symbols, each one lasting $0.8\mu s$, $1.6\mu s$ or $3.2\mu s$ in case the channel width is set to 20 MHz, 10 MHz or 5 MHz. Usually, OFDM receivers detect the beginning of a short preamble by identifying this periodic structure, i.e. by correlating two windows of signal samples corresponding to two consecutive symbols. Working at a fixed sampling rate of 20 Msample/s, a preamble symbol includes 16, 32 or 64 samples according to the channel width used in transmission. Therefore, rather than working with a correlator whose window value is statically configured, we replicated the correlator blocks, in order to perform three parallel correlations on windows of 16, 32 and 64 samples. The channel width of an incoming frame can be estimated by observing the minimum window size which gives a high correlation result. The total detection delay is 2 symbols, because two preamble symbols are enough for detecting the first correlation peak. For deciding if the correlation is positive or not, the correlation result is compared with a percentage of the sum of the modules of the first window W of samples used for correlation (i.e. with the theoretical correlation result in case of perfect periodic samples of the signal, $s(nT + WT) = s(nT)$ for $n = 0, \cdots W - 1$ and $T = 1/20\text{MHz}$).

Spectral analysis. In case a valid short preamble is detected, a spectral analysis of the sub-sequent preamble symbols is performed by means of a 64-point FFT. The number of preamble symbols required for collecting 64 samples is obviously dependent on the channel width, and in particular is equal to 4 symbols transmitted at 20 MHz, 2 symbols transmitted at 10 MHz and 1 symbol transmitted at 5 MHz. In the worst case, such an analysis lasts 4 symbols of the preamble, thus leading to a total time of 6 symbols before taking a decision on the channel width. The results of the FFT allows to immediately identify preambles transmitted with a central frequency different from the possible ones. Moreover, they also provide an additional evidence of the channel width used for transmission. Indeed, because of the preamble structure, sub-carriers with non-null coefficient appear in contiguous positions, spaced of two sub-carriers or spaced of four sub-carriers when the channel width is, respectively, 5 MHz, 10 MHz, or 20 MHz.

In our implementation, the decision logic works by comparing the sub-carrier amplitude with a threshold calculated by averaging the amplitude of 12, 18 or 24 sub-carriers around the central frequency and at +/-5 MHz. We chose to limit the average operation to these sets of sub-carriers, rather than considering the whole set of 64 sub-carriers, in order to discard the power of

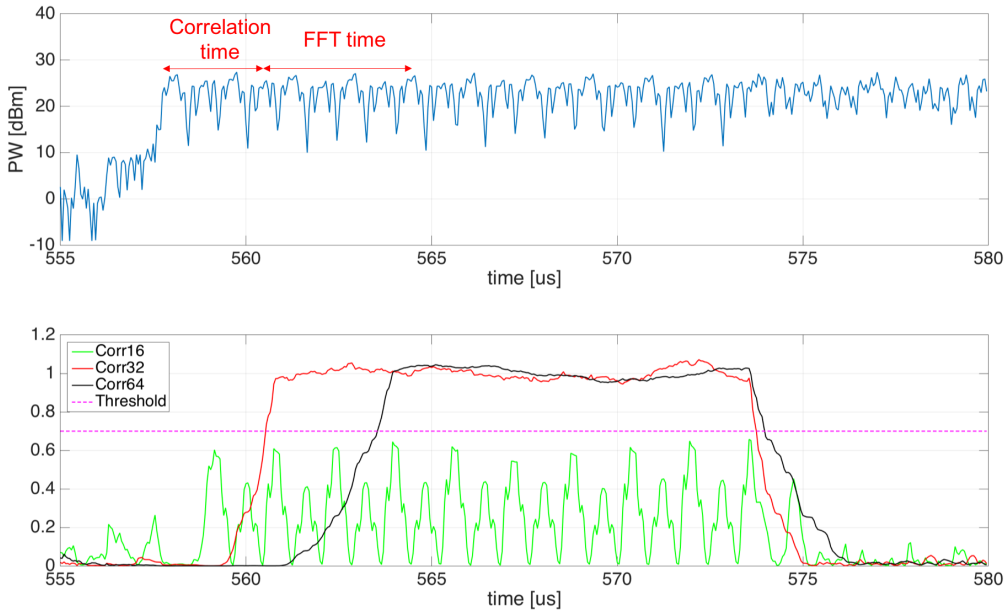


FIGURE 2.6: Preamble time and correlations.

interfering signals occupying adjacent bands. If six sub-carrier amplitudes are higher than the threshold in contiguous positions or spaced of a null sub-carrier or spaced of three null sub-carriers around all the possible central frequencies, the frame is recognized as a valid frame transmitted at 5 MHz, 10 MHz or 20 MHz. This result is used for reconfiguring the clock of the system and central frequency to be used for demodulation.

Fig. 2.6 shows the temporal structure of a short preamble (top part of the figure) transmitted at 10 MHz, and the parallel correlations of windows with 16, 32 and 64 samples (bottom part of the figure). Fig. 2.7(a) shows the results of the 64-point FFT. Both the correlation results and the FFT analysis allows to identify that the channel width of the incoming frame is set to 10 MHz; moreover, the FFT results indicate the position of the central frequency used in transmission.

Clock and Shift Reset. After completing the reception of the frame, the receiver switches the clock to the basic value (i.e. switch to the reference bandwidth of 20 MHz) and the central frequency to the default value (with zero shift). In case the receiver is the destination of the frame, the reset is deferred until the completion of the ACK frame transmission. In case the receiver is not the destination of the frame, the reception can be suspended after the demodulation of the frame header and the reset can be anticipated for enabling the reception of a new frame transmitted in other channel portions (non occupied by the frame under reception).

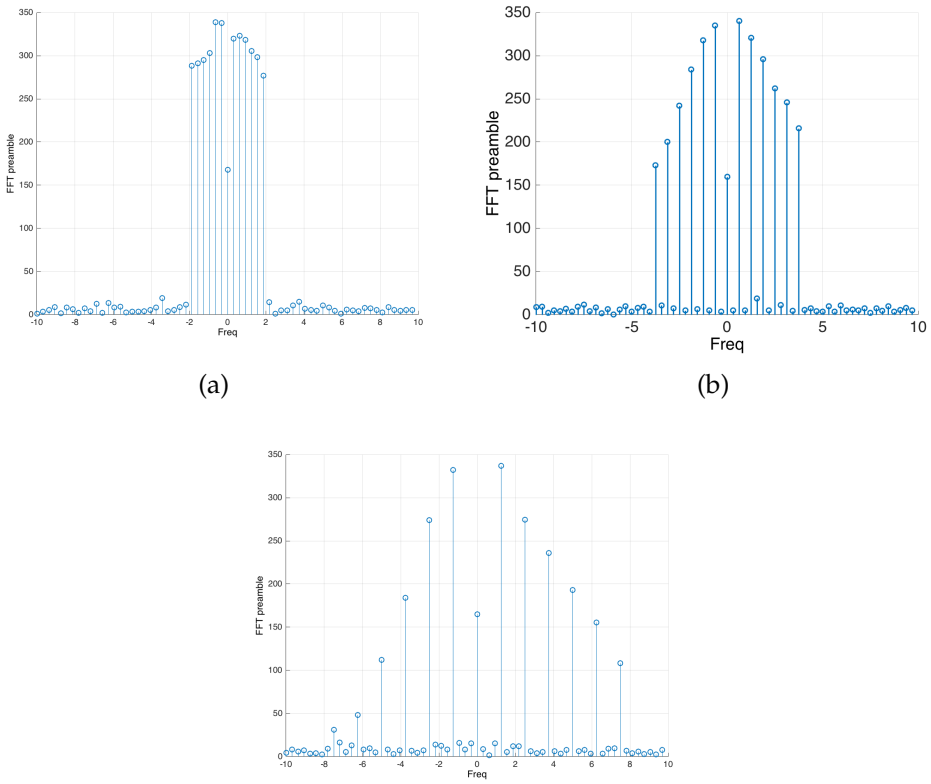


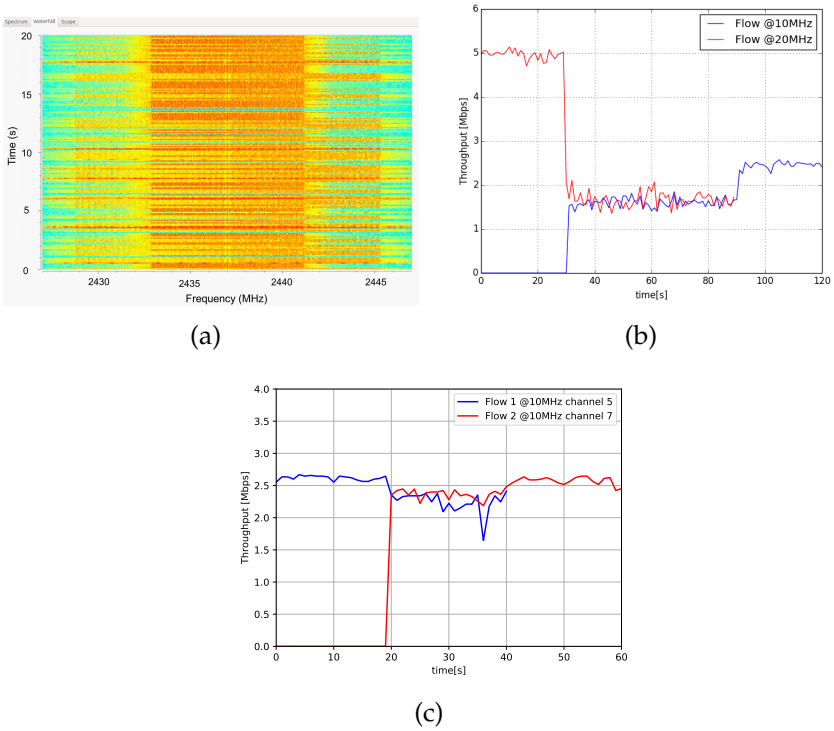
FIGURE 2.7: FFT shift of a preamble sent at (a) 5 MHz, (b) 10 MHz and (c) 20 MHz.

2.5 Functional Validation

Reconfiguring the channel width at each reception. We validated the receiver ability of correctly demodulating a sequence of frames without any a-priori knowledge about the channel width used by each one. We consider a simple network with three nodes only, devised to showcase the functionalities of our bandwidth-agnostic receiver: two senders, A and B, working on the same central frequency f_c, contend the medium for transmitting to a common receiver C. In this scenario, the sequence of channel widths experienced in consecutive frame receptions is unpredictable, due to the fact that transmitters A and B randomly win consecutive contentions. Therefore, even pseudo-random sequences of channel widths adopted by A and B cannot be mapped into a deterministic sequence of channel widths for the receiver.

Fig. 2.8 shows the results obtained when nodes A and B are statically configured for transmitting, respectively, at 20 MHz and 10 MHz, with a data rate set to 6Mbps, as shown in Fig. 2.9(a). In this set-up, we have the following percentage of correlations shown in Fig. 2.9(b) and the results in Fig. 2.8 show the temporal sequence of random spectrum occupancy due to the contention mechanism (Fig. 2.8(a)) acquired by a monitoring USRP node, and

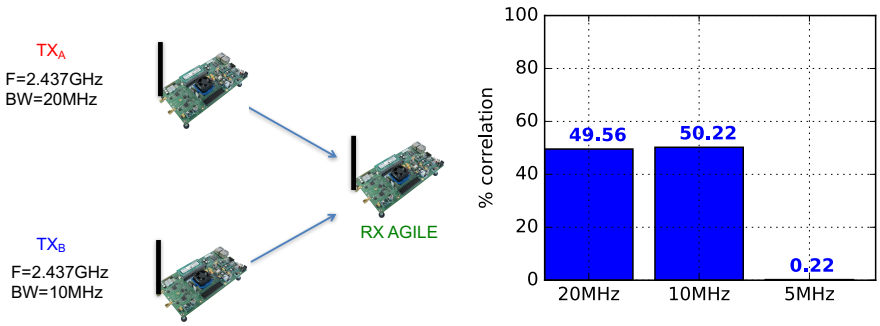
the throughput results (Fig. 2.8(b)) when only node A is active, both nodes A and B are active, and when only node B is active.



(a) (b)

(c)

FIGURE 2.8: Agile Receiver Performance: (a) waterfall, (b) throughput of two flows at 10 and 20 MHz at the same central frequency, (c) throughput of two flows at 10 MHz, whose central frequencies is spaced of 10 MHz.



(a) (b)

FIGURE 2.9: Agile Receiver Experiment: (a) set-up and (b) percentage of correlations.

The receiver is able to simultaneously work with both the transmitters, which achieve a similar throughput when both active, because of the performance anomaly phenomenon [24]. The average results, about 1.7 Mbps for each link, are equivalent to the coexistence of 2 flows with a link at 20 MHz

and a doubled frame transmission time.

Enabling the operation of two 10 MHz links in the same 20 MHz channel. We validated the possibility of using a contiguous spectrum portion of 20 MHz as two adjacent independent channels of 10 MHz or 5 MHz. Indeed, the use of partially overlapped channels has already been demonstrated beneficial for WiFi networks in many scenarios, despite the fact that OFDM systems suffer of high out-of-band radiation. For this validation, we configured two pairs of nodes in proximity statically using a frequency shift of 5 MHz (flow 1) and -5 MHz (flow 2) respect to the frequency f_c, and a channel width of 10 MHz. Fig. 2.8(c) shows the throughput results obtained when only flow 1 is active, both flows are active, or only flow 2 is active. The simultaneous operation of the two links leads to a minor throughput degradation. In case one of the links is configured for working at 5 MHz, the inter-link interference is much smaller and the results (not shown for space reasons) are completely equivalent to the ones obtained in isolation.

Switching from one sub-channel to another. We first tried to quantify all the latency components required for reconfiguring the transmission or the reception sub-channel. In case the transmitter decides to change the configuration of the channel width and frequency shift, it is required to act on the clock, ADC block, decimator/interpolator block and initialization of the physical header fields. On the WARP board, ADC and decimator/interpolator blocks are configured via a SPI, whose clock is 40 MHz. Being the required data corresponding to a total number of 2 words of 24 bit, these configurations take 1.2μs. An additional delay of about 10 μs is due to the dynamic reconfiguration port designed for taking decisions from the upper protocol logic. Regarding the receiver, as previously discussed, the time required for detecting the channel width and frequency shift is lower than a 6 symbol times, which allow to complete the reconfiguration of the clock and frequency registers via the SPI by the end of the preamble.

Chapter 3

Hopping Pilot Tones

In this chapter, we present new techniques that allow being more robust to jamming attacks. These techniques take advantage of the flexibility in order to mitigate interferences and jammers. Hence, in this context the PHY layer flexibility is a key for security of any OFDM-based communication system.

3.1 Introduction

Nowadays, Wireless Local Area Network (WLAN) technologies based on the 802.11a/g/n/ac/ad/ax standards, 3GPP Long Term Evolution (LTE) and the very recent 3GPP 5G Release 15, the leading cellular broadband technology, all use Orthogonal Frequency Division Multiplexing (OFDM). The driving reasons of this massive use of this modulation technique are high spectral efficiency and robust performance in multipath environments. These features permit to have very high data throughput using a limited spectral bandwidth, in order to satisfy the continuously increasing mobile data demand.

Despite these benefits, OFDM is not robust from the point of view of security. The physical layer implementation of OFDM is vulnerable to different types of jamming strategies[25], where an opponent intentionally tries to jam the communication. In the contrary to modulation schemes such as direct sequence spread spectrum (DSSS) or frequency hopping spread spectrum (FHSS) which offer significant power advantages over jammers, the OFDM signals can be disrupted with low-power signals acting as interference. For this reason, the United States military even forbids the use of wireless metropolitan area networks (WMAN)[26] in adverse environments that rely on OFDM.

One of the fundamental reason for the vulnerability of OFDM to jamming attacks is the timing and frequency synchronization between transmitter and receiver which is necessary to avoid intersymbol interference (ISI), intercarrier interference (ICI) and the loss of orthogonality among OFDM subcarriers. For an optimum performance, estimation and equalization of the channel's frequency response at the receiver is done by the insertion of equal power and equally spaced pilot tones in the signal. The signal bandwidth is divided into multiple sub-carriers of fixed bandwidth and the synchronization is usually performed using predetermined training symbols transmitted each frame [27]. When an attacker knows these OFDM communication and synchronization parameters, it can interfere with a matched signal that maximizes the impact at the receiver. For example, since the channel impulse response is estimated and equalized using fixed pilot tones [28, 29], various efficient jamming attacks target these pilot tones [30] in order to destroy information used by the equalization algorithm. Another jamming strategy consists of interfering with the sub-carriers. Since the location and bandwidth of the active sub-carriers are known a priori, an attacker can disturb each sub-carrier by transmitting a matched signal on all the sub-carrier frequencies.

In this work, we propose and evaluate randomization techniques that render OFDM signals less vulnerable to jamming attacks. In order to make the signal less vulnerable to jammers that target the pilot tones, we propose to hop the pilot tone frequencies in a pseudo-random manner. To secure against jammers which interfere with the sub-carriers, we suggest to randomly activate/deactivate sub-carriers such that the attacker cannot follow the actual sub-carrier bands being used. In a sense, these randomization techniques take inspiration from classical FHSS modulation which randomly hops the signal in the coding or in the frequency domain to make the signal less predictable to an attacker. However, our approach is basically different and consists of randomly hopping the OFDM system parameters such that the attacker cannot match its signal according to an optimized jamming strategy which requires knowledge about these parameters.

We evaluate the performance and the power advantage of these OFDM randomization techniques in simulations and with a software-defined radio implementation. Our results indicate that in the absence of jamming, the OFDM bit error performance is almost identical with pilot hopping and randomized sub-carrier activation compared to a classical OFDM system while a power advantage of about 15 dB can be achieved when a jammer is active. We also develop and evaluate an adaptive algorithm which optimizes the data throughput depending for different levels of jamming.

We organize the remainder of this chapter as follows. Section 3.2 establishes related work. Section 3.3 presents a little OFDM background and studies the importance of the pilot sub-carrier for equalization. Section 3.4 studies the robustness of the standard OFDM in presence of five different jamming techniques in terms of BER performance. In Section 3.5 two solutions are describe to increase the performance in presence of different jamming strategies

by nulling some data sub-carrier and applying a hopping pilot OFDM-based system. Section 3.6 shows evaluation with simulation and real experiments in the air, that validates simulations.

3.2 Related work

Our purpose is to mitigate as much as possible some of the jamming strategies that are very problematic for an OFDM-based communication. Therefore, it is important to give a look at various jamming techniques and the solutions that have been developed so far.

The simplest attack techniques are based on the generation of intentional interference for a target OFDM link. Indeed, these types of attacks do not require additional information about the target and are optimal strategies in absence of any a priori knowledge about the target signals [31]. A jamming scheme generating intentional interference on the whole OFDM bandwidth is called broadband jamming, while when the interference affects only a part of the OFDM bandwidth (even with non-contiguous portions) is called partial-band jamming [32]. Partial jamming can be more effective than broadband jamming because it allows to focus the interference power on certain specific bandwidth. The effect of this type of jamming attack in presence of Rayleigh fading channel is analyzed in [33], while [34] studies the effect of nonlinear amplifiers combined with partial-band jamming. Finally, the effects of space-time coding for OFDM links in presence of jamming is explored in [35].

A more sophisticated jamming strategy is based on preventing channel estimation for the OFDM receiver. Channel estimation approaches for SISO and MIMO OFDM systems are summarized in [36], while some generalizations for non-regular pilot tone transmissions are presented in [37]. The devastating impact of imperfect channel estimation on the OFDM link performance is analyzed in [38], where it clearly emerges the vulnerability of channel estimation mechanisms based on regular pilot tones, which can be easily affected by narrow-band and partial-band jamming. Pilot jamming aims at exploiting this vulnerability, by increasing the noise floor of the target pilot-tones with Additive White Gaussian Noise (AWGN) signals transmitted at the same pilot tone frequencies. The fundamental assumption here is that the jammer has knowledge about the pilot frequencies used in the target OFDM link and is synchronized with the target. Analytical and simulation studies of pilot jamming are presented in[39] and in [40], where it is shown that attacking pilots is more power efficient than jamming the entire target signal. BER performance are derived in [41]. A number of other studies are available for assessing the impact of jamming attacks against SISO and MIMO channel estimation, such as [42, 43, 44] and [45, 46, 47, 48] respectively. Another approach for preventing channel estimation is based on pilot nulling [49],[50]. When the adversary has a more extended knowledge about the channel between the target transmitter and receiver and between itself and the target

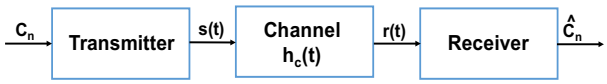


FIGURE 3.1: OFDM system.

receiver, it can transmit special pilot signals, nulling the reception of pilot tones at the intended receiver [30].

So far, countermeasures to OFDM attacks, such as coding/modulation, boosted pilots, frequency-hopping or permutation-based sub-carrier assignments, have been only partially characterized, mostly relying on analytical or simulation results [42].

3.3 OFDM Background

OFDM-based communication systems critically depend on the reception of pilot sub-carriers, which can be impaired by selective channels or by intelligent jammers. In this section, we first describe the principles of OFDM, then we explore the importance of pilot tones even in ideal channel conditions, by quantifying the bit-error rate achieved over the reference OFDM link as the number of pilot tones are gradually reduced to zero. Error distributions over different sub-carriers also show the impact of the distance between each data sub-carrier and the pilot tone. We then evaluate the impact of a realistic selective channel, which results in a non-uniform SNR value between different sub-carriers.

3.3.1 OFDM Primer

We take into consideration the generic OFDM system depicted in Figure 3.1. Let C_n be the complex symbols to be transmitted and the serial to parallel conversion $C_i^{[l]} = C_{lN+i}$ with $0 \leq l < N$ the groups of N elements with signaling frequency of $1/(NT)$. Then, $C_i^{[l]}$ are subjected to the Inverse Discrete Fourier Transform (IDFT) in

$$c_k^{[l]} = \frac{1}{N} \sum_{i=0}^{N-1} C_i^{[l]} e^{j2\pi \frac{ik}{N}}. \tag{3.1}$$

A linear modulated signal in a single carrier system can be described by

$$s_{RF}(t) = Re\left\{ \sum_{n=-\infty}^{\infty} c_n g(t - nT) e^{j2\pi f_0 t} \right\}$$

with $g(t)$ being the square-root raised-cosine pulse. If we model the channel with multipath as $h_c(t)$, the equivalent discrete-time channel response

$$h_{n,\epsilon} = g(t) * h_c(t) * g^*(-t)|_{nT+\epsilon} \tag{3.2}$$

where $g^*(-t)$ is the matched filter to the pulse shape of an usual OFDM receiver. This type of filter in the receiver side ensures that noise samples results independent. Hence, the received samples can be expressed as

$$r_n = \sum_{l=-\infty}^{\infty} \sum_{k=0}^{N-1} c_k^{[l]} h_{n-(lN+k),\epsilon} \tag{3.3}$$

where ϵ is the timing error due to the sampling error of the receiver.

In order to have a correct detection of transmitted data and to demodulate the OFDM signal, the receiver has to perform a channel estimation. There are different techniques that can be considered, but the most popular in the new generation of WLAN standards is based on sending reference signals within each transmitted symbol. More specifically, equal power and equally spaced pilot tones are inserted in each symbol at specific sub-carriers and the channel response is estimated in the frequency domain using FFT processing and by comparing received pilots with the locally stored reference pilots. Clearly, this approach requires that the receiver exactly knows the frequency position of pilot tones.

3.3.2 Importance of pilot tones

In order to understand the fundamental importance of pilot tones for OFDM links and why these tones make OFDM so vulnerable to jamming attacks, we simulate a transmission between a transmitter and a receiver starting from the limit case in which all the pilot sub-carriers are nulled.

For simulating the OFDM link, we implement a classical OFDM transmission using a 64-point Fast Fourier Transform (FFT), with 48 data sub-carriers and 4 pilot sub-carriers. We consider data packets lasting 500 OFDM symbols, under a Quadrature Phase-Shift Keying (QPSK) per-carrier modulation (i.e. packet length is $48 \cdot 2 \cdot 500 = 48000$ bits). The bit error rate (BER) performance is evaluated by averaging the results achieved in the transmission of 1000 packets.

Figure 3.2 shows the results achieved in presence of a flat channel (i.e. with a noise floor constant at each sub-carrier). It is possible to see that the absence of pilot tones is disruptive at any Signal-to-Noise Ratio (SNR), since the BER is always around 0.5. Instead, in presence of pilot tones, for SNR values lower than -10 dB, we can observe that the BER is about 0.5, while it is reduced down to zero when the SNR value is higher than 12 dB.

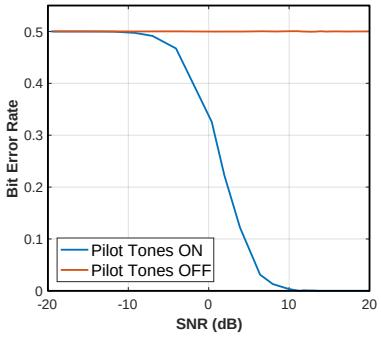
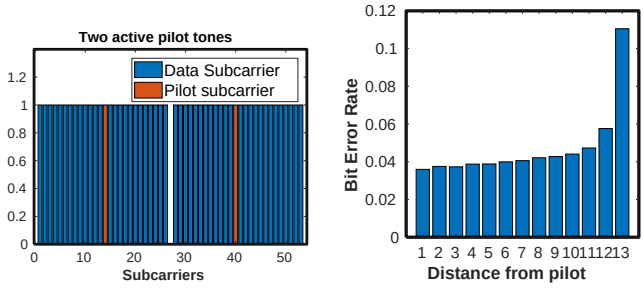


FIGURE 3.2: BER performance when varying the SNR.

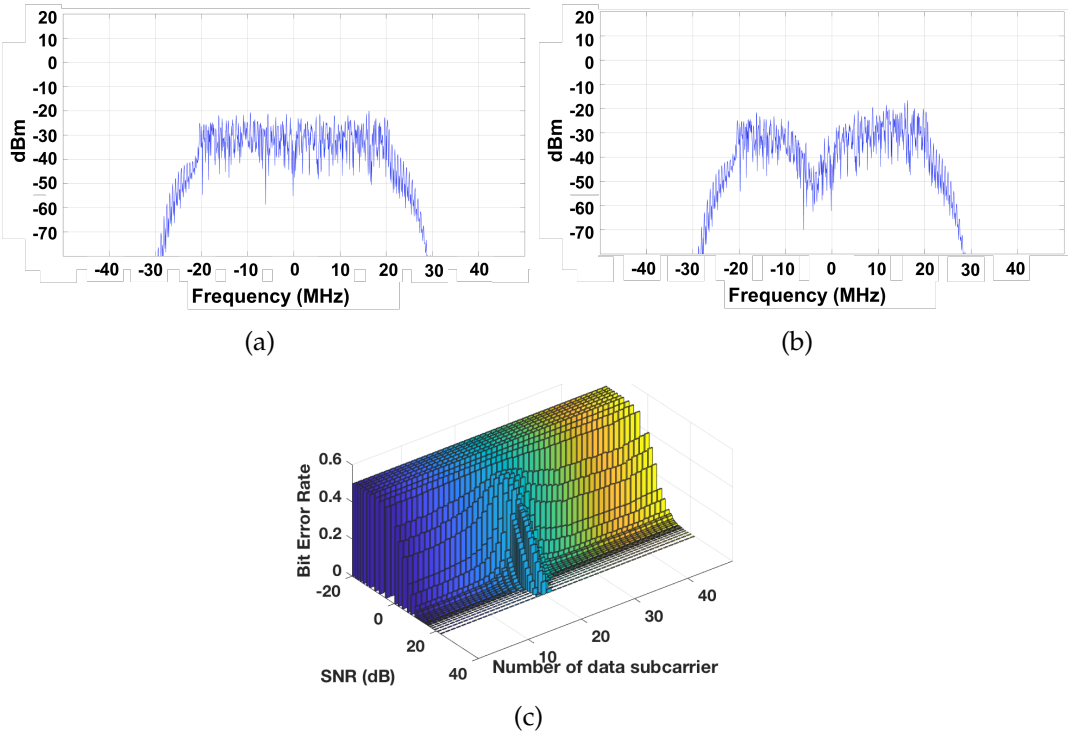


(a) (b)

FIGURE 3.3: Configuration data and pilot sub-carriers (a) and bit error rate (b) for data sub-carriers depending on the distance with the nearest pilot tone at 5 dB of SNR.

In case pilot tones are present, the distance between each data sub-carrier and the pilot tone can have an impact on the BER as well, i.e. bits transmitted at different sub-carriers do not experience homogeneous error rates. Figure 3.3(a) shows an OFDM configuration with two pilot tones only, while Figure 3.3(b) shows the BER disaggregated for different data sub-carriers for a reference SNR value of 5 dB. We observe that the BER increases with the distance from the pilot tones.

The last important investigation is understanding the behaviour of the BER for each data sub-carrier in presence of a selective frequency fading. In order to provide a visual representation of the phenomenon, Figures 3.4(a) and 3.4(b) represent the effect of the channel, by depicting the spectral representation of a reference packet before and after the application of a selective channel model. From the figures, it is evident that some sub-carriers on the left side of the bandwidth are affected by attenuation values much higher than the average ones. The impact of channel attenuation on BER performance is quantified in Figure 3.4(c), where there is a clear correlation between the channel model and the BER results achieved at different sub-carriers. Indeed, as the SNR value gets smaller, BER are not uniform, with worst results for the data sub-carriers suffering of higher channel attenuations.



(a) (b)

(c)

FIGURE 3.4: Spectral analysis before (a) and after (b) the channel model application and BER performance for each sub-carrier with the previous Frequency-Selective fading channel (c).

3.4 OFDM Performance under Jamming

In order to quantify OFDM vulnerability to imperfect channel estimation, we describe in this section the performance of a simulated OFDM link under different channel and jamming models. We analyze the impact of different jamming strategies acting on pilot tones and the effectiveness of a counter-measure based on reducing the number of data sub-carriers.

3.4.1 Jamming Strategies against OFDM

In our simulation study, we consider different jamming strategies proposed in the literature which can be divided in two main categories: (i) sub-carrier jamming and (ii) pilot tone attacks [25]. In sub-carrier jamming, the attacker interferes with noise to increase the noise floor of the data carriers and thus degrade the SNR. The noise is typically Gaussian, but any modulated signal will also effectively degrade the receiver performance. Broadband jamming and partial-band jamming fall in this category. Pilot tone attacks can be based on pilot jamming or nulling, i.e. the adversary can transmit AWGN signals to constructively interfere with the pilot tones or destructively null the pilot tones. In the category of pilot tone jamming, the attacker interferes with the

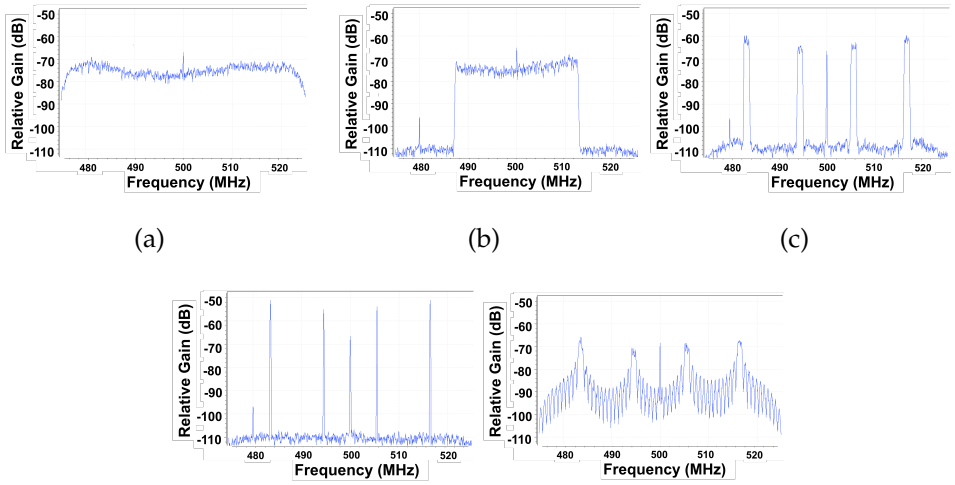


FIGURE 3.5: Attack strategies adopted: broadband jamming (a), partial-band jamming (b), pilot tone jamming (c), pilot nulling jamming (d) and pilot random-phase jamming.

pilot tones of the OFDM signal. These attacks are generally more effective because they require less power to damage and destroy the OFDM transmissions. By interfering with the pilot tones, an attacker will render the pilot tones useless for synchronization and channel equalization. Pilot tone jamming can be performed by generating very narrowband signals at the pilot carriers or by adding sinusoid signals (i.e. tones) with random phase in two ways [25].

In the following, we refer to broadband jamming as BBJ, partial-band jamming as PBJ, pilot tone jamming as PTJ, pilot random-phase jamming as PRJ, and pilot nulling jamming as PNJ.

3.4.2 Jamming Performance Evaluation

To better understand the impact of the different jamming strategies, we present here simulation results. The power spectral density of the different jamming strategies is shown in Figure 3.5. For PBJ, the jamming band covers half of the sub-carriers of the packet; for PNJ, the jamming attack covers only the pilot tones and it is created by the sum of four sinusoids opposite in phase to the pilot tones, while PTJ is created by filtering an AWGN signal near the pilot tones frequencies and finally PRJ is formed from four sinusoids in correspondence of the four pilot sub-carriers, but with a random phase for each symbol of the packet.

Simulations are executed for 1000 iterations for different Signal-to-Jammer Ratios (SJR). For all contexts the SNR is fixed to 30 dB. Figure 3.6 shows the result of the simulations. As expected, the pilot nulling jamming is the most

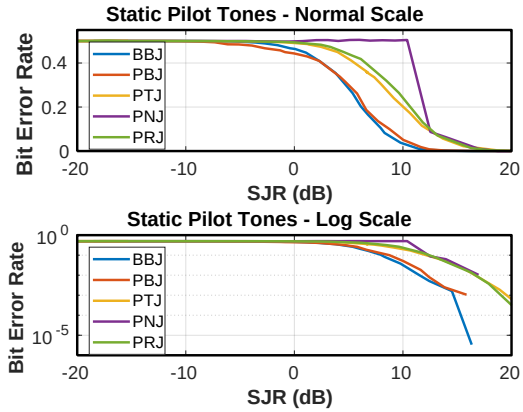


FIGURE 3.6: Performance of the five jamming strategies at 30 dB of SNR with static pilot tones.

effective method to destroy the communications in a OFDM-based system. This is due to the fact that the receiver fails the equalization and then the decoding, because the equalization information carried by pilot tones is disrupted. In general, we can say that a relatively high SJR above 10 dB is required for all jamming strategies in order to produce tolerable bit error rates. In other words, a jammer with 10 dB less power than the legitimate communication signal can still take down the OFDM transmissions. This clearly shows that OFDM is highly susceptible to jamming compared to other modulation forms such as DSSS or FHSS. These latter modulations are supposed to still perform well even when the SRJ is below -20 dB [51, 52]. In the next section, we will present two signal randomization techniques which improve the resistance of OFDM for all jamming strategies.

3.5 Mitigation Solutions

We propose two countermeasures which in combination make the OFDM signals more resistant to jamming attacks. Both solutions are based on randomization techniques. The first solution is devised to improve channel estimation robustness, by adopting a randomized hopping of the pilot tones in order to prevent the pilot jamming. The second solution is devised to improve the SNR experienced by data sub-carriers, by randomly choosing a sub-set of the available sub-carriers, in order to increase the transmission power on each active carrier. This section describes the attacker model and the design of both mitigation solutions.

3.5.1 Attacker Model

The jammer is assumed to be in transmission range of both the transmitter and the receiver, so that he can overhear the signals from the transmitter as well as interfere with its own signals at the receiver. For this, the jammer

may rely on half duplex or full duplex radios [53]. Regardless of the radio type, we assume that the jammer has reactive capabilities, i.e., the jammer can sense the channel and interfere with a signal based on the sensed channel information [54].

We assume the jammer reaction time to be lower-bounded. We denote the time difference between the arrival of the original signal and the jammer signal at the receiver as the jamming reaction time τ. The minimal reaction time τ_{min} is bounded by the sum of (i) the signal propagation delay between the sender and the jammer, (ii) the hardware and software reaction delay of the jammer to process the incoming signal and to make a jamming decision, and (iii) the signal propagation delay between the jammer and the receiver. It is therefore safe to assume that the minimum reaction time τ_{min} is greater than the duration of one OFDM symbol [54].

Both the legitimate transmitter and the jammer are assumed to have infinite energy but have a limited transmission power budget. The jammer can thus interfere with any signal waveform and an arbitrary signal bandwidth, as long as it does not exceed its power budget. In order to attack on a classical OFDM without any randomization, the jammer may therefore sense the location of the pilot tones and the active sub-carriers and react with a jamming signal, e.g. an AWGN signal, that interferes with only the pilots tones or the data sub-carriers that are active.

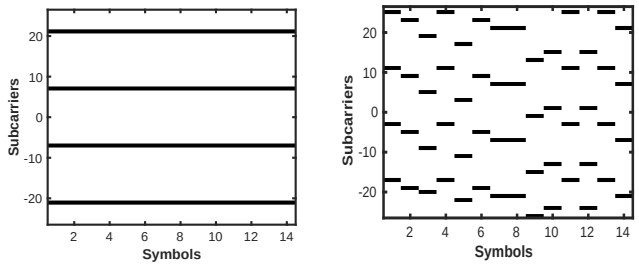
3.5.2 Hopping Pilot Tones

To prevent jamming strategies which attack the pilot tones, we propose to dynamically change the position of the pilot tones symbol-by-symbol. Our assumption is that if the receiver knows the pilot hopping pattern, it is still able to use the pilots for synchronization and equalization and to correctly decode the signals.

In the OFDM modulation used by the 802.11a/g standards, the total number of active sub-carriers is 52, with two groups of 26 sub-carriers around a null central sub-carrier. Numbering sub-carriers with index from -26 to 26, pilot tones are identified by positions -21,-7,7 and 21, while all the other sub-carriers are used for data. Pilot tones are represented by BPSK symbols, while data sub-carriers are modulated with an QPSK modulation and mapped to complex values.

Rather than considering a fixed mapping between pilot and data sub-carriers, we design a scheme in which such an assignment is dynamic. For simplicity, we consider a randomization scheme which maintains an equal spacing between the pilot tones. Figures 3.7(a) and 3.7(b) show the difference between the static and dynamic approach in 14 consecutive data symbols.

To synchronize the pilot hopping pattern between the transmitter and the receiver, we rely on pre-shared secret keys from which the pattern can be



(a) (b)

FIGURE 3.7: Standard (a) and hopping (b) pilot tones.

derived [55]. An alternative would be to rely on unsynchronized pattern discovery schemes [56].

3.5.3 Randomized Sub-carrier Activation

Our second countermeasure is to dynamically activate and deactivate individual data sub-carriers in order to increase, when needed, the SJR available for each one. When we do this randomly, on a symbol-by-symbol level, the jammer cannot guess which sub-carriers will be activated at a given point in time and therefore cannot implement effecting strategies of partial-band jamming. Obviously, using a reduced number of sub-carriers implies a reduction of the achievable data rate; however, because of the increased SJR ratio due to the transmission power spread over a smaller bandwidth, it generally corresponds to a reduction of the BER. Consider for example an OFDM system with n sub-carriers and a transmitter with a power budget of P. The power per sub-carrier is therefore P/n. By deactivating half of the sub-carriers, the transmission power of the remaining sub-carriers is doubled leading to a power of $2P/n$ per sub-carrier. Assuming a broadband jammer (BBJ) with a fixed overall power budget of J, the jamming power per sub-carrier is J/n. By deactivating half of the sub-carriers, the SJR per sub-carrier is thus increased by a factor of 2, or 3 dB. The SJR can further be increased by reducing the number of active sub-carriers up to a single active sub-carrier. In the case of one active sub-carrier, the SJR is increased by a factor of n. If we assume an OFDM system with 64 sub-carriers, we can thus improve the SJR by up to 18 dB.

The challenge of this approach lies in finding an optimum sub-carrier activation factor F for a given jammer power J. As the throughput decreases when individual sub-carriers are deactivated, we have to trade-off jamming resistance against throughput. Let us assume that the signal can be decoded on each sub-carrier when the signal-to-noise-plus-jamming ratio (SJR) is above a certain threshold δ. The goal of the transmitter can then be formulated as

an optimization problem:

$$\begin{aligned} \underset{F}{\text{maximize}} \quad & \text{throughput}(F) \\ \text{subject to} \quad & SJR > \delta, 1 \leq F \leq n. \end{aligned}$$

In other words, the goal is the reduce as few sub-carriers as possible in order to obtain an SJR above the minimum required value to be able to decode the signal at the receiver.

To solve this problem, we propose an adaptive algorithm at the transmitter which relies on the feedback from the receiver. In our adaptive algorithm, the initial value of the percentage of active data sub-carriers is Pr $= 100\%$. In case that the receiver can decode the signal, it acknowledges the reception and the transmitter continues to activate all sub-carriers. In case, the transmission is not acknowledged successfully by the receiver, the transmitter decreases a random set of active sub-carriers. A decrease in the number of active sub-carriers, will improve the SJR at the receiver and the likelihood that the receiver is able to decode the data. If the receiver successfully acknowledges the transmission, the transmitter will remain at this activation rate. Otherwise, it will further decrease the sub-carrier activation rate until it receives a successful acknowledgment from the receiver, or until only one sub-carrier is active. In the latter case, the jammer is so strong that it is not possible to mitigate its impact and additional anti-jamming techniques such as for example directional antennas or beam-forming would be necessary which is outside the scope of this work. To adapt to temporal changes in the channel, the transmitter should periodically increase its sub-carrier activation rate to test if the channel conditions have improved.

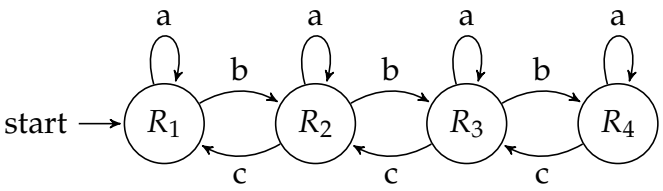


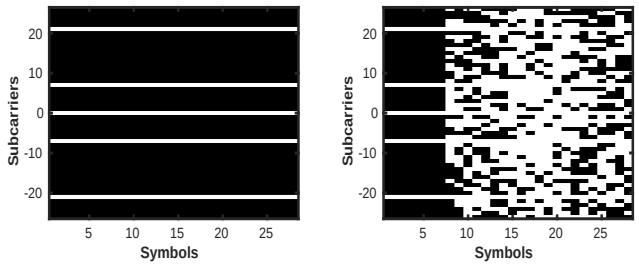
FIGURE 3.8: Final state machine of the adaptive algorithm at the transmitter.

Except for $Pr = 100\%$, the data sub-carriers are selected randomly across all the possible data sub-carriers. An exemplary implementation of the algorithm is shown in Figure 3.8 as a finite state machine, whose states represent the rate of data sub-carriers activated by the transmitter at a given time, while transitions correspond to the receiver feedbacks, i.e. to the throughput reported by the receiver as specified in Table 3.1.

Consider N as the number of transmitted packets in order to calculate the Packet Error Rate (PER). Every N packets, the transmitter calculates the normalized throughput as $thr_{F_r} = 1 - PER$. Let R_{F_r} be the normalized data transmission rate for a given data sub-carrier activation ratio F_r, T a counter and t a certain threshold that can be tuned to tradeoff adaptation reactivity

	Events
a	if $R_{F_r} > thr(R_{F_r}) > R_{F_{r+1}}; T++$
b	if $thr(R_{F_r}) < R_{F_{r+1}}; T = 0$
c	if $thr(R_{F_r}) = R_{F_r}$ & $T > t$

TABLE 3.1: Events of the finite state machine.



(a) (b)

FIGURE 3.9: Standard (a) and randomized (b) data sub-carriers location.

versus stability. Based on the normalized throughput, the transmitter takes three different decisions, as shown in Table 3.1: (i) if thr_{F_r} is between R_{F_r} and $R_{F_{r+1}}$, it means that the transmitter cannot improve its throughput by deactivating sub-carriers; hence, the transmitter holds the current state and increments T by 1; (ii) if thr_{F_r} is smaller than $R_{F_{r+1}}$, it means that the throughput can be improved by deactivating sub-carriers. The transmitter thus moves its state to $R_{F_{r+1}}$ and resets T to 0; (iii) if thr_{F_r} is equal to R_{F_r} and T is larger than t, the transmitter moves its state to $R_{F_{r-1}}$ in order to test if the channel conditions are still the same or they have improved. Obviously, the reactivity of the algorithm depends on the value of t, i.e. for small values, the algorithm will probe more often states with higher sub-carrier activation rates.

Figures 3.9(a) and 3.9(b) show the difference between the static and dynamic approach in 24 consecutive data symbols. More specifically, in Fig. 3.9(b), the configurations selected by the algorithm are $Pr = 100\%$, $Pr = 50\%$, $Pr = 25\%$ and $Pr = 50\%$ respectively. Except for $Pr = 100\%$, it is possible to note that the data sub-carriers are random on a symbol-by-symbol level.

3.6 Evaluation of mitigation solutions

In this section, we present numerical results of the proposed countermeasures devised to improve OFDM resilience in presence of different jamming strategies, obtained in simulations and in real experiments. For running these experiments, we implemented both the pilot hopping scheme and the dynamic tuning of the number of active sub-carriers on top of the USRP Software Defined Radio platform (SDRs) platform.

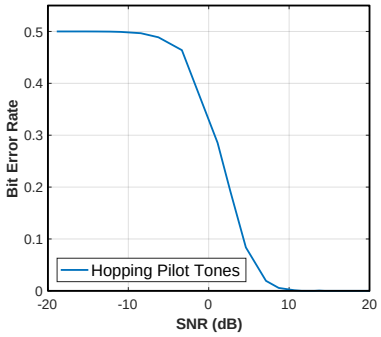


FIGURE 3.10: BER performance when varying the SNR in case of hopping pilot tones.

3.6.1 Effects of Pilot Tone Hopping

A. Simulations We developed a simulation-based OFDM system with a simple channel model, based on AGWN additive noise, in which different jammer attacks are considered. The OFDM modulation uses a 64-point FFT with a cyclic prefix length of 1/4. Deterministic assignment of pilot tones is based on the selection of 4 tones at fixed positions, while dynamic assignment is based on the regular right shifts at each symbol transmission.

In absence of jamming and assuming that the transmitter and the receiver employ a synchronized hopping sequence, the dynamic shift of pilot tone positions do not have an effect on the BER performance. Indeed, if we compare the BER simulation results depicted in Figure 3.10 under dynamic pilot hopping with the same curve depicted in Figure 3.2 under static assignment of active pilots, we can observe that the results are practically the same.

Results are obviously very different in presence of jamming signals. In order to quantify the performance improvements that can be achieved under pilot hopping, we set-up an OFDM link with a high SNR value (i.e. 30 dB) and attack the received signal with the different jamming strategies summarized in Figure 3.5. For implementing the jamming attacks, we combine the reference and jamming signal at the receiver, before running the usual receiver processing chain (which includes the FFT and signal equalization based on linear interpolation of the channel coefficients estimated on the pilot tones). Simulations are executed for 1000 iterations and for different SJRs. BER results are summarized in Figure 3.11 for each jamming technique under both static and dynamic pilots.

From the figure, we can draw some interesting observations. First, jamming techniques based on the generation of additional intentional interference, such as BBJ and PBJ, as expected, are not affected by the adoption of dynamic pilots. Indeed, the BER results for a given SJR value are the same under both static and dynamic pilots. Conversely, BER curves obtained under PTJ and PRJ jamming strategies have an improvement by adopting dynamic pilots: the attacker has to increase the jamming power of about 5 dB for achieving the same BER results obtained in case of static pilots. Note also

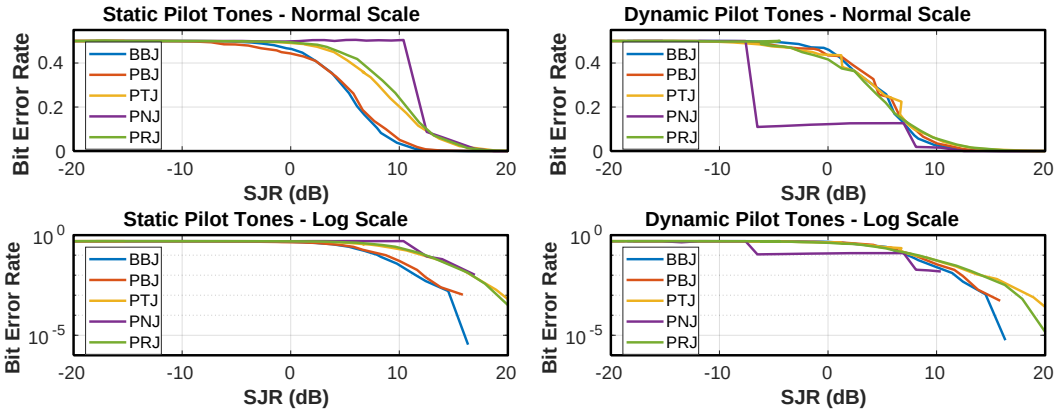


FIGURE 3.11: Performance in simulations of the five jamming strategies at 30 dB of SNR with dynamic pilot tones.

that using dynamic pilots make the behaviour of PTJ and PRJ attacks comparable to BBJ and PBJ for SJR values lower than 16 dB. Conversely, with the PNJ strategy, there is a consistent enhancement, more specifically of about 15 dB. Under this circumstance, the sum of the amplitude of the four sinusoids is always the same symbol-by-symbol which is why this type of jamming attack has a threshold behaviour at about -7 dB, where the corresponding value of BER is about 0.14. This specific value is due to the fact that, for simplicity, the simulation was made with a random pattern of the pilot tones from 7 possible patterns, in which one pattern corresponds with the pattern adopted in the standard. Hence, PNJ strategy attacks data sub-carriers in the $6/7$ of cases, while it attacks pilot sub-carriers in only the $1/7$ of cases (i.e. BER is $6/7 \cdot 4/48 + 1/7 \cdot 0.5 = 0.1429$). We can note that there is another threshold behaviour at about 8 dB of SJR, because pilot tones are not affected by the jammer since the contribution of PNJ is very low.

The reason why PNJ has a different behaviour than PTJ and PRJ is due to the amplitude. The pilot nulling jamming strategy is formed from the sum of four sinusoids with constant amplitude, while in PTJ and PRJ the resulting amplitude is variable. In both cases, the four components are different symbol-by-symbol and the combination of them gives a variable amplitude. In some cases, this behaviour causes a wrong channel estimation made through the preamble Long Training Symbols (LTS) that damages the correct decoding of the packet. In fact, in a OFDM system, the first stage of packet detection uses an auto-correlator that asserts on the Short Training Symbols (STS) of the 802.11 preamble. Then, after the assertion of the auto-correlation packet detector there is a 64-point complex cross correlator matched to the preamble LTS. This correlator asserts when two sequential 64-sample LTS are observed in the incoming samples. If the correlation succeeds the receiver pipeline is enabled. The probability of a false positive in this stage is very small. Moreover, LTS is also used for channel estimation [57].

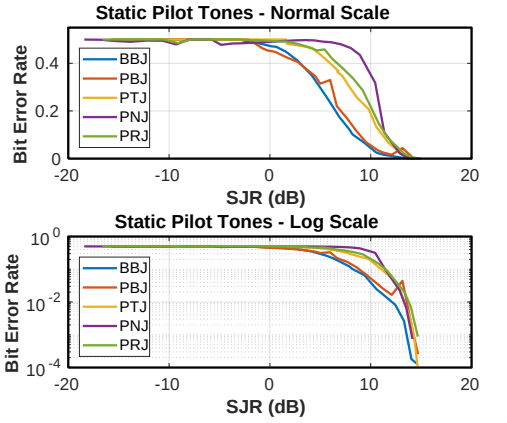
B. Experimental Validations In order to analyze the impact of the proposed countermeasures over real channels, we performed experiments with two software-defined radios USRPs X310: the first one, acts both as transmitter and jammer, while the second one acts as a receiver. Indeed, implementing the jammer at the same transmitter node allows to have a perfect knowledge of the transmitter to receiver channel and a perfect synchronization with the transmitter, for achieving pilot nulling. Obviously, this setting corresponds to a worst case scenario, because the pilot nulling achieved by an independent jammers cannot work as in the ideal case considered in our experiments.

The OFDM link has been configured at a central frequency of 500 MHz, in which we expect to not have interference by other coexisting signals. The channel bandwidth is set to 100 MHz, while the effective channel of the transmitted signal is set at 50 MHz. We use an interpolation filter on the transmitter side in order to increase the rate and suppress the image frequencies at the input date rate. Every packet has a 802.11 preamble with 10 short training symbols and 2 long training symbols, while the rest of the packet is formed by 500 OFDM symbols. On the receiver side, we consider a half-band digital filter in order to reduce the output sample rate by a factor of 2, while rejecting aliases that fall into the band of interest. Through the UHD software API and MATLAB environment, we have been able to perform all the necessary analyses for each type of jamming strategies. BER is calculated on the average of 1000 packets. The SNR for all experiments was fixed at 30 dB as in the case of the simulation results, while the SJR is variable.

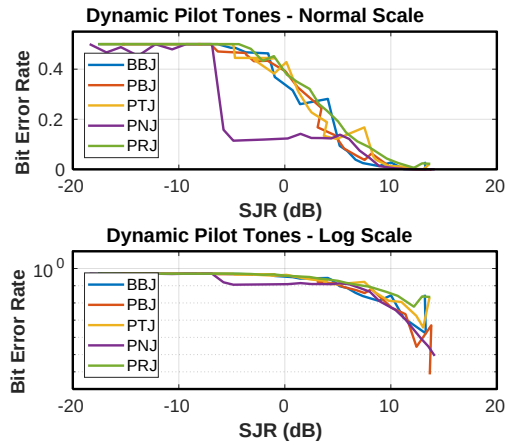
The performances for static and hopping pilot tones of a real OFDM transmission is shown in Figure 3.12. As expected, behaviours are almost in agreement with our simulations. Unlike the simulations, in which we considered a flat channel model, in the real world there is a channel with a very probable presence of fading. For this reason, it is possible to see that the curves are more oscillating than simulations. But otherwise, we confirm that the USRP experiments are inline with the simulation results, showing a clear improvement of BER performance under PTJ, PNJ and PRJ jamming strategies in presence of dynamic pilots.

3.6.2 Effects of Random Data Sub-carriers Activation

Another performance evaluation is to quantify the impact of random data sub-carrier activation on the jamming resistance. In other words, we want to investigate the effects of randomly activating data sub-carriers in order to increase the power level of the signal in the other sub-carriers. To this purpose, we implemented an OFDM transmitter able to change dynamically the percentage of active data sub-carriers, from 100% to 50%, 25% and 2% respectively. With a percentage of 2%, only one data sub-carrier is available



(a)



(b)

FIGURE 3.12: Performance in USRP experiments of the static (a) and dynamic (b) pilot tones OFDM solutions at 30 dB of SNR.

for transmission (i.e. the link is based on a traditional single-carrier modulation). The sub-carriers are chosen randomly symbol-by-symbol and reception is possible because the receiver knows the pattern of the active data sub-carriers.

It is important to understand that with a lower percentage of active data sub-carriers, the BER curve moves to the left, which means a lower BER with the same SJR. Obviously, the throughput also changes for each configurations. For the estimation of the throughput, we assume the presence of Forward Error Correction (FEC) that can fix the packet with a maximum of 8 wrong bits. For all the jammer attacks taken into consideration, the performance of the throughput is shown in the Figure 3.13. As expected, decreasing the number of data sub-carriers usually implies a throughput reduction, but for some critical SJR values it can be beneficial. In addition, Figure 3.14 shows the BER performance for the BBJ attack, confirming the effectiveness of the proposed technique.

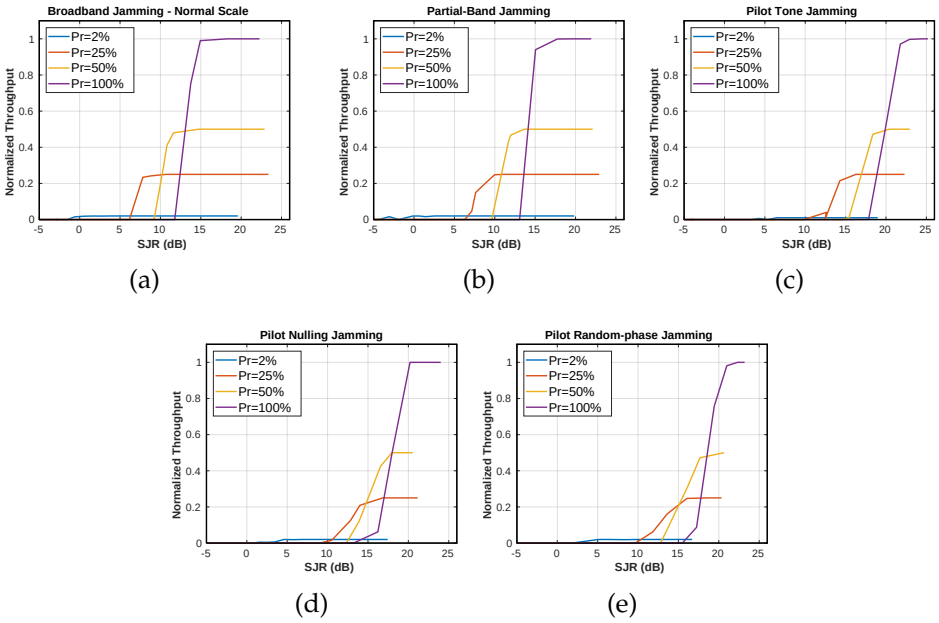


FIGURE 3.13: Throughput performance changing the percentage of active data sub-carriers for broadband jamming (a), partial-band jamming (b), pilot tone jamming (c), pilot nulling jamming (d) and pilot random-phase jamming.

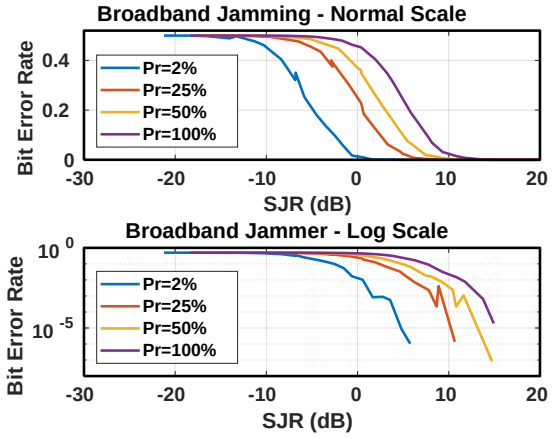


FIGURE 3.14: BER performance with BBJ attack.

3.6.3 Dynamic Sub-carrier Activation

Rather than considering a fixed percentage of active sub-carriers, we finally evaluate the performance of an adaptive scheme, able to dynamically adjust such a percentage. Results have been obtained in simulations. An example of a temporal throughput trace achieved under broadband jamming for SJR equal to 8 dB is shown in Figure 3.15. The algorithm works at the transmitter side at regular temporal steps, by collecting throughput results for a given monitoring interval and by performing an adjustment of the percentage of active sub-carriers to be randomly selected for data transmission at the end

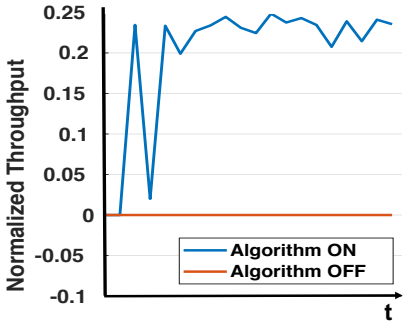


FIGURE 3.15: Throughput performance of an OFDM-based communication with a Broadband Jamming strategy at 8 dB of SJR with and without the adaptive algorithm.

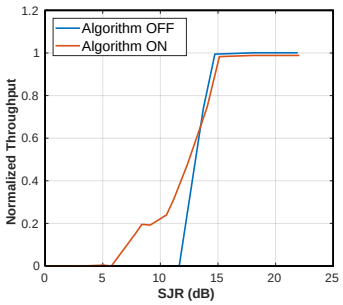


FIGURE 3.16: Throughput performance of an OFDM-based communication with a Broadband Jamming strategy when varying SJR with and without the adaptive algorithm.

of each interval. In our simulation, 20 steps are performed, while throughput calculation is made by averaging results of 1000 packet transmissions at each step. The scheme starts with an initial sub-carrier percentage equal to 100%, which leads to a throughput equal to zero due to the strong jammer signal. At the end of the first monitoring interval, the percentage of activated sub-carriers is reduced to 50%, but the throughput remains the same. Finally, at the third step the performance increases with a percentage of active sub-carriers equal to 25%. A further reduction to 2% achieves a throughput lower than the 25% case and therefore the scheme switches back to the 25% percentage until the end of simulation. This result shows that dynamic randomized sub-carrier activation is able to achieve a normalized throughput of 0.25 while the throughput of a classical OFDM transmission is zero.

We finally evaluate the trend of the throughput varying the SJR. We set the SNR to 30 dB and we calculate the average of the throughput for 1000 packets in absence and in presence of our algorithm. Figure 3.16 shows the difference between the two approaches. It is apparent to see that with our dynamic algorithm there is an evident enhancement of the throughput for SJR between the range of 5 and 12 dB despite the fact that we deactivate sub-carriers.

Chapter 4

Repeated Contention (ReCo)

In this chapter, we define innovative and flexible contention mechanisms for distributed systems by leveraging the flexible physical layer capabilities of recent wireless technologies. Hence, in this context the PHY layer flexibility is a key for developing a new mechanism for the random access contention.

4.1 Introduction

In the last years, the original IEEE 802.11 standard has been extensively amended for providing breakthrough capacity improvements by exploiting the latest PHY enhancements [58][59], such as bandwidth aggregation, efficient modulation and coding schemes, advanced MIMO (up to 8 spatial streams can be exploited in the IEEE 802.11ac). Still the MAC contention procedure is based on random countdown of back-off time slots. Its efficiency has been improved by allowing a station to transmit multiple data frames in a single channel access, but the contention mechanism wastes a significant amount of capacity and introduces jitter of service times due to the probability of attempting multiple transmissions after collisions, and to the Binary Exponential Back-off (BEB).

Although not included in current standards, another promising pathway to boost wireless network capacity is full-duplex radio, which is becoming a viable technical solution [60, 61]. As a matter of example, in [53] a cancellation capability of up to 110 dB is demonstrated over up to 80MHz bandwidth. Full-duplex capabilities have a strong impact on the design of more efficient MAC schemes, as discussed in [62]. However, most of the protocols proposed so far exploit these capabilities for performing collision detection in classical CSMA schemes, thus reducing the collision times [63]. Alternative solutions for improving the contention mechanism are explored in [64, 65],

where the concept of contention in the frequency domain is introduced. The idea is selecting random subcarriers rather than random back-off delays, and exploiting full-duplex for identifying the station with the smallest random extraction.

Regardless of the specific physical solutions, there are two main issues to be solved for random distributed systems [66]: arbitrating the access to a common channel, and scheduling frame transmissions within the channel holding times. While specific mechanisms have been standardized for introducing flexibility in the management of the channel holding time, such as the set-up of reverse links, cumulative acknowledgements and frame aggregations, in current standards the contention rules cannot be negotiated among the stations. Protocol flexibility is limited to the tuning of some parameters, which specify the contention windows, the retry limits, or the selection of pre-defined operation modes, because the contention logic needs to be implemented in the card hardware and firmware for efficiency reasons and cannot be easily extended or updated. An interesting approach for overcoming the technological problem of modifying time-critical MAC operations has been proposed in [67], by envisioning a novel architecture for wireless cards called Wireless MAC Processor (WMP). The card does not implement a specific protocol, but rather a generic *MAC Engine*, able to load and run different MAC programs (from CSMA to TDMA) working on the same hardware events and actions (the WMP application programming interface).

In this work, we focus on the possibility to define innovative and flexible contention mechanisms for distributed systems, by leveraging the physical layer capabilities of recent wireless technologies, as well as emerging architectures which support the implementation of programmable MAC protocols. We follow two approaches: a short term one, where the emphasis is on exploiting current off-the-shelf technology; and a longer term perspective, based on recent advances in full-duplex radios, where frequency domain contention turns out to simplify random access contention and make it most effective. Specific novel contributions of this work are: (i) the generalization of the contention defined in [65] to any number of contention rounds and to both time and frequency domains; (ii) the development of an analytical model of this new procedure (Repeated Contention, ReCo), yielding an asymptotically tight upper bound of the collision probability; this in turn provides a simple, closed-form tool for dimensioning the key parameters of ReCo; (iii) experimental results on off-the-shelf WiFi cards, where the new ReCo scheme has been implemented.

We organize the remainder of this chapter as follows. After a literature review provided in Section 4.2, we define the proposed access procedure in Section 4.3, provide an analytical model for dimensioning criteria and give numerical exempts of throughput performance in Section 4.4, and present an experimental validation in Section 4.5. The impact of imperfect carrier sensing emerged in the real experiments is assessed also in a simulation environment in Section 4.6.

4.2 Related Work

The review of the literature is organized in subsections, touching the main topics related to our work.

4.2.1 Optimization of DCF

CSMA schemes implemented in current technologies, such as the 802.11 DCF, expose a limited form of flexibility by enabling the dynamic configuration of contention windows and retry limits, as well as the possibility to activate or not 4-way handshake mechanisms. Several research work have been focused on the optimization of these parameters as a function of the network load and topology. For example, in [68], inspired by the throughput-optimal CSMA theory (e.g., see [66][69]), the Authors present the so called Optimal DCF, that implements in off-the-shelf 802.11 devices the principles of adaptation of contention windows and channel holding times as a function of the difference between the bandwidth demand and supply of the node.

Another variation of the IEEE 802.11 DCF, the so called *Idle sense*, is defined by Heusse et al. [70]. The Authors start from observing that there exists an optimal contention window in the basic DCF protocol, depending on the frame lengths and details of the PHY and MAC layer format, and on the number of actively contending stations N. The optimal operating point can be assessed by exploiting the mean number of idle back-off slots between two transmission attempts. It is found that the target optimal level of this metric has a weak dependence on N. The Authors show the throughput improvement offered by Idle Sense, as well as short and long term fairness. Weak points of the proposal is that it entails estimating the mean number of idle slots: this requires a number of transmissions (the parameter *maxtrans* in the algorithm in Fig. 6 of the paper). As the number of stations grows, the time to get a reliable estimate of the mean number of idle slots grows proportionally. Eventually, for large levels of N, the system could fail to settle at the optimal operating point due to the time variation of the number of contending stations. As a matter of example, Hassan et al. [71] show that a fairness issue arises when relaxing the hypothesis that all contending stations share the same current estimate of the contention window. Moreover, there are parameters in the algorithm that are difficult to tune properly, e.g., the additive increase and multiplicative decrease factors of the transmission probability.

4.2.2 Repeated contention access schemes

A general framework is set up by Zame et al. [72], aiming at defining a broad class of MAC protocols for distributed, sensing-based coordination protocols. The key idea is repeated *cycles* of contention that provide contending

stations a history of channel observations, leading eventually to perfect coordination (hence no collisions) with high probability after a given number of contention cycles. Numerical examples provided in the paper point out that the number of contention slots required for a moderate number of stations (e.g., 32) can ramp up to several hundreds if not in the order of thousand. In terms of contention time, this corresponds to several tens of ms. As a result, the goodput is close to the theoretical maximum in settings where there is a limited number of stations and they have a large backlog to send. Moreover, it is not clear how adaptive the protocol could be as the rate of arrivals of new active stations or termination of previously active station grows up, since the time scale of convergence is much bigger than the time required to send a single frame.

Different mechanisms devised to provide constant contention times have been proposed, e.g., see [73][74]. Here contending stations decide randomly to transmit a busy signal or not in a contention round. Stations that refrain from transmitting the busy signal, listen to the channel and drop out if they sense it busy. The Authors give a detailed approach to the optimization of the transmission probabilities in each round and several numerical examples. However, the optimization depends on the knowledge of the number of contending stations. Gowda et al. [74] illustrate the principle of repeated contention round to overcome the performance limitations of the traditional "linear" DCF contention, i.e., the one based on a single random extraction from a set of back-off values. Although recognizing the power of repeated contention, Gowda et al. [74] end up defining a rather complicated access procedure. Moreover, they only state the repeated contention approach in time, as a generalization of standard DCF. Another repeated round contention scheme is provided by Mao and Shen [75]. They target their contention scheme, named First Round-Bye (FRB), to handling different priority level flows. Repeated round supported by jamming is the basic means for priority management in a fully distributed way. The analysis of FRB is quite involved and does not yield a good insight into the effectiveness of the repeated round concept as a general means for sharing a channel. Zhou et al. [76] define a repeated contention mechanism in the time domain, alike ReCo_t. They discuss the selection of the protocol parameters (number of contention rounds, maximum number of back-off slots per round) and give guidelines for an optimal choice to minimize the collision probability. An interesting analytical model is presented for the case of uniform probability distribution of the back-off. Overall, it is a very good work. Our analysis approach lends itself to more general probability distributions. We introduce the frequency domain approach of repeated contention, that is the key to boost performance as the air bit rate grows. We also develop a test-bed implementation and offer measurements of the frequency-domain and time-domain versions of the ReCo algorithm, namely ReCo_f and ReCo_t, unlike [76] where performance are only based on simulation.

4.2.3 Frequency domain contention

The works [77, 65] propose a frequency domain MAC procedure where up to two consecutive contentions are carried out by selecting random sub-carriers rather than random back-off delays. The stations transmitting on the smallest frequency sub-carrier win the contention round. Frequency domain contention requires the capability of detecting other stations' signals while transmitting one's own sub-carrier. The feasibility of this operation is demonstrated experimentally in [65]. A Collision Detection (CD) scheme is defined in [63] for WiFi networks based on the full-duplex radio capability with standard CSMA access. The emphasis of the work is on optimization of the CD threshold. Full-duplex communication capabilities are exploited in a non-trivial way at MAC layer in [78]. The proposal is based on beacon (BCN) frames sent by the receiver during the data frame reception. The BCN frames act as acknowledgements that the reception is successful. BCN frames are also used to classify different network scenarios (collision region, transmitter-only region, receiver-only region; see Fig. 3 in [78]). The performance evaluation is focused on a special aspect, namely the resilience of the proposed MAC protocol to jamming attacks.

In [64] frequency domain contention is considered to define a random access reservation protocol. Reservation aims at electing a femtocell that transmits on a given channel, for mitigating the interference among nearby femtocells. A key point of that work is the assumption of a reliable feedback control channel from the receiver to the transmitter, which fits well the cellular paradigm. Moreover, the overhead of the reservation protocol is not a big issue in that context, given that the channel is required for intense, non-sporadic usage.

Frequency domain contention is exploited by Fayaz et al. [79] as well. They define a signaling protocol based on transmission and detection of tones, that aims at channelizing the available bandwidth so that non-interfering, concurrent links can operate simultaneously. The approach is suitable for infrastructured as well as ad-hoc networks. It requires the ability to transmit and detect sub-carrier tones at the same time. A synchronization scheme is discussed. A critical point is to fix the duration of the data phase so as to strike a good balance between potential low efficiency in case of long data phase duration and excessive weight of the signaling overhead for a short data phase. Only simulations are used to assess performance, without an in-depth analysis of the issue of simultaneous transmission and reception of signaling tones.

4.2.4 PHY-based optimization of DCF

Another direction for improving the MAC efficiency is the reduction of control messages' overheads. In [80], control messages like RTS, CTS and ACK are encoded by using Correlatable Symbol Sequences (CSS). The properties

of the CSS allow a substantial reduction of the vulnerability intervals and of the air time wasted to contend for the medium (RTS/CTS) and to send ACKs. In [81] a PHY-based explicit signaling among the AP and the stations and frequency domain contention are proposed. The proposed scheme relies on additional control signals for solving the contention, whose duration is limited to one back-off slot. It achieves a significant reduction of the channel overhead due to collisions.

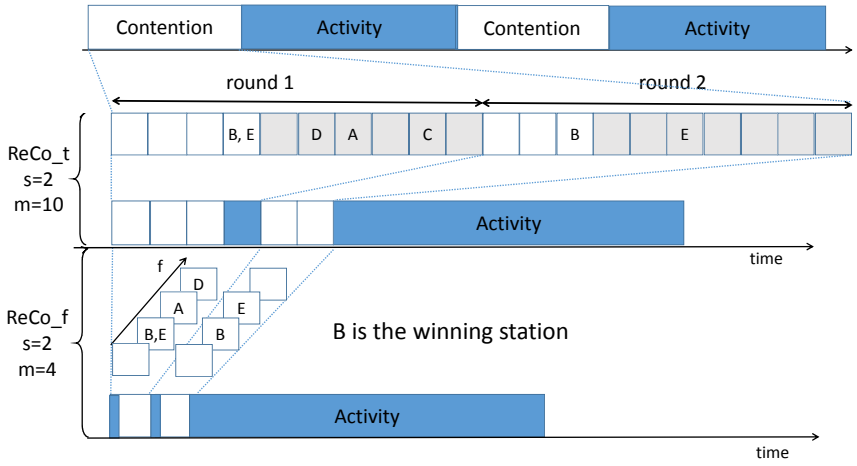


FIGURE 4.1: Channel access operations as a sequence of contention and activity phases: comparison between ReCo in the time (top) and frequency domain (bottom).

4.3 Repeated Contention Procedure

In this section we present a *robust contention scheme* whose performance is not critically affected by the configuration of the contention parameters. The idea is running repeated contention rounds, devised to select a sub-set of stations among the contending ones. The iteration of the basic contention round turns out to be a very powerful mechanism to reduce the collision probability to any desired low level. As discussed in Section 4.2, repeated contention round is not a new idea in itself, e.g., see [73, 74, 75, 77, 65] for some recent work. An early example of the idea of successive elimination round can be traced back to splitting algorithms, e.g., see [82, Ch. 4]. However, an innovation element of our proposal is decoupling the protocol logic from the physical implementation of the mechanisms used for performing the elimination rounds, and defining a complete, general analytical model.

As long as there are backlogged stations contending for the access to the channel, the channel time is divided into *cycles*, made up of a *contention phase* and an *activity phase* (Fig. 4.1). During the contention phase, the time axis is divided into s consecutive *contention rounds*. The contention phase is devised to identify the station that is allowed to transmit on the channel in the

ensuing activity phase. The activity phase includes all the frame transmissions performed within the same transmission opportunity, i.e., data and acknowledgment frames, or multiple data frames with a final acknowledgment request/response. Whatever the outcome of the activity phase, namely either a successful transmission or a failure, all backlogged stations, take part in the next contention phase, by repeating exactly the same algorithm as performed in the previous cycles. No binary exponential back-off or state variables are required, so that the entire access procedure is regenerated at each new cycle.

Within each contention round, a backlogged station has to choose one 'level' among $m \geq 2$ possible choices. Regardless of the specific mechanism to implement the scheme, the key aspects for supporting repeated contention rounds are:

1. the m levels are strictly ordered; we can label them as the integers of the set $\{1, \ldots, m\}$;
2. during the contention round every contending station can sense whether a level lower (or higher, based on the victory logic) than its own choice has been chosen by any other station.

The stations selecting the lowest level win the contention round and move forward to the next contention round. Note that possibly more than one station could win a contention round. If we assume a perfect channel sense, even if it is not so, as we will see later, there is *at least* one winner, since this corresponds to the existence of the minimum of a finite set. All the losing stations, having sensed that a level strictly lower than their choice has been selected, drop out of the current contention phase and wait for the next cycle.

In the following we specialize this general concept to specific implementations in the frequency domains. The first one is definitely the way to choose to boost performance respect to the time domain [83], but it requires that each station has the ability to detect other stations' signals *while* it is transmitting its own signal.

Repeated contentions can be implemented very efficiently in the frequency domain. A set of m frequencies is defined, denoted with $\{f_1, \ldots, f_m\}$. As a matter of example, if the PHY layer is based on OFDM, the m levels to be used for contention can be identified with (a subset of) the available subcarriers. Let q_i, $i = 1, \ldots, m$ the probability that frequency f_i is selected at a given round, for the sake of simplicity we will use them as a uniform distribution in the experiments, the advantages and disadvantages of the non-uniform distribution will be discussed in Sec. 4.4.4. The pseudo-code of the contention round algorithm for a station is listed in Alg. 1. In the algorithm, we call the following functions:

- `rand`: generates samples uniformly distributed in $[0, 1]$.
- `transmit_burst`(r, f) transmits a busy tone on frequency f during contention round r.

Algorithm 1 Pseudo-code of the contention phase algorithm.

```
1: round = 0;
2: dropout = FALSE
3: while (round < s)&(dropout == FALSE) do
4:    round = round + 1;
5:    r = min{x | 1 ≤ x ≤ m, Σ_{j=1}^{x} q_j ≥ rand};
6:    transmit_burst(round, f_r);
7:    if r > 1 then
8:       dropout = isbusy_channel(round, [f_1, f_2, ..., f_{r-1}]);
9:    end if
10: end while
```

- `isbusy_channel`$(r, [f_a, f_{a+1}, \ldots, f_b])$ checks if signal is detected on any one of the frequencies $f_a, f_{a+1}, \ldots, f_b$ during contention round r.

The algorithm states that a contending station picks a frequency f_r at random, according to the probability distribution $\{q_r\}_{r=1,\ldots,m}$, transmits on that frequency and *at the same time* listens to check whether a frequency *lower* than f_r is being transmitted: here it comes into play the full-duplex capability. Note that the contention phase does not require the capability of decoding any frame. A station must simply check whether it receives a tone whose frequency is lower than its own choice. This is a special case of full-duplex radio capability.

The station elects itself as winning the contention round if it does not sense any frequency lower than its own choice f_r. In that case the station will move to the next round and it will repeat the contention algorithm just as outlined in Alg. 1. Note that *at least one* station must survive at the end of any contention round, if channel sensing works. To improve the functioning of the channel sensing, it is necessary to choose the frequencies to send the tones during the contests, to minimize the problem of spurious tones, this will be explained in Sec. 4.5.1. If the station goes on winning until the s-th round inclusive, then it has won the contention phase and it has gained a right to use the channel.

The bottom diagram in Fig. 4.1 shows an example of ReCo in the frequency domain (called ReCo_f), with $s = 2$ and $m = 4$, under the assumption that each contention round lasts exactly one back-off slot. This is a reasonable assumption, because it is possible to transmit more than one OFDM symbol within a back-off slot. The boxes along the frequency dimension represent the tones used for the contention round. Four stations are contending, each marked by a letter. After the first contention round, two stations survive and are admitted to the second round, after which only station B survives. The contention time of ReCo_f has a fixed duration that depends on the number of rounds s.

4.4 Analysis of the Contention Procedure

Given the full regenerative access procedure of ReCo, each contention cycle is independent of all others. Hence, we focus on a single contention cycle.

Let n be the number of backlogged contending stations at the beginning of the contention phase, s be the number of rounds and m be the number of levels characterizing the scheme as described in Section 4.3. Let q_r denote the probability that a station picks level r, $r = 1, \ldots, m$. Let also $G_r = \sum_{j=r}^{m} q_j$ be the Complementary Cumulative Distribution Function (CCDF) associated to q_r. The probability $P_{k,h}$ that h stations survive after a single contention round, given that k stations are contending at the beginning of that round, is

$$P_{k,h} = \sum_{i=1}^{m-1} \binom{k}{h} q_i^h G_{i+1}^{k-h}, \quad h = 1, \ldots, k-1 \tag{4.1}$$

and

$$P_{k,k} = \sum_{i=1}^{m} q_i^k \tag{4.2}$$

We can form the $n \times n$ matrix $\mathbf{P}$ whose k-th row entries are $P_{k,h}$, for $h = 1, \ldots, k$, and 0 for $h = k+1, \ldots, n$ ($k = 1, \ldots, n$). $\mathbf{P}$ is the one-step transition probability matrix of a Markov chain $\mathcal{X}$ on the state space $\{1, 2, \ldots, n\}$ with an absorbing state at 1. The state probability vector at time t is denoted with $\mathbf{x}(t)$, $t \geq 0$, where $x_i(t) = \mathcal{P}(\mathcal{X}(t) = i)$, $i = 1, \ldots, n$. It is $\mathbf{x}(0) = [0 \ldots 0\ 1]$, i.e., at the initial time $t = 0$ the Markov chain is in state $\mathcal{X} = n$ with probability 1.

The probability distribution of the number $\mathcal{W}$ of winning stations that survive through the s contention rounds is $\mathcal{P}(\mathcal{W} = h) = \mathcal{P}(\mathcal{X}(s) = h) = x_h(s)$, $h = 1, \ldots, n$, with $\mathbf{x}(s) = \mathbf{x}(0)\mathbf{P}^s$. We have a success after the completion of s rounds with probability $\mathcal{P}(\mathcal{W} = 1) = x_1(s)$.

Let $\mathbf{Q}$ denote the square matrix obtained by taking the last $n-1$ rows and columns of $\mathbf{P}$. $\mathbf{Q}$ is the one-step transition probability matrix of a transient Markov chain.

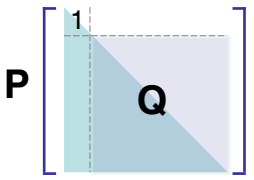


FIGURE 4.2: Relationship between the matrices $\mathbf{P}$ and $\mathbf{Q}$.

The collision probability p_c can be expressed as $p_c(s) = \mathcal{P}(\mathcal{W} > 1) = \mathbf{e}_1\mathbf{Q}^s\mathbf{e}$, for $s \geq 1$; $\mathbf{e}$ is a column vector of ones of size $n-1$, $\mathbf{e}_1$ is a row vector of size $n-1$ whose entries are $e_1(j) = 0$ for $j \neq n-1$ and $e_1(n-1) = 1$.

The matrix $\mathbf{Q}$ is lower triangular, with diagonal elements given by the right hand side of eq. (4.2) for $k = 2, \ldots, n$. Hence, its dominant eigenvalue is $\eta \equiv Q_{11} = \sum_{i=1}^{m} q_i^2$. Since $\mathbf{Q}$ is also a non-negative matrix, the left and right eigenvectors $\mathbf{v}$ and $\mathbf{u}$ associated to η are positive. Then, the asymptotic behaviour of the collision probability as $s \to \infty$ can be written as $p_c(s) \sim \kappa \eta^s$, where $\kappa = \mathbf{e}_1 \mathbf{u} \mathbf{v} \mathbf{e}$.

We can state this result as follows: the collision probability decays geometrically as the number of rounds s grows, with a decay rate $\eta = \sum_{i=1}^{m} q_i^2$. Note that η is minimized for $q_i = 1/m$, $i = 1, \ldots, m$, i.e., when the level selection probability distribution is uniform. In that case it is possible to find closed forms for the dominant eigenvalue and associated eigenvectors of $\mathbf{Q}$. It is $\eta = 1/m$, $\mathbf{v} = [1\ 0\ \ldots\ 0]$ and $\mathbf{u} = [2\ 3\ \ldots\ n]^T/2$. Hence the asymptotic expansion of the collision probability is $p_c(s) \sim n/(2m^s)$ as $s \to \infty$. We have also:

$$p_c(s) = \mathbf{e}_1 \mathbf{Q}^s \mathbf{e} \leq \mathbf{e}_1 \mathbf{Q}^s \mathbf{u} = \frac{1}{m^s} \mathbf{e}_1 \mathbf{u} = \frac{n}{2m^s} \tag{4.3}$$

since all involved vectors and matrices are made up of non-negative entries and it is $\mathbf{e} \leq \mathbf{u}$, where the inequalities are meant to be entry-wise. Then, an asymptotically tight upper bound for the collision probability is

$$\hat{p}_c(s) = \min\left\{1, \frac{n}{2m^s}\right\}, \qquad s \geq 1 \tag{4.4}$$

It is apparent from eq. (4.4) that the collision probability drops quickly as s is increased, the more the bigger m. As a matter of example, if we require that the collision probability be no bigger than 10^{-4}, it can be easily checked that $s = 4$ is enough with $m = 32$ for whatever value of $n \leq 200$. The accuracy of the upper bound is discussed in [83].

The tight bound of the collision probability gives insight on why the repeated contention procedure is expected to be superior to "linear" CSMA. The maximum number of contention back-off slots for the time domain implementation is $m \cdot s$. Since CSMA performs a *single* contention round, its collision probability goes as $p_c^{CSMA} \sim 1/(ms)$, whereas the repeated contention procedure attains $p_c^{RECO} \sim 1/m^s$ for *the same contention time overhead in terms of maximum number of back-off slots in case of ReCo_t, much less time contention overhead for ReCo_f*.

The analysis of the collision probability applies to both frequency and time domain procedures, while the duration of the contention phase is different. Let B denote the number of back-off slots required to complete the contention phase. With frequency domain, the contention phase is made up of a fixed number s of rounds. If we assume that a contention round lasts one back-off slot, then $E[B] = s$. With time domain, let us consider a tagged round where k stations are contending. The probability that i back-off slots are counted is:

$$\sum_{h=1}^{k} \binom{k}{h} q_i^h G_{i+1}^{k-h} = G_i^k - G_{i+1}^k, \quad i = 1, \ldots, m-1, \tag{4.5}$$

and $q_m^k = G_m^k$ for $i = m$. The mean number of back-off slots counted down is $\sum_{i=1}^{m-1} i\,(G_i^k - G_{i+1}^k) + m\,G_m^k = \sum_{i=1}^{m} G_i^k$. The probability of having k contending stations at the end of round j has been denoted with $x_k(j)$. Let also $x_k(0)$ be the probability of having k contending stations at the beginning of the contention phase. Then, the mean of the number B of back-off slots required by s rounds is:

$$\mathrm{E}[B] = \sum_{j=0}^{s-1} \sum_{k=1}^{n} x_k(j) \sum_{i=1}^{m} G_i^k \tag{4.6}$$

4.4.1 Activity times

Fig. 4.1 shows the system time evolution as a sequence of contention and activity times. The duration A_s (A_c) of successful (collision) activity times can be represented as sum of two contributions: (i) overhead time $T_{oh,x}$ ($x = s, c$) accounting for PHY/MAC overhead and inter-frame spacings; (ii) payload transmission time.

Let $\mathcal{W}$ denote the number of stations that transmits concurrently and U_i be a random variable representing the time the frame payload takes to be transmitted by the i-th station. Then, we can write $A_s = T_{oh,s} + U_1$ in case $\mathcal{W} = 1$, and $A_c = T_{oh,c} + \max\{U_1, U_2, \ldots, U_{\mathcal{W}}\}$ for $\mathcal{W} > 1$. It is $U = L/R$, R being the air bit rate of the MAC interface and L the MAC PDU payload length. Both quantities take a discrete spectrum of values, so that we model U as a discrete random variable. Let $U \in \{a_1, a_2, \ldots, a_\ell\}$ with $a_1 \leq a_2 \leq \cdots \leq a_\ell$, and $Q_j = \mathcal{P}(U \leq a_j)$ for $j = 1, \ldots, \ell$. For notation convenience we set also $Q_0 = 0$. By the independence assumption, the payload times U_i are independent of one another, so it is straightforward to check that $\mathcal{P}(\max\{U_1, \ldots, U_r\} \leq a_j) = Q_j^r$ ($j = 1, \ldots, \ell$), and $\mathrm{E}[\max\{U_1, \ldots, U_r\}] = \sum_{j=1}^{\ell} a_j (Q_j^r - Q_{j-1}^r)$, for $r \geq 1$. Specifically, we have $\mathrm{E}[U] = \sum_{j=1}^{\ell} a_j (Q_j - Q_{j-1})$. Letting $v_h \equiv x_h(s) = \mathcal{P}(\mathcal{W} = h)$, for $h = 1, \ldots, n$, the average activity times in case of successful transmissions or collisions are given by:

$$E[A_s] = T_{oh,s} + \sum_{j=1}^{\ell} a_j (Q_j - Q_{j-1}) = T_{oh,s} + \mathrm{E}[U] \tag{4.7}$$

$$E[A_c] = \frac{\sum_{k=2}^{n} v_k \sum_{j=1}^{\ell} (T_{oh,c} + a_j)(Q_j^k - Q_{j-1}^k)}{\sum_{k=2}^{n} v_k} \tag{4.8}$$

4.4.2 Saturation throughput

We evaluate the saturation throughput ρ for n stations continuously backlogged. By considering that the end of each activity time is a regeneration instant for the repeated contention procedure, we can express the normalized saturation throughput of ReCo as the ratio of the mean time spent to

transmit the payload of a successful frame and the average duration of the regeneration cycle:

$$\rho_{ReCo} = \frac{(1-p_c)\mathrm{E}[U]}{\delta \mathrm{E}[B] + (1-p_c)\mathrm{E}[A_s] + p_c \mathrm{E}[A_c]} \tag{4.9}$$

where δ is the back-off slot time, $\mathrm{E}[B]$ is given in eq. (4.6), p_c is the collision probability, $\mathrm{E}[U]$, $\mathrm{E}[A_s]$ and $\mathrm{E}[A_c]$ are given in eqs. (4.7) and (4.8). The expression is valid for both the frequency and time domain, with the only difference that the contention phase duration is constant and equal to $s \cdot \delta$ for ReCo_f, while it is random with average $\mathrm{E}[B] \cdot \delta$ for ReCo_t.

As reference comparison terms, we also consider the throughput achievable under legacy DCF and under perfect scheduling. For the legacy DCF, the normalized throughput ρ_{DCF} can be found as a simple generalization of the model proposed in [84][85]:

$$\rho_{DCF} = \frac{P_s \mathrm{E}[U]}{P_e \delta + P_s T_{oh,s} + P_c T_{oh,c} + \sum_{j=1}^{\ell} a_j (Y_j - Y_{j-1})} \tag{4.10}$$

where τ is the transmission probability in each channel slot, $Y_j = (1 - \tau + \tau Q_j)^n$, $j = 0, 1, \ldots, \ell$ and $P_e = (1-\tau)^n$, $P_s = n\tau(1-\tau)^{n-1}$, $P_c = 1 - P_e - P_s$. The result of eq. (4.10) follows from $\rho_{DCF} = \frac{P_s \mathrm{E}[U]}{P_e \delta + P_s \mathrm{E}[A_s] + P_c \mathrm{E}[A_c]}$, with $\mathrm{E}[A_s]$ and $\mathrm{E}[A_c]$ given by eqs. (4.7) and (4.8) with $v_h = \binom{n}{h} \tau^h (1-\tau)^{n-h}$ for the DCF.

The probability τ can be computed, given the number n of stations, the DCF maximum retry parameter, M, and the contention window sizes, $W_i, i = 0, 1, \ldots, M$, by solving a non-linear equation system (see [84][85]), namely

$$\begin{aligned} \tau &= \frac{1 + p + p^2 + \cdots + p^M}{\beta_0 + \beta_1 p + \beta_2 p^2 + \cdots + \beta_M p^M} \\ p &= 1 - (1-\tau)^{n-1} \end{aligned}$$

with $\beta_i = (W_i + 1)/2$ for $i = 0, 1, \ldots, M$.

In case of centralized scheduling, no contention and back-off are required. Each channel cycle is devoted to a successful transmission. Then

$$\rho_{ideal} = \frac{\mathrm{E}[U]}{T_{oh,s} + \mathrm{E}[U]} \tag{4.11}$$

4.4.3 Optimization of the contention parameters

In this section we give guidelines to the choice of m and s for maximizing the throughput of ReCo.

Replacing $\mathrm{E}[A_c]$ in eq. (4.9) with an upper bound $T_{c,max}$ (e.g., the maximum allowed TxOP time) and p_c with the upper bound $\hat{p}_c$ given in eq. (4.4), we

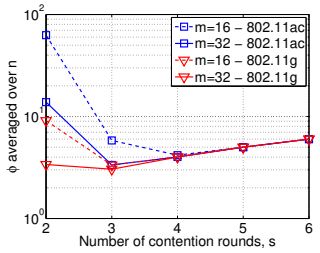


FIGURE 4.3: The function ϕ for ReCo_f versus s, averaged over n for $20 \leq n \leq 200$, for two values of m (16 and 32) and two values of the parameter a, $a \approx 24$ (IEEE802.11g) and $a \approx 220$ (IEEE 802.11ac).

obtain a lower bound of the throughput:

$$\rho_{ReCo} \geq \rho_{lb} = \frac{(1-\hat{p}_c)\mathrm{E}[U]}{\delta \mathrm{E}[B] + (1-\hat{p}_c)\mathrm{E}[U] + \hat{p}_c T_{c,max}} \tag{4.12}$$

Maximizing ρ_{lb} is equivalent to minimizing the following function of s and m:

$$\phi(s,m;n) = \frac{\mathrm{E}[B] + \hat{p}_c T_{c,max}/\delta}{1-\hat{p}_c} \tag{4.13}$$

The only parameter that depends on the frame formats, timing, bit rate and other details of the protocol is the ratio $a \equiv T_{c,max}/\delta$. Given a, the quantity ϕ depends only on s and m and on the number of contending stations n. For ReCo_f we have

$$\phi_f(s,m;n) = \frac{s + a\frac{n}{2m^s}}{1-\frac{n}{2m^s}} \tag{4.14}$$

for all values of s, m, n such that $n < 2m^s$. It is apparent that ϕ_f is monotonously decreasing with m. The limit on m is posed by practical feasibility of the radio hardware. As an example, let us consider the range $2 \leq n \leq 200$ and two relatively small values of m, namely 16 and 32. The values of ϕ averaged over the considered range of n is displayed in Fig. 4.3 as a function of s, for two values of a, i.e., $a \approx 24$ (a value consistent with IEEE 802.11g) and $a \approx 220$ (consistent with IEEE 802.11ac). It is seen that $s = 3$ is optimal except of the case $m = 32$ and IEEE 802.11ac, where $s = 4$ is better. The reason why of this weak dependance of the optimal level of s on the number of contending stations is highlighted by the expression of the optimal s^*, provided that the collision probability is small. In that case, it can be found easily that $s^* = \log_2(n\,a\log(m)/2)/\log_2(m)$. hence, s^* grows only with the logarithm of n.

As for ReCo_t, the overhead can be written as

$$\phi_f(s,m;n) = \frac{\mathrm{E}[B] + a\frac{n}{2m^s}}{1-\frac{n}{2m^s}} \tag{4.15}$$

where $\mathrm{E}[B]$ is given by eq. (4.6).

4.4.4 Non uniform repeated contention

Optimization of the parameters has been carried out by assuming the same pdf for the choice of the contention level (frequency or back-off delay) in each contention round. It is possible to relax this condition and let the probability distribution $\{q_k\}_{k=1,\ldots,m}$ change with the contention round.

The intuition is as follows. In the first contention round there could be from very few up to a very large number of contending stations, depending on the scenario. The probability distribution $\{q_k\}_{k=1,\ldots,m}$ should be chosen so as to minimize the expected number of stations surviving after the first round, $\mathrm{E}[S_1]$. Let n be the initial number of the stations; then

$$\mathrm{E}[S_1] = n \sum_{i=1}^{m} q_i G_i^{n-1} \tag{4.16}$$

This is to be minimized under the constraint $\sum_{i=1}^{m} q_i = 1$. Using Lagrange multipliers, we have to minimize the function

$$f(\mathbf{q}) = n \sum_{i=1}^{m} q_i G_i^{n-1} - \Lambda \sum_{i=1}^{m} q_i \tag{4.17}$$

Imposing that the gradient be null, we obtain the following m equations in the $m+1$ unknowns Λ and q_i, $i = 1, \ldots, m$:

$$n G_j^{n-1} + n(n-1) \sum_{i=1}^{j} q_i G_i^{n-2} - \Lambda = 0 \tag{4.18}$$

for $j = 1, \ldots, m$. Taking differences, we find

$$G_j^{n-1} - G_{j-1}^{n-1} + (n-1) \sum_{i=1}^{j} q_i G_i^{n-2} = 0 \tag{4.19}$$

for $j = 2, \ldots, m$. This can be re-arranged as follows:

$$(n-1)\frac{q_j}{G_j} = \left(\frac{G_{j-1}}{G_j}\right)^{n-1} - 1 = \frac{1}{(1 - q_{j-1}/G_{j-1})^{n-1}} - 1 \tag{4.20}$$

holding for $j = 2, \ldots, m$. Letting $z_j \equiv 1 - q_j/G_j$, we find

$$z_{j-1} = \frac{1}{\left[n - (n-1)z_j\right]^{\frac{1}{n-1}}} \tag{4.21}$$

for $j = m, m-1, \ldots, 2$, starting with $z_m = 1 - q_m/G_m = 0$. Once the z_j's have been calculated, the optimal probability distribution is found by

$$q_j^* = \begin{cases} 1 - z_1 & j = 1 \\ (1 - z_j)\left(1 - \sum_{i=1}^{j-1} q_i^*\right) & j = 2, \ldots, m \end{cases} \tag{4.22}$$

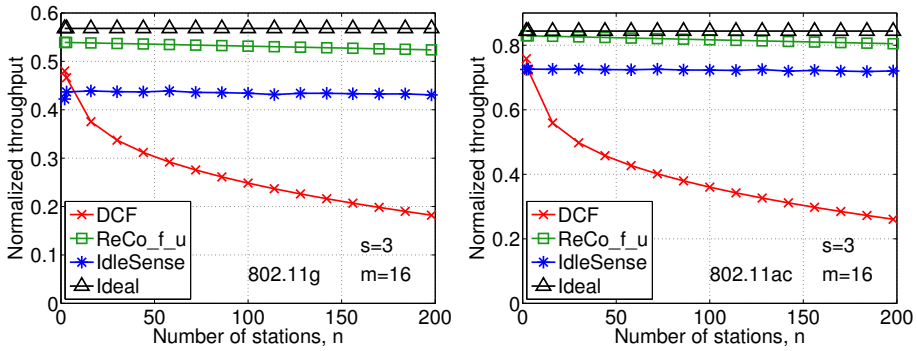
Substituting back the optimal solution into the expression of the mean number of surviving stations, we find $\mathrm{E}[S_1^*] = 1 + (n-1)q_1^*$. In the special case $m = 2$, the expression of $\mathrm{E}[S_1]$ simplifies to $nq_1 + nq_2^n$ and $q_1^* = 1 - 1/n^{\frac{1}{n-1}}$. Then, $\mathrm{E}[S_1^*] = 1 + (n-1)q_1^* = n - (n-1)e^{-\frac{\log(n)}{n-1}} \sim 1 + \log(n)$, for large n. This shows that the optimal level probability distribution reduces the number of contending stations from n to a value S_1 whose mean is in the order of $\log(n)$. It can be expected that using the optimal distribution is especially effective when a large number of station contend initially, while it does not have a strong impact in case a small number of stations are contending. To minimize the potential waste of contention time (which is important in case of ReCo_t), we could assume $m = 2$ for the first contention round, with a value of q_1 corresponding to the optimal one for large n, e.g., $q_1 = 0.05$. If $n \gg 1$, with high probability at least one station will choose level 1, thus winning the contention and setting off most of the others. If instead $n \sim 1$, then most probably all stations will choose 2 and the two contention slots will be simply wasted.

A further optimization can be introduced by having the contention mechanism becoming stateful. Since it is expected that the number of contending stations evolves on a much slower time scale than the transmission time of a single frame, a station undergoing multiple consecutive contentions can adjust its parameters based on the outcome it obtains. If the idle time of the first contention is significant with respect to m, n can be deemed to be small.

4.4.5 Numerical examples

We consider examples based on the IEEE 802.11g and 802.11ac PHY parameters. The back-off slot duration is $\delta = 9\ \mu s$ and it is $SIFS = 16\ \mu s$. As for IEEE 802.11g, we have a 20 MHz channel, the air bit rate rate set to 54 $Mbps$, and $T_{oh,s} = T_{oh,c} = 121.8\ \mu s$ (including SIFS, DIFS and acknowledgments). With IEEE 802.11ac, we consider a 40 MHz channel, the air bit rate set to 200 $Mbps$ (1 spatial stream, 256-QAM with code rate 5/6), and $T_{oh,s} = T_{oh,c} = 162.9\ \mu s$. Payload lengths are uniformly distributed over the set $\{80, 1500, 2304\}$ bytes in case of 802.11g and over the set $\{80, 1500, 9000, 11454\}$ bytes in case of 802.11ac by also taking into account the aggregation of 4 MPDU for the latter. For the standard IEEE 802.11 DCF the contention window values are $W_i = \min(16 \cdot 2^i, 1024)$ for $i = 0, \ldots, 7$.

ReCo performance have been compared with the standard IEEE 802.11 DCF; an ideal MAC, with no collision and no contention overhead; and Idle



(a) (b)

FIGURE 4.4: Normalized throughput vs. n: comparison among ideal (no collisions), ReCo_f with uniform tone selection probabilities, IdleSense and IEEE802.11 DCF with standard and optimized contention window sizes.

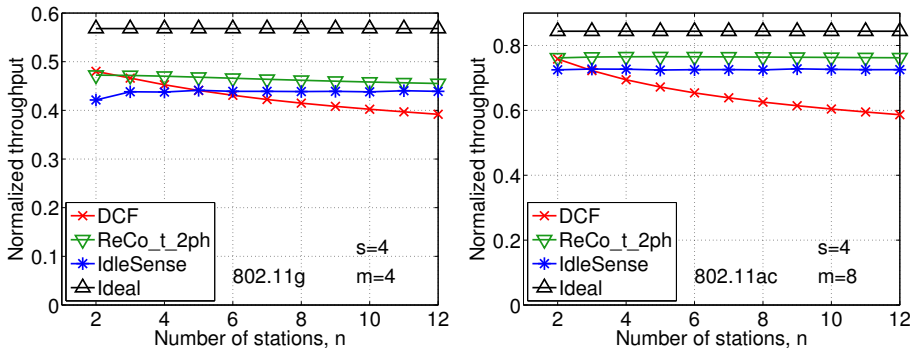
Sense [70]. Idle Sense has been selected since it achieves the best performance among the variants of IEEE 802.11 DCF. It has been simulated, by implementing carefully the algorithm described in [70] for each values of n.

ReCo_f performance. In this case, the duration of each contention round is identified with the back-off slot duration. Fig. 4.4 shows the normalized throughput ρ for $s = 3$ and $m = 16$ as a function of the number of contending stations n for the ideal MAC (triangle markers), ReCo_f with uniform tone selection probabilities (curve labelled 'ReCo_f_u', with square markers), standard IEEE 802.11 DCF ('x' markers) and Idle Sense (asterisk markers). Figures 4.4(a) and 4.4(b) refer to IEEE 802.11g and to IEEE 802.11ac, respectively.

The most relevant outcome is that ReCo_f exhibits close-to-ideal performance results, and that the achieved throughput is almost insensitive to the number of contending station in the range between 2 and 200. While Idle Sense exhibits excellent performance, except at small n levels, ReCo_f is definitely superior. We observe that ReCo_f throughput performance are achieved with a *fixed* parameter configuration and a relatively small value of m[1]. There is no need of implementing an estimator of the number of contending stations as in Idle Sense. This is a critical point whenever the offered traffic is volatile and intermittent, so that the number of contending stations varies quickly over time, possibly by large amounts. ReCo_f does not suffer the offered traffic variability, given that a *static* parameter setting is essentially optimal for n ranging between 2 and 200.

ReCo_t performance. The normalized saturation throughput is compared for the time domain contention procedure in Fig. 4.5 for the same protocols as in Fig. 4.4. We have considered the variant of ReCo_t where the first

[1]In our test-bed implementation of ReCo_f, $m = 11$ is achieved with standard hardware.



(a) (b)

FIGURE 4.5: Normalized throughput vs. n: comparison among ideal (no collisions), ReCo_t with uniform back-off selection probabilities, IdleSense and IEEE 802.11g/ac DCF with standard and optimized contention window sizes.

contention round comprises only two back-off slots with non-uniform probability distribution. Specifically, it is $q_1 = 0.05$, $q_2 = 0.95$. The relevant curves are labelled with 'ReCo_t_2ph'.

It is apparent that ReCo_t performance are not so brilliant as those of the frequency domain counterpart, yet it still improves on the best performance yielded by Idle Sense, especially for small values of n, and also improves the performance show in [83]. It is apparent that ReCo_t outperforms the traditional DCF for any value of n. This is obtained with a *static* parameter configuration, suitably chosen for each type of standard (either g or ac).

We believe that the simplicity of having a fixed setting is a key point for a reliable and cost-effective implementation, along with the 'regenerative' access style of ReCo. By this we mean that stations need not remember any state variable from one contention (the s rounds) to the next one. This approach guarantees the maximum possible level of short time fairness, given that a random access is used.

4.5 Experimental Validation

In order to validate the ReCo performance in a real wireless network, we implemented the contention procedure in the time [83] and frequency domain. The time version has been implemented on commercial off-the-shelf 802.11g cards, because the scheme does not require hardware primitives which are not supported by off-the-shelf cards. Indeed, ReCo_t is based on the repetition of back-off extractions and count-downs, transmission of short control frames at the end of the round, and sensing of the channel. All these primitives are supported by standard DCF, whose contention logic is usually implemented at the firmware level. Rather than working with an open

firmware, we decided to exploit the high-level programming language exposed by the Wireless MAC Processor architecture (WMP) [67]. A firmware implementing this architecture with a generic executor of state machines has been developed for a commercial card by Broadcom and is publicly available, together with a graphical editor for programming state machines and a control interface for loading them inside the card. The ReCo_t state machine has been implemented as a straightforward generalization of legacy DCF as described in [83]. Conversely, the frequency version of the scheme requires the implementation of novel physical primitives, for transmitting and detecting contention tones. To this purpose, we worked on the FPGA-based WARP board, for which a legacy 802.11g transceiver and DCF protocol implementation are available in the so called 802.11 reference design. Moreover, for the WARP board, we also implemented the WMP architecture which allows to easily modify DCF contention logics, by simply defining and injecting a MAC protocol state-machine.

4.5.1 Physical primitives for ReCo_f implementation

So far, prototypes of wireless nodes exploiting tone-based contention mechanisms have been mainly built on top of software defined radio (SDR) platforms, such as the GNURadio/USRP platform [65, 86]. In our case, we decided to work on the FPGA-based WARP platform in order to exploit both PHY layer programmability (to implement tone transmission and reception mechanisms) and MAC layer programmability (to implement the ReCo_f logic), while relying on the WMP abstractions which allow to dramatically limit the complexity of MAC protocol definitions. Moreover, the WARP board allows the support of legacy 802.11g PHY for data transmissions, working up to 54 Mbps, i.e. to data rates much faster than SDR implementations.

Considering that recognition of tones is much easier than modulated signals, especially if tones are opportunistically spaced, in ReCo_f approach, contentions are performed by identifying the stations that transmit tones at the lowest frequency.In principle, multi-carrier modulation, such as OFDM, can be easily adapted for transmitting and detecting tones. On the transmitter side, it is simply necessary to null all available sub-carriers except one subcarrier index corresponding to the desire tone, while on the reception side, it is necessary to compare the reception power of each sub-carrier with a threshold.

Increasing tone duration at the transmitter side and incrementing the frequency resolution at the receiver side, detection of the transmitted tones is more robust in presence of channel attenuation and interfering signals. For improving the frequency resolution, we considered the possibility to use FFT blocks with a number of sub-carriers higher than 64 in the receiver chain. Conversely, in the transmitter chain there is the possibility to replicate tone samples several times (i.e. 2 times for a resolution of 128 points and 4 times

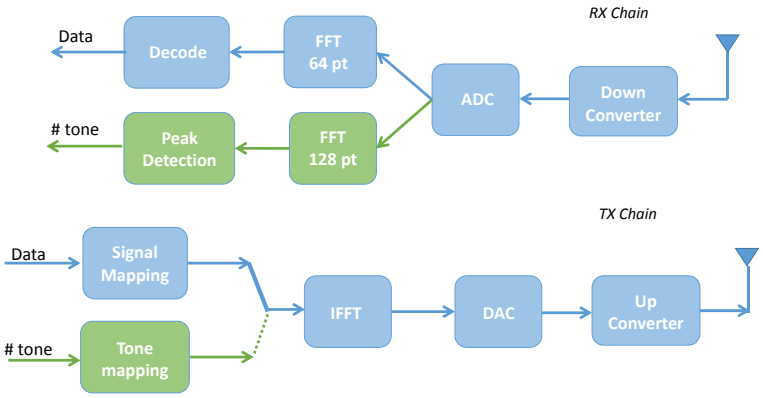


FIGURE 4.6: Modifications to the WARP reference design for 802.11g PHY enabling tone transmissions and receptions.

for 256). This type of approach would guarantee the minimum changes to the standard architecture. Considering factors such as transmission time, peaks detection errors and number of possible tones for contentions, we have decided to use an empirical optimal trade-off with a 128 points FFT resolution. In Sec. 4.5.2 we will discuss various experiments with various frequency resolutions. For the implementation of a tone-based communication, a general architectural TX/RX design is described in Fig. 4.6. Green blocks are modifications necessary to TX and RX chains of a general transceiver in order to operate this new contention mechanism.

A crucial aspect of this contention mechanism is to perform in parallel these two operations. This feature implies the capability of transmitting and receiving tones simultaneously. This type of capability is included in the logic of full duplex radios, in which advanced digital and analog cancellation mechanisms are present[53]. However, in absence of this kind of technology, the same requirement can be satisfied by two independent transceivers in a single node.

The tone transmitted by the transmission chain will create a self-interference in the receiver chain, which will involve the presence of high power values at the same transmitted frequency from the transmitter. Moreover, because of the non-linearity of the transmitter, the transmitted tone will create some attenuated spurious signals at other frequencies (i.e. at the mirror frequency and at twice the frequency of the tone). Self-interference signals can prevent the detection of tones at the same frequency transmitted by other nodes, but this capability is not required by the ReCo_f scheme. On the other hand, spurious signals could affect the ReCo_f contention mechanism. In fact, they can be erroneously considered as valid tones transmitted by all competing nodes. If the tone frequencies chosen for the contention mechanism are different (or chosen with a small overlapping probability) from all possible spurious signals, the probability of this event can be reduced to zero (or minimized). To this purpose, it is possible to choose a sub-set of the total number of available sub-carriers as contention tones. Table 4.1 shows a possible list of 8, 11 and 16 sub-carriers chosen among a set of 64 available ones. The choice was made

8 TONES	sub-carrier index	39	46	53	59	9	16	23	29
	frequency [MHz]	-8.13	-5.94	-3.75	-1.88	2.50	4.69	6.88	8.75
11 TONES	sub-carrier index	38	44	50	55	61	3	9	15
	frequency [MHz]	-8.44	-6.56	-4.69	-3.12	-1.25	0.62	2.50	4.37
	sub-carrier index	20	26	32					
	frequency [MHz]	5.94	7.81	9.68					
16 TONES	sub-carrier index	37	40	44	47	50	53	56	59
	frequency [MHz]	-8.75	-7.82	-6.56	-5.63	-4.69	-3.75	-2.81	-1.88
	sub-carrier index	5	9	12	15	18	21	25	28
	frequency [MHz]	1.25	2.50	3.44	4.38	5.31	6.25	7.50	8.44

TABLE 4.1: An exemplary selection of contention tones.

through a simple algorithm in order to maximize the distance between spurious signals and contention tones. Hence, tone detection is based on a simple comparison between the value of the FFT samples at the frequencies of the potential tones and a threshold value, which is tuned as a function of the background noise[2]. As mentioned before, working on 128 (or 256) samples allows to improve the frequency resolution of peak detection, thus leading to a more robust identification of tones. In Sec. 4.5.3, we decided to use 11 tones in order to compare the results with our previous work, ReCo in the time domain [83].

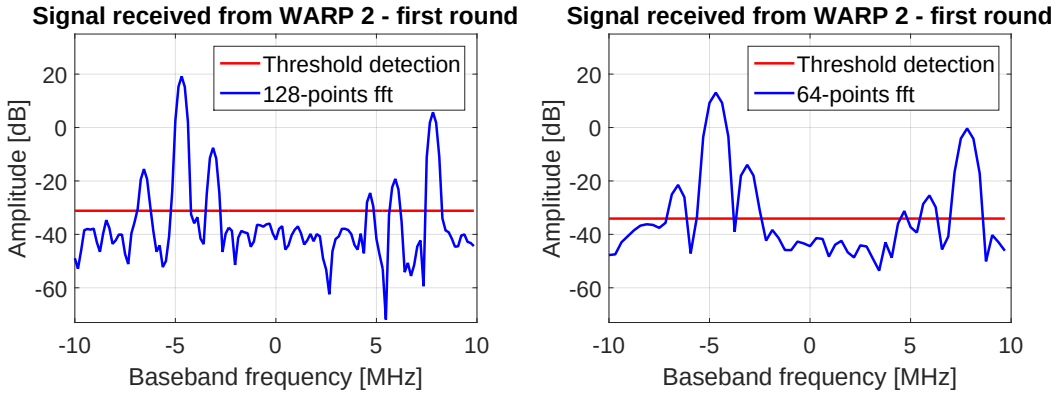
4.5.2 ReCo_f channel sensing

In order to quantify previous considerations, Fig. 4.7 shows the FFT samples received by a wireless node, while it is transmitting a tone at -4.69MHz respect to the central frequency. The tone lasts 128 (Fig. 4.7(a)) or 64 (Fig. 4.7(b)) samples. Despite the self-interference generated by the transmitted tone, it is evident from the figures that it is possible to perform parallel transmissions and receptions of tones. This interference causes a power peaks at -4.69MHz, 4.69MHz and 9.38MHz, which are the transmitted tone, the spurious tones generated at the mirror frequency and at twice the frequency of the tone respectively. Considering that the power of the second spurious tone is comparable with the noise, it is not important to be considered. The narrow bandwidth of spurious tones and the opportunistic selection of contention tones allow the correct identification of other four tones transmitted at -6.56MHz, -3.12MHz, 5.94MHz, and 7.81MHz. Before comparing ReCo_f performance with legacy DCF (in the next section), we tested the cover range and the robustness of the frequency-domain contention mechanism under different propagation and interference conditions.

Concerning the study of the cover range, we conducted two different experiments: (i) outdoor and (ii) indoor evaluations.

A first study was performed in an anechoic chamber, in order to reproduce the same conditions of outdoor scenario. This investigation is necessary to understand the impact on the cover range. Moreover, this study also allow

[2]The power of background noise is estimated by averaging the FFT samples at frequencies different from the ones in which tone transmissions or spurious signals can be detected. The threshold is then obtained by adding a margin to this noise level.



(a) (b)

FIGURE 4.7: FFT samples received by a wireless node in a first contention round with 5 competing stations, with tones lasting 128 samples (a) or 64 samples (b). Shorter tones result in an increased width of the power peak lobs.

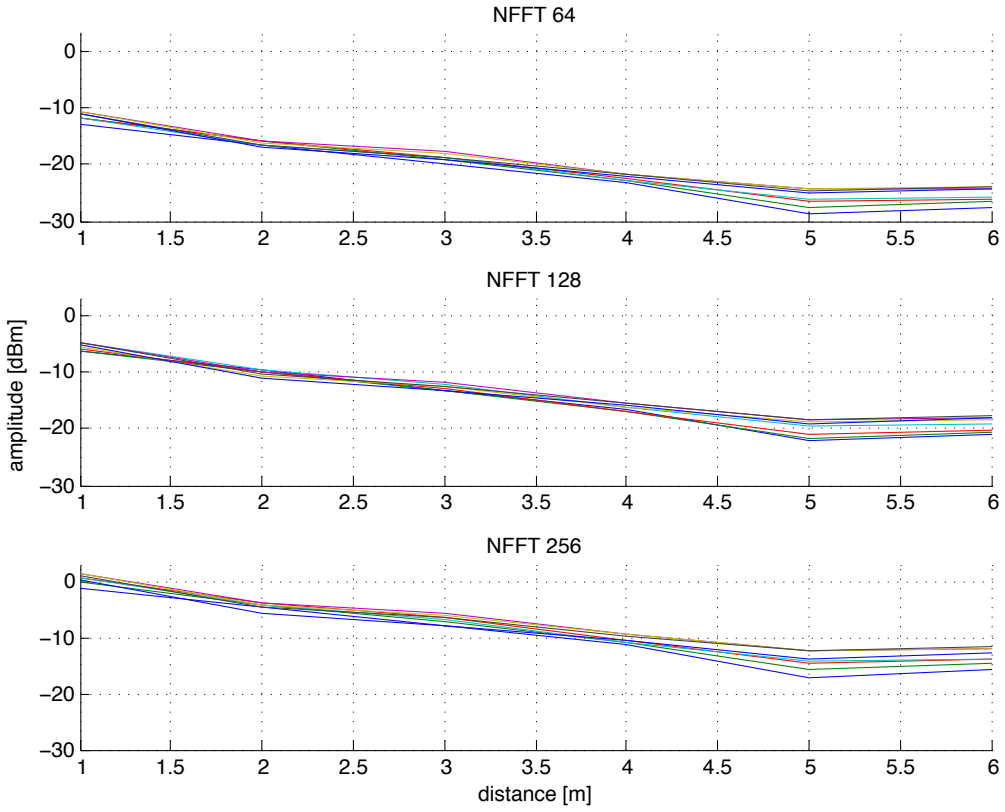


FIGURE 4.8: Ploss Anhecoic

to find a trade-off between the duration of tones (equivalent to the resolution of the IFFT) and the Tone Detection Error Rate. Because of limit of the anechoic chamber in terms of width, we transmitted with low power. We deployed two WMP WARP nodes with various distances with steps of $1m$ and for each distance we run 200 transmissions over all available tones. The maximum distance is $6m$ and ReCo_f is set to $s = 1$ and $m = 8$. For statistical

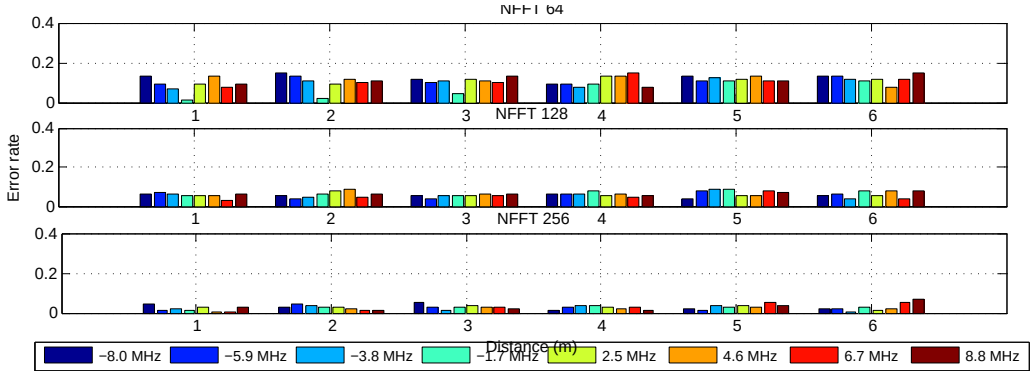


FIGURE 4.9: Peak detection error estimation in anhecoic room

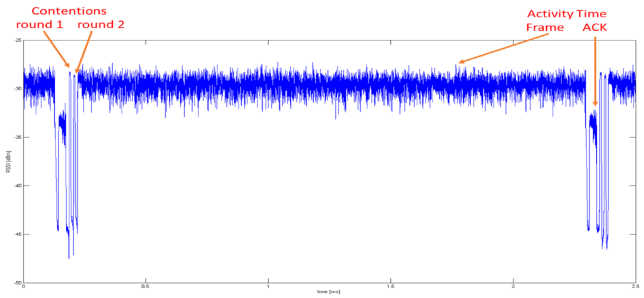


FIGURE 4.10: Channel trace acquisition during traffic session when WMP ReCo_f implementation is active

purposes, in this evaluation the tone for the contention is not chosen randomly but in a deterministic way. In Fig. 4.8 and in Fig. 4.9, we compared respectively pathloss and the Tone Detection Error Rate over distance when the FFT resolution changes. It is possible to note that Tone Detection Error Rate is not equal to zero. This is due to the low power level in reception. Hence, in this kind of set-up (anechoic chamber with only one transmitter) the gaussian noise is considered as possible tones.

Regarding the indoor scenario, we decided to study the cover range of ReCo_f for a simple reason. Considering that the node send tones in a specific sub-bandwidth respect to the total bandwidth, the power spectral density of a specific tone is higher. Thus, the reception power will be higher, as is confirmed in Fig. 4.10, as well as the coverage region. This makes visible nodes that would be hidden with the traditional WiFi transmission.

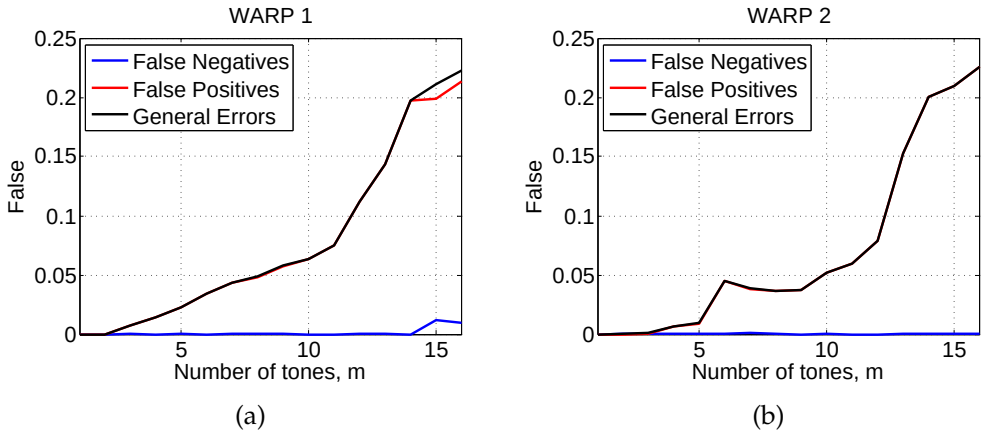
For this purpose, we deployed two WMP WARP nodes in an indoor scenario, with different position, in order to check the coverage area of the sent frames and tones. This was performed with an FFT of 128 points on the receiver side and 11 random tones. We run 3 experiment trials with 2 WMP WARP, placed at three different distances (i.e. 5, 10 and 15 meters). For each trial, we sent 1000 tones and 1000 frames. We repeated each trial three times, with three different transmission power levels, more specifically 0dBm (low), 11dBm (medium) and 22dBm (high). Table 4.2 shows the result of the experiment in term of received tones and frames. This kind of evaluation demonstrates that the transmitted tone can cover an higher distance in comparison

with frame. As expected, this feature of the ReCo scheme could be used in order to solve the problem of hidden node in WiFi networks.

In addition, ReCo tones could be improved in order to transport additional information signal. The information signal will be able to disseminate a network allocation virtual (NAV) to nodes that are not able to sense the normal frame sent by the transmitter. In this way, these nodes will not attempt to access to the channel until the end of current transmission, also if they are not able to recognize the frame.

	Distance [m]	Noise [dBm]	RX Tone [#]	RSSI Tone [Average dBm]	RX Frame [#]	RSSI Frame [Average dBm]
Low TX Power	5	-94.362	1000	-70.490	0	-93.816
	10	-94.367	981	-84.140	0	-94.333
	15	-94.364	881	-86.901	0	-94.335
Medium TX Power	5	-94.372	1000	-55.122	1000	-88.129
	10	-94.347	1000	-70.330	407	-92.955
	15	-94.355	1000	-66.789	326	-93.154
High TX Power	5	-94.362	1000	-49.777	1000	-75.198
	10	-94.346	1000	-65.571	1000	-89.081
	15	-94.365	999	-64.210	1000	-88.391

TABLE 4.2: Tones and frame sensing in indoor scenario.



(a) (b)

FIGURE 4.11: False detection made by the detection algorithm with variable threshold tuned as a function of the background noise.

As mentioned, a second analysis addressed in this section concerns the robustness of the frequency-domain contention mechanism. For this reason, we conducted two different experiments: (i) analysis of detection errors when the nodes number varies and the determination of the threshold value and (ii) analysis of the whole contention mechanism.

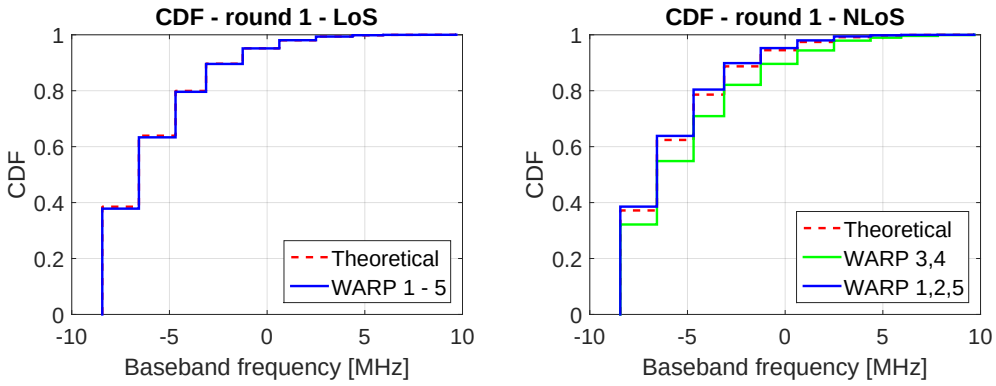
For the first study about the robustness of the frequency-domain contention mechanism, we traced more than 60000 contentions, with $s = 1$, for each number of tones (m). We used two WARPs in LoS and with a distance of $1m$. For each round we collected three variables: the two indices of the transmitted tones from the two stations and the result of the Tone detection algorithm. Fig. 4.11 shows the false detection as result of the detection algorithm with a specific threshold selected according to the background noise.

The false negatives occur when the detection algorithm does not detect that the other station has sent a tone with a higher index. Indeed, if this event happens, the station believes to have won and to be able to proceed to the next round. In the case of the last round both stations believe to have won causing a collision. Conversely, false positives occur when the detection algorithm erroneously detects a tone with a higher index that is not present. This event could be due to external disturbances or impulsive noise. If this event occurs in the last round, it causes a period of silence equal to a DIFS. Using the detection algorithm with a hardcoded threshold, the number of false positives and negatives is almost zero. Comparing the efficiency in term of throughput, it is obvious that false negatives are more catastrophic than false positives, since a collision is worst than a period of silence. In Fig. 4.11 we note that the false negatives are almost zero, while the false positives reach high values, but this event does not involve great loss in term of time (only a DIFS slot and the repetition of the contention). We also note that for 11 tones ($m = 11$) the number of false positives is also low. This evaluation is very important for our real implementation which uses exactly 11 tones.

For the second study about the analysis of the whole contention mechanism, we traced more than 30000 contentions with five WARP-based nodes extended for supporting tone transmission and reception primitives. A contention mechanism with two contention rounds has been implemented by modifying the DCF firmware available for the WARP 802.11 reference design. At each node, we collected the tone index of the station winning the contention (i.e. the smallest frequency in which a tone transmission has been recognized) each contention round. We then compared the cumulative probability distribution of the winning tone found by each station.

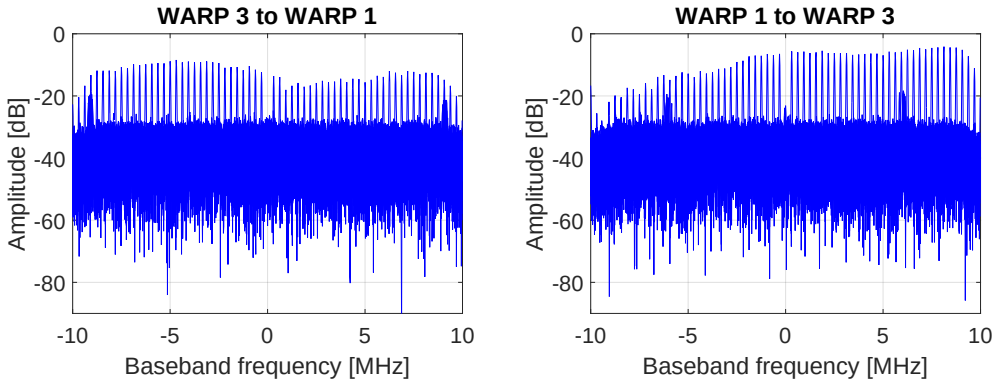
When all the nodes are located in the same room under line-of-sight propagation conditions, we found that each node sees exactly (very nearly) the same distribution. In the first contention round the distribution is given by the minimum of five uniform distributions of 11 possible values, as depicted in Fig. 4.12(a). The negligible mismatch between the theoretical and experimental results is given by imperfect round detection (not considered in the analysis). When one node is moved to a different room or is hidden by means of an obstacle, we found that distributions observed by each node do not coincide anymore. In Fig. 4.12(b), for example, we can clearly observe that stations 3 and 4 see a probability equal to 0.32 that the first contention round ends with a transmission on the first tone, while the other stations see a probability value equal to 0.38. Indeed, in some cases, nodes 3 and 4 are not able to hear the tones sent by the other stations. The possibility to hear or not tones also depends on the specific frequency selected by the far station for contention. Indeed, in absence of a dominant propagation path, the channel can be selective in frequency and therefore the tone transmissions performed by the far station that can be detected by the other contending nodes are no more uniformly distributed among the available frequencies. These considerations are quantified in Fig. 4.13(a) and Fig. 4.13(b), where we visualize

the channel response between station 3 and station 1 in two different link directions. Because tone attenuations strongly depend on the sub-carrier index and the channel is not symmetrical, the contention process is no more fair. For example, since transmitted tones by station 1 with low sub-carrier indexes are highly attenuated at the receiver of the station 3 (as depicted in Fig. 4.13(b), the winning probability in the first contention round of the station 3 is higher.



(a) (b)

FIGURE 4.12: Cumulative Distribution Function of tone transmissions observed by five contending stations in Line Of Sight (a) and No Line Of Sight (b) propagation conditions among the stations.

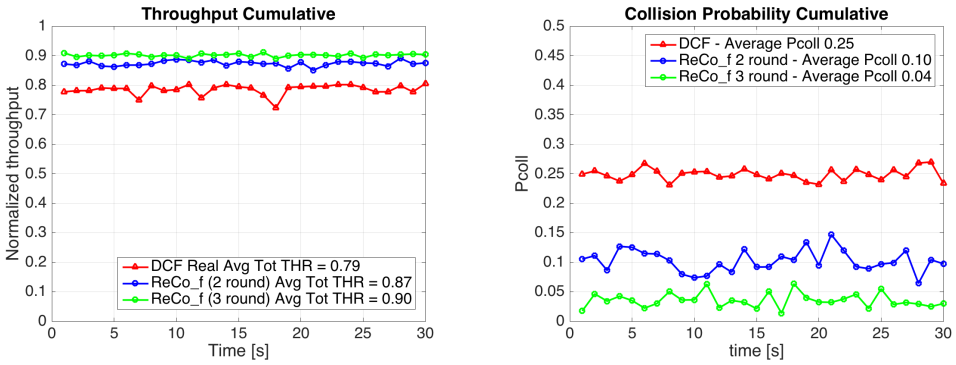


(a) (b)

FIGURE 4.13: Effects of selective fading on tone detection: channel response between station 3 and station 1 in two different link directions.

4.5.3 ReCo_f performance evaluation

We then run several performance tests by limiting our observations when all stations work in line-of-sight. In this context, tone contention is not degraded



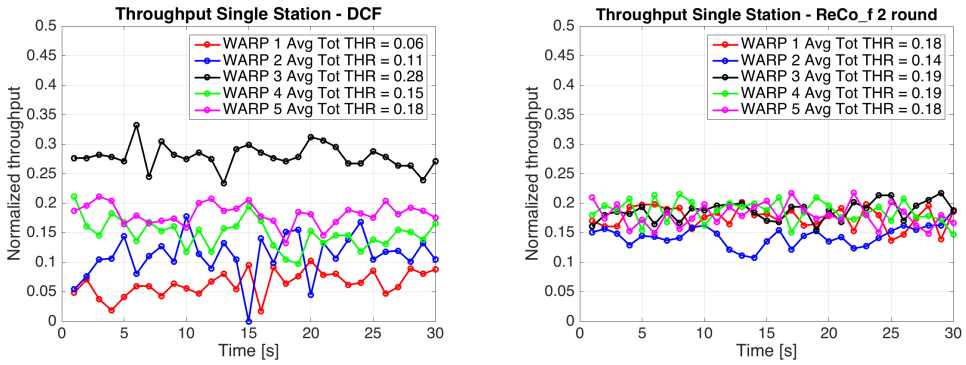
(a) (b)

FIGURE 4.14: Experimental throughput (a) and collision probability (b) results in case of legacy DCF (red curve), ReCo_f with 2 rounds (blue curve) and ReCo_f with 3 rounds (green curve) with 5 contending stations.

by selective fading, but only by errors due to the detection algorithm of the tones. Source rates have been configured for guaranteeing saturation conditions with data packets of 1500 *bytes* and a data transmission rate of 6 *Mbps*. The duration of each experiment has been set to 30 seconds.

Fig. 4.14(a) shows the total normalized throughput achieved with 5 contending stations in case of legacy DCF and in case of ReCo_f with two ($s = 2$) or three ($s = 3$) contention rounds and a number of contention tones m equal to 11. Contention tones have been selected according to the list summarized in table 4.1. From the figure, we see that the normalized throughput is 79% for DCF, 87% for ReCo_f with $s = 2$ and 90% for ReCo_f with $s = 3$.

Note that ReCo_f spends a fixed contention time for each channel access, which is given by product between the number of contention rounds and the duration of a contention tone (i.e. 2 or 3 times 9 μs), while the DCF contention time depends on the number of contending stations and on the minimum contention window CW_{min}. Although for 5 stations and $CW_{min} = 15$ the average contention time for DCF is lower than ReCo_f (about 1.5 backoff slots of 9 μs), ReCo_f efficiency is higher because of the reduction of the collision rate (as shown in Figure 4.14(b)). Indeed, the average collision probability perceived with DCF is 0.25 (consistent with the well known Bianchi's result [84]), while such a value is reduced to 0.10 and 0.04 for ReCo_f with, respectively, $s = 2$ and $s = 3$. Finally, as summarized in Fig. 4.15, we observe that ReCo_f improves the per-station fairness in comparison with DCF, because the average throughput perceived by each station exhibits a variability lower than DCF, even with two contention rounds. More into details, in our experiment we found that per-station normalized throughout achieved under legacy DCF varies in the range $[0.06, 0.28]$ between the worst and best performing station, while for ReCo_f case this range is reduced to $[0.14 - 0.19]$.



(a) (b)

FIGURE 4.15: Per-station throughput results in case of legacy DCF (a) and ReCo_f whit 2 round (b)

4.6 Impact of imperfect channel sensing

Our experimental results have shown that imperfect tone detection can lead to non-uniform views of contention results among the stations. In order to gain insight into the effect of imperfect channel sensing on ReCo, we run some simulations thus enabling more complex network configurations than with the test-bed setup.

Following the approach of [87, 63], we adopt a multi-slope path loss model. In case of two slopes, the key parameters of the model are the cut-off distance and the path loss exponents of the close-in range and of the far range. The path gain G_{set} as a function of the distance d between the transmitter and the receiver is given by:

$$G_{det}(d) = \begin{cases} \kappa \left(\frac{d}{d_0}\right)^{\alpha_1} & d_0 \leq d \leq d_c \\ \kappa \left(\frac{d_c}{d_0}\right)^{\alpha_1} \left(\frac{d}{d_c}\right)^{\alpha_2} & d \geq d_c \end{cases} \tag{4.23}$$

where κ is the reference gain at distance d_0 (e.g., 1 m) and d_c is the cut-off distance. In the following, we assume $d_c = 10\ m$ (reminiscent of an indoor environment), $\alpha_1 = 2$, $\alpha_2 = 4$, $\kappa = 9.27 \cdot 10^{-5}$ (i.e., $\approx -40.3\ dB$; this value corresponds to a carrier frequency of $f_c = 2.48\ GHz$ and 0 antenna gains).

Besides the deterministic component of the path gain, we assume also a log-normal shadowing S and a Rayleigh fading channel coefficient $H(f_k)$ at frequency f_k, independently for each sub-carrier frequency. Then, $S \sim e^{\beta\sigma_S Z} e^{-\beta^2\sigma_S^2/2}$, with $\beta = \log(10)/10$, $Z \sim \mathcal{N}(0,1)$ and the scaling factor is set so that $\mathrm{E}[S] = 1$. As for the Rayleigh fading, it is $|H(f_k)|^2 \sim \mathrm{Exp}(1)$, i.e., a negative exponential random variable with mean value equal to 1. Then, the power gain between two stations at a distance d on a sub-carrier k can be written as $G(d,k) = G_{det}(d) S |H(f_k)|^2$.

With ReCo_f, a sample of the signal received by station j on sub-carrier k can be written as

$$y(j,k) = \sum_{j \neq i} x(i,k) \sqrt{G(d_{ij},k) P_{tx}} + w(k) \tag{4.24}$$

where $x(i,k) = 1$ iff station i selects sub-carrier k for sending its tone, and d_{ij} is the distance between the station i and station j. The additive noise $w(k)$ encompasses the noise floor and the unsuppressed self-interference on the sub-carrier k. It is modeled as a Gaussian random variable with zero mean and power $\sigma^2_{w(k)} = (P_N + P_{tx}/A_{SIS})/n_{sc}$, where n_{sc} is the number of sub-carriers, P_N is the noise floor on the entire bandwidth, A_{SIS} is the self-interference suppression. We assume that $A_{SIS} = 100\ dB$[3]. The noise floor is assumed to be $P_N = -90\ dBm$ for a bandwidth of 20 MHz.

With ReCo_t, we assume that a transmitting station spreads its power budget uniformly over all sub-carriers. Then, a sample of the signal received by station j is

$$y(j) = \sum_{j \neq i} x(i) \sqrt{\sum_{k=1}^{n_{sc}} G(d_{ij},k) \frac{P_{tx}}{n_{sc}}} + w \tag{4.25}$$

where $x(i) = 1$ if station i transmits, d_{ij} is defined as above, and $w \sim \mathcal{N}(0, P_N)$.

To assert whether a sub-carrier (ReCo_f) or the entire channel (ReCo_t) is idle (physical Clear Channel Assessment, CCA), the power level is sampled n_s times, say y_ℓ is the ℓ-th sample. The estimated average power level metric is evaluated as $\hat{P}_{rx} = \frac{1}{n_s} \sum_{\ell=1}^{n_s} |y_\ell|^2$. The metric $\hat{P}_{rx}$ is compared with the *Defer Threshold* (DT), set to the noise floor plus a margin. Specifically, the DT is set 3 dB over the noise floor, i.e., $DT = 2P_N = -87\ dBm$[4].

In the simulated WLAN, the Access Point (AP) is located at $(x_0, y_0) = (0,0)$. The positions of n stations around the AP are distributed uniformly within a maximum distance R from the AP. A station receiving an average power level less than the *Carrier Detect Threshold* (CDT) from the AP is considered to be in outage and excluded from the WLAN (in other words, it cannot associate with the AP). The CDT is set to $-85\ dBm$ for a bandwidth of 20 MHz.

Table 4.3 summarizes the simulation parameters and gives the numerical values used.

Figure 4.16 shows the probability distribution of the number of stations surviving one contention round for $m = 11$, the same value used in the test-bed experiments. Square markers correspond to simulations results (including the 95% confidence intervals), while the dashed red line is the theoretical

[3] 110 dB of suppression with a single antenna system have been demonstrated successfully [53], so our assumption for A_{SIS} is conservative.

[4] This technique of transmitting the transmitted tones is not the same used in Sec. 4.5.2, but we have found it more correct to express the problem mathematically in this way, experimentally the two methods provide the same results.

P_N	Noise floor power level	$-90\ dBm$
W_{ch}	Radio channel bandwidth	$20\ MHz$
DT	Defer Threshold	$2 \cdot P_N$
CDT	Carrier Detect Threshold	$-85\ dBm$
P_{tx}	Transmission power level	$20\ dBm$
A_{SIS}	Self-interference suppression	$100\ dB$
σ_S	Shadowing standard deviation	$8\ dB$
d_c	Cut-off distance of the path loss	$10\ m$
n_{sc}	Number of sub-carriers	64
R	Radius of the WLAN area	$20\ m$
n_s	Number of samples	64

TABLE 4.3: Numerical values of parameters used in the simulation.

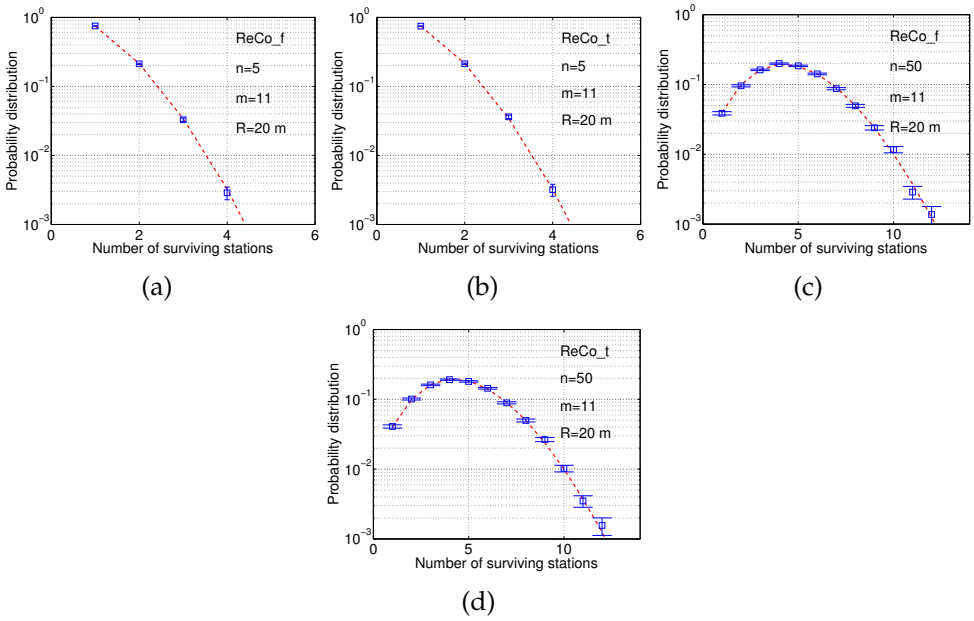
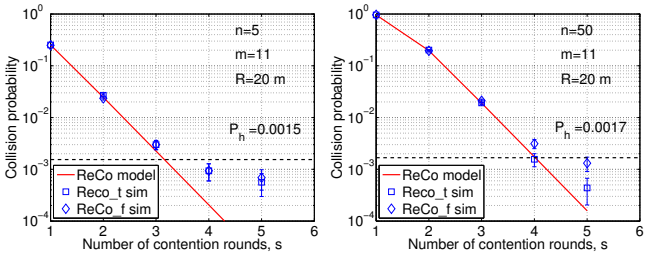


FIGURE 4.16: Probability distribution of the number of station winning a single contention round (square marks: simulations, with 95% confidence intervals; dashed line: analytical model). The maximum distance of a station from the AP is $R = 20\ m$, $m = 11$. (a) $n = 5$ stations with ReCo_f; (b) $n = 5$ stations with ReCo_t; (c) $n = 50$ stations with ReCo_f; (d) $n = 50$ stations with ReCo_t.

probability distribution as found from the analytical model of Sec. 4.4. We consider two scenarios: a small WLAN with $n = 5$ stations (Fig. 4.16(a) for ReCo_f and Fig. 4.16(b) for ReCo_t), and a crowded WLAN with $n = 50$ stations (Fig. 4.16(c) for ReCo_f and Fig. 4.16(d) for ReCo_t).

It is apparent that the analytical model matches the outcome of the simulations in spite of the radio channel impairments accounted for by the simulation model. In no one of the considered scenarios the event of no station surviving is triggered. This could occur in case a station mistaked a spike of



(a) (b)

FIGURE 4.17: ReCo collision probability as a function of the number of contention rounds s for $m = 11$, $n = 5$ stations (left plot) and $n = 50$ stations (right plot), with a maximum distance of $R = 20$ m from the AP. The probability that two stations be hidden to each other is annotated into the graph boxes and marked by a dashed horizontal line.

noise and/or self-interference for a busy tone.

While the first round of the access contention is not affected sensitively by physical layer impairments, the analyze of the collision probability highlights some issues. Figure 4.17 shows the collision probability as a function of the number of contention rounds, up to $s = 5$ contention rounds, for $n = 5$ stations (Fig. 4.17(a)) and 50 stations (Fig. 4.17(b)), $m = 11$, both for ReCo_f and ReCo_t.

The solid line represents the analytical model results that assume ideal sensing. The square and diamond markers (with 95% confidence intervals) represent the outcome of simulations of ReCo_t and ReCo_f, respectively. The probability that a couple of stations be hidden (i.e., the average power level received when one transmits and the other receives be less than DT) is annotated on each graph. It is apparent that the analytical model predicts the collision probability correctly both with few and many stations, up to the point where the collision probability level falls below the probability of having hidden stations (marked by a dashed horizontal line). Below that level, the analytical model is optimistic. The actual level of collision probability is bigger, due to false negatives, i.e., to stations missing the busy tones of the hidden stations. While ReCo_t and ReCo_f achieve close performance levels with few stations, in a crowded WLAN ReCo_f appears to be more critical. The main conclusion pointed out by the simulation experiments is that ReCo holds the promise of attaining a low level of collision probability ($3.1 \cdot 10^{-3}$ for $s = 4$ with $n = 50$ stations), yet it looses its effectiveness as the physical carrier sensing does not work fully any more, as quite natural with any version of a CSMA protocol. It is a development line for future work to understand fully and be able to predict by means of quantitative models the impact of radio channel impairments on ReCo (e.g., interference, non-ideal sensing circuitry, imperfect self-interference suppression).

Chapter 5

Conclusions

In this thesis, we exploit advantages of the flexibility of the PHY layer over different point of views.

At the beginning, we have introduced the concept of in-band spectrum agility, for improving link-level and network-level performance of emerging wireless networks, in many different operating conditions. New physical layer capabilities have been envisioned and demonstrated in a real prototype for adapting the channel width at each transmission attempt within a predefined operating channel. Our prototype has been designed with minor modifications on a legacy 802.11 OFDM transceiver. Although these new capabilities can be further exploited with specialized access protocols, for example by taking independent carrier sensing and decisions at each subchannel, we demonstrated significant performance improvement even under legacy access policies.

Next, we analyzed in detail the behaviour of an OFDM-based communication system in different important scenarios in order to examined the weaknesses of a standard OFDM system. We evaluated also the response of this modulation technique at different types of jammers in order to evaluate an intelligent strategy to avoid the bad performance in some situations. We proposed a physical solution and an adaptive mechanism regarding the improvement of the safety. New physical layer modifications have been envisioned and demonstrated with experiments. Our verification was carried out with some adjustments of a standard 802.11 OFDM implementation. Although this solution can be extended randomizing the pattern of pilot subcarriers according to a logic mechanism so that receiver and transmitter can be safe from any pilot nulling attacks without an a priori scheme, we demonstrated significant performance improvements in terms of BER also in absence of randomization of pilot tones. Hopping of pilot tones is a promising solution for improving the physical layer security of OFDM communications. We also propose an adaptive algorithm in order to increase the power level

of the signal and make the situation more difficult for the opponent. The combination of this pilot hopping solution with the data subcarrier adaptive algorithm could be the key to mitigate jamming attacks.

Finally, we have explored the possibility of running multiple contention rounds in random access networks for improving the channel utilization efficiency, by considering the practical feasibility of multiple contentions and the achievable performance improvements. Regarding the first aspect, we have demonstrated that repeated contentions can work, as well as in the domain of time, also in the time and frequency domains and can be easily implemented on current wireless technologies. Indeed, the time-based version is built on primitives already provided by commercial IEEE 802.11 cards, which can be composed in a new protocol by exploiting programmable firmwares, while the frequency-based version, which in principle requires new primitives for transmitting and receiving signaling tones, can be easily supported by OFDM-based PHY layers.

Appendix A

Hardware Equipment

In this appendix, we present a description of hardware equipment adopted for development, testing and different experiment setups. We used two FPGA-based SDRs: WARP v3 and USRP X310.

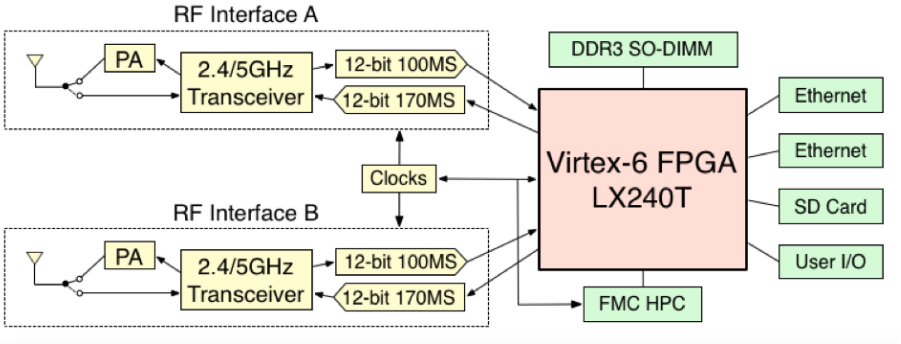
A.1 Wireless Open-Access Research Platform (WARP)

WARP v3 is the latest generation of WARP hardware. It is designed and sold by Mango Communication. The Mango Communications team also designs and maintains many of the resources in open-source WARP Repository.

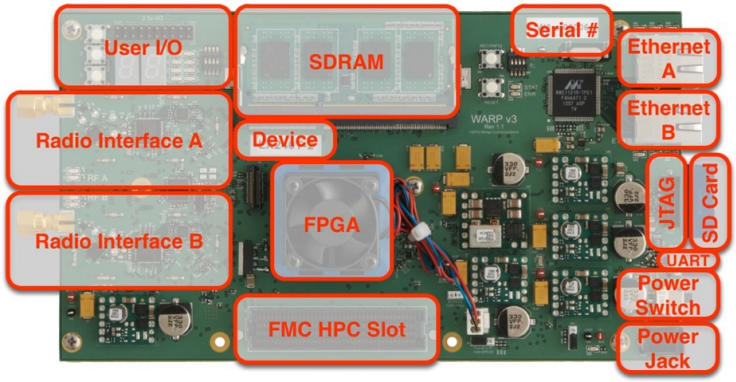
WARP v3 is shown in A.1(b). The block diagram below shown in Fig. A.1(a) gives an overview of the hardware design that integrates:

- a Xilinx Virtex-6 LX240T FPGA;
- two programmable RF interfaces. Each includes:
  - a 2.4/5 GHz transceiver;
  - two 100MSps 12-bit ADCs;
  - two 170MSps 12-bit DACs;
  - a dual-band PA (Power Amplifier) with transmission power up to 20 dBm;
  - Shared clocking for MIMO applications.
- a high-pin count (HPC) FMC (FPGA Mezzanine Card High Pin Count) carrier slot;
- two Ethernet interfaces;
- a 2 GB slot DDR3 SO-DIMM;

- FPGA configuration through JTAG, SD card or SPI flash;
- user I/O:
  - an USB-UART;
  - 12 LEDs (6 green, 6 red);
  - two 7-segment displays;
  - 4 push buttons;
  - 4 bit DIP switch.



(a)



(b)

FIGURE A.1: Block chain of the WARP (a) and platform (b).

The WARP v3 board integrates two identical RF interfaces shown in Fig. A.2. An RF interface is composed by three main block:

- the Analog Devices AD9963 handles the conversion between the analog I/Q and digital I/Q domains. It integrates two 100MSps 12-bit ADCs, two 170MSps 12-bit DACs, interpolation and decimation filters and programmable analog gain and offset adjustments;
- the Maxim MAX2829 transceiver translates between baseband and RF. It implements both 2.4 and 5GHz Tx/Rx paths;
- the Anadigics AWL6951 dual-band power amplifier.

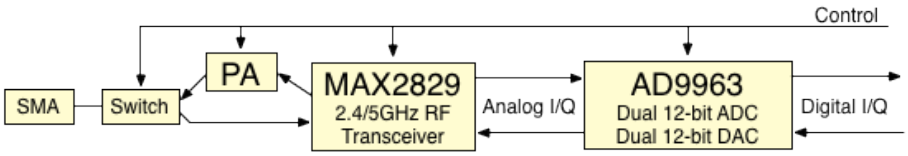


FIGURE A.2: RF interface in a WARP platform.

A.1.1 802.11 Reference Design

The 802.11 Reference Design is implemented in the FPGA: OFDM transmission technique is implemented in the PHY layer with multiple cores. Instead, the MAC is implemented in software running in two MicroBlaze CPUs, with a support core in the FPGA to achieve accurate inter-packet timing. The architecture is shown in A.3. The entire 802.11 implementation is instanced in five main FPGA blocks:

- *CPU High*: a MicroBlaze CPU executes the top-level MAC code and other high-level functions. All non-control packets for transmission and the various handshakes with nodes (probe request/response, association request/response, etc.) are generated from CPU High, which is also responsible for implementing encapsulation and de-encapsulation of Ethernet frames according to the IEEE 802.11 standard. CPU High is clocked at 160MHz.
- *CPU Low*: a MicroBlaze CPU executes the low-level code for the MAC distributed coordination function (DCF). This code is responsible for all MAC-PHY interactions and for handling intra-packet state that includes transmission of ACKs, scheduling of backoffs, maintaining the contention window and other DCF functions. CPU Low is clocked at 160MHz.
- *MAC DCF Core*: an FPGA core which acts as the interface between the MAC software design and the Tx/Rx PHY cores. This core implements the timers required for the DCF (timeout, backoff, DIFS, SIFS, etc.) and the various carrier sensing mechanisms.
- *PHY Tx/Rx*: These peripheral cores implement the OFDM physical layer transceiver specified in the 802.11 standard.
- *Hardware Support*: these cores enable control of the various peripheral interfaces on WARP v3 from the code in CPU Low (for example the ad_controller and the radio_controller).

The 802.11 design is composed by these various cores that are integrated in Xilinx Platform Studio (XPS). The source code/models for all components are available in the repository (http://warpproject.org/trac/browser/ReferenceDesigns/w3_802.11). Then, the output of the XPS project is integrated in Xilinx Software Development Kit (SDK), which compiles and integrates the software of the two MicroBlaze CPUs in the entire design. Ultimately, the combination

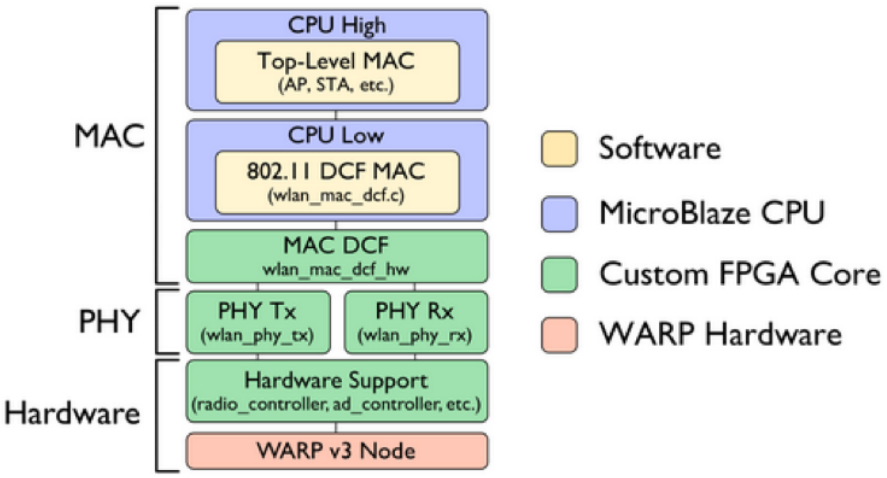


FIGURE A.3: WARP architecture.

of hardware and software projects allow to configure the FPGA through a loading of bitstream.

A.1.2 WARPLab Reference Design

The WARPLab Reference Design enables rapid PHY prototyping using WARP hardware for waveform Tx/Rx and MATLAB for signal processing. It is a framework for rapid physical layer prototyping that allows for coordination of arbitrary combinations of single and multi-antenna transmit and receive nodes. Moreover, it allows many physical layer designs to be constructed and tested.

A.2 Universal Software Radio Peripheral (USRP)

USRP X310 is an SDR designed and sold by Ettus Research and National Instrument.

USRP X310 is shown in A.4.

The hardware design integrates:

- a Xilinx Kintex-7 FPGA;
- two wide-bandwidth RF daughterboard slots:
  - up to 160MHz bandwidth;
  - selection covers DC to 6 GHz.
- multiple high-speed interfaces:
  - PCI Express;

  - dual 10 Gigabit Ethernet;
  - dual 1 Gigabit Ethernet.
- external PPS input & output;
- external 10 MHz input & output;
- external GPIO Connector with UHD API control;
- external USB Connection for built-in JTAG debugger.

FIGURE A.4: USRP X310.

The USRP hardware driver (UHD) is the device driver provided by Ettus Research for use with the USRP product family. Several frameworks including GNU Radio, LabVIEW, MATLAB and Simulink use UHD.

Appendix B

Implementation Details

In this appendix, we present a description of the implementation details for all the different levels of programmability previously examined in this thesis.

B.1 Agile Receiver Implementation

For implementing the *Agile Receiver* we used some Xilinx available tools: (i) System Generator, (ii) Project Navigator, (iii) Xilinx Platform Studio (XPS), (iv) Xilinx Software Developer Kit (Xilinx SDK) and (v) ChipScope Pro.

System Generator is an architecture-level design tool to define, test and implement high-performance algorithms on Xilinx devices. Also, System Generator enables FPGA implementation of algorithms, developed in MATLAB and Simulink. We used System Generator in order to develop, build and test the new clock selector Intellectual Property Core (IP Core) and to modify the wlan_phy_rx IP Core of the whole design provided by Mango Communication. IP Cores are blocks or modules that have been designed and tested for a specific function such as processors, ethernet interfaces and RAM controllers.

Project Navigator manages design files and allows to run processes to move the design from design creation through implementation to programming the targeted Xilinx device. We used Project Navigator only for modifying the VHDL and/or Verilog code of some IP Cores provided by Mango Communication (i.e. ad_controller and radio_controller) and for the simulation of the input/output pins behaviour.

Xilinx Platform Studio helps the hardware designer to easily build, connect and configure embedded processor-based systems, from simple state

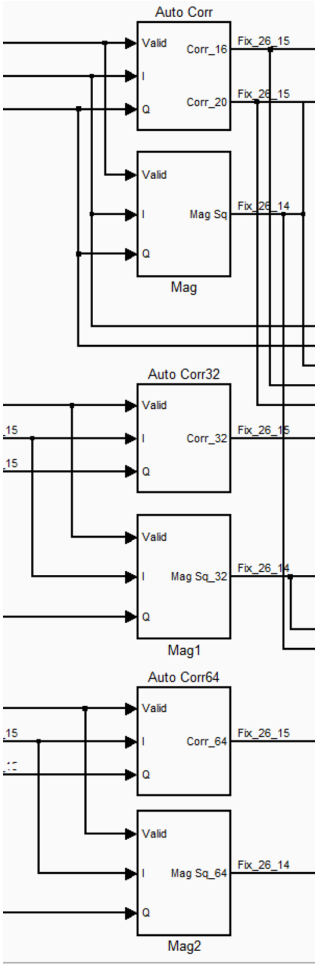


FIGURE B.1: Three parallel correlations on windows of 16, 32 and 64 samples.

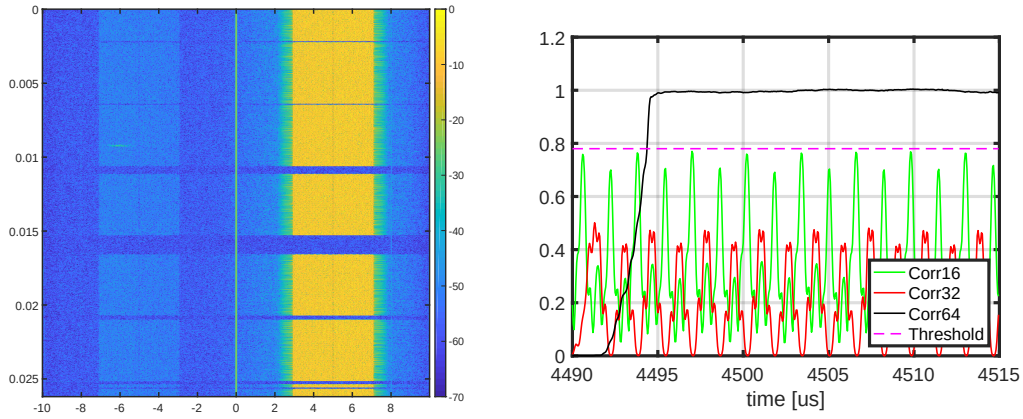
machines to 32-bit RISC microprocessor systems. Moreover, it has the ability to configure and integrate IP cores from the Xilinx Embedded IP catalog, with custom or 3rd party Verilog and VHDL designs. We used XPS in order to integrate our custom IP Cores into the whole design.

Xilinx Software Developer Kit is the Integrated Design Environment (IDE) for creating embedded applications on any of Xilinx microprocessors (for example Zynq UltraScale+ MPSoC and Zynq-7000 SoCs) and the MicroBlaze soft-core microprocessor. We used Xilinx SDK in order to modify some values of some certain registers and to create other primitive functions so to perform the necessary actions for the proper operations of the *Agile Receiver*.

ChipScope Pro tool inserts logic analyzer, system analyzer, and it allows to view any internal signal or node, including embedded hard or soft processors. Signals are captured in the system at the speed of operation. Captured signals are then displayed and analyzed using the ChipScope Pro Analyzer tool. We used ChipScope Pro Analyzer in order to control the behaviour of some selected signals of our implementations.

As mentioned in the chapter regarding the Agile Receiver, using System

Generator we created a custom wlan_phy_rx IP Core in order to extend the capabilities of a standard receiver. Indeed, we replicated the correlator blocks, in order to perform three parallel correlations on windows of 16, 32 and 64 samples, as shown in Fig. B.1. For deciding if the correlation is positive or not, the correlation result is compared with a percentage of the sum of the modules of the first window W of samples used for correlation. This implementation do not consider possibilities to have transmissions with a channel bandwidth of 10 MHz and 5 MHz at +/-5 MHz respect to the central frequency. Indeed, in these kind of scenarios, the correlators on windows of 32 and 64 samples produce an output greater than the reference threshold causing the activation of the receiver chain.



(a) (b)

FIGURE B.2: Spectrogram (a) and correlation results (b) in presence of incoming packets with a channel bandwidth of 5 MHz and with a shift of +5 MHz respect to the central frequency.

Figure B.2 is an evaluation in MATLAB of a possible scenario with a transmission with a channel bandwidth of 5 MHz and shifted of +5 MHz respect to the central frequency. This kind of behavior can be used to detect packet sent with a shift of +/-5 MHz from the central frequency with a channel bandwidth of 5 MHz or 10 MHz. For this reason, we decided to introduce a further analysis, a spectral spectral, through an FFT, as show in Fig. B.3. The results of the FFT allows to immediately identify also preambles transmitted with a central frequency different from the possible ones. As mentioned before, the decision logic works by comparing the sub-carrier amplitude with a threshold calculated by averaging the amplitude of 12, 18 or 24 sub-carriers around the central frequency and at +/-5 MHz. When all the sub-carriers of the selected sub-set are "active", then a flag is set to 1 and a preamble is recognized among the 7 possible configurations (i.e. channel bandwidth of 5, 10 and 20 MHz in the central frequency, 5 and 10 MHz with a shift of -5 MHz and 5 and 10 MHz with a shift of +5 MHz). Moreover, we changed also the wlan_agc IP Core in order to have a right DCO correction also for 10 and 5 MHz. Indeed, we replicated the DCO correction block at 20 MHz, but using different clocks (i.e. 10 and 5 MHz).

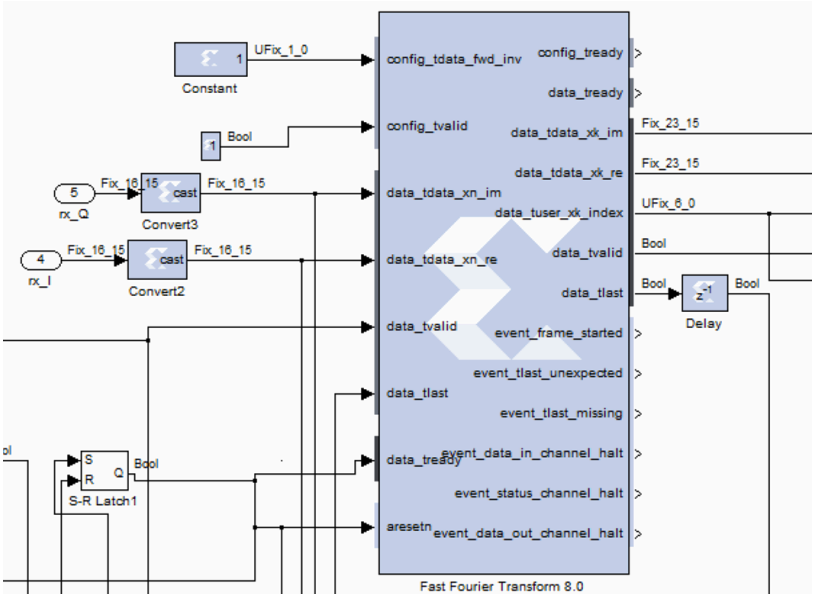


FIGURE B.3: FFT block in the implementation.

For decoding the packet in the right way according to the frequency and/or the channel bandwidth detected, we have to modify: (i) the central frequency and/or (ii) the clock of the receiver chain.

For modifying the ADC rate and the central frequency, it is necessary change some parameters of AD9963 and MAX2829 chips respectively. These parameters can be modified by changing some values of some registers, but writing operation on register takes long time. For this reason, we decided to execute these operations in hardware. We used Project Navigator for modifying and test the native ad_controller and radio_controller IP Cores. With our implementation, we can perform all the modification in time and on-the-fly.

In IEEE 802.11g standard the only possible channel bandwidth is 20 MHz. For this reason, in addition to the two system clocks (CLKOUT0 and CLKOUT1) at 160 and 80 MHz, only more two clocks are generated (CLKOUT2 and CLKOUT3) at 20 MHz and at 20 MHz shifted by 90 degree phase respectively. The latter clock is necessary to feed the ad_bridge, an important IP Core for interfacing user designs with the digital I/Q interfaces of the AD9963 ADCs/DACs, whose digital ports are double data rate (DDR) interfaces with interleaved I/Q. Conversely, in order to change properly the width of the channel, we need to have different clocks corresponding to the different channel bandwidths. Figure B.4 shows the block related to the generation of the clocks necessary for the whole agile design. In addition to the two system clocks and the other two clocks at 20 MHz, we added others 4 clocks, two for each possible bandwidth. Having these available clocks, now we have to selected the corresponding clock depending on the detection. For this reason, we used again System Generator for creating a new IP Core, called clock_selector IP Core. It selects the right clock for the ad_bridge and the wlan_phy_rx IP Cores. As shown in Fig. B.5, the clock_selector IP Core has a selector and 6 different clocks as inputs. Depending on the value

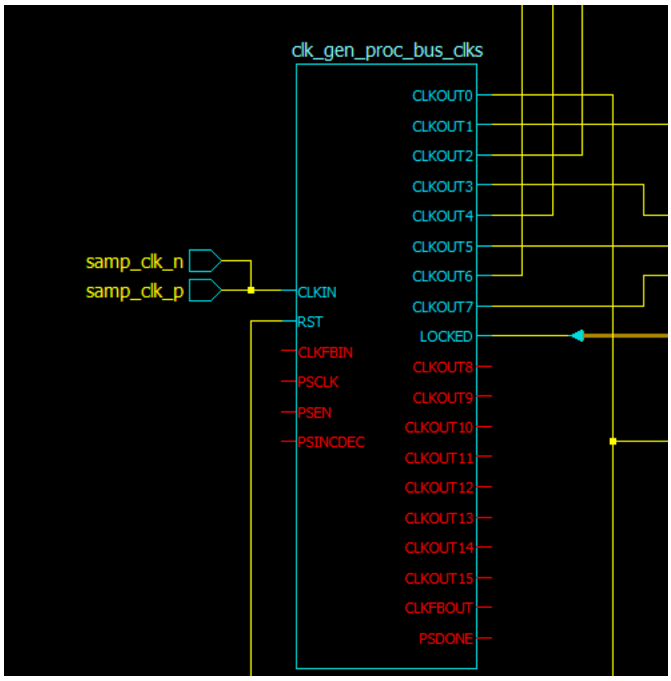


FIGURE B.4: Block instantiated for the generation of the necessary clock signals for all the possible channel bandwidth.

of the selector, only 2 clocks are selected as outputs: the reference clock (20 or 10 or 5 MHz) and the 90 degree phase shifted of the reference clock, respectively. For integrating and connecting all the new and modified IP Cores

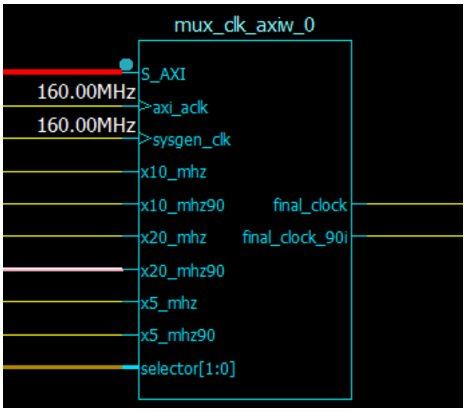


FIGURE B.5: clock_selector IP Core.

in the design, we used Xilinx Platform Studio. This tool allows to generate a part of the bitstream to load into FPGA. The generation takes almost one hour and half with a RAM of 16 GB.

As mentioned in the Appendix A, the whole system includes two 32-bit RISC microprocessor MicroBlaze. For this reason, we need two software applications described by two ELF (Executable and Linkable Format) files. An

ELF file, which is a product of the SDK, is a binary data file that contains an executable program image ready for running on an embedded processor. The ELF file contains the data to be mapped into the address ranges of the BRAMs. Indeed, we created some functions in order to change some parameters of some registers. Finally, we can merge the ELF files and the previous bitstream in order to create a new resulting bitstream file to load into FPGA.

Some final evaluations was made. ChipScope Pro tool helped us for controlling the proper behaviour of the signals in our implementation. For example, Figure B.6 highlights the latency to write on a register of the AD9963 chip, which fits with the technical requirements. Moreover, the final test was performed by iperf, a popular network tool that was developed for measuring TCP and UDP bandwidth performance, for evaluating the performance in terms of throughput.

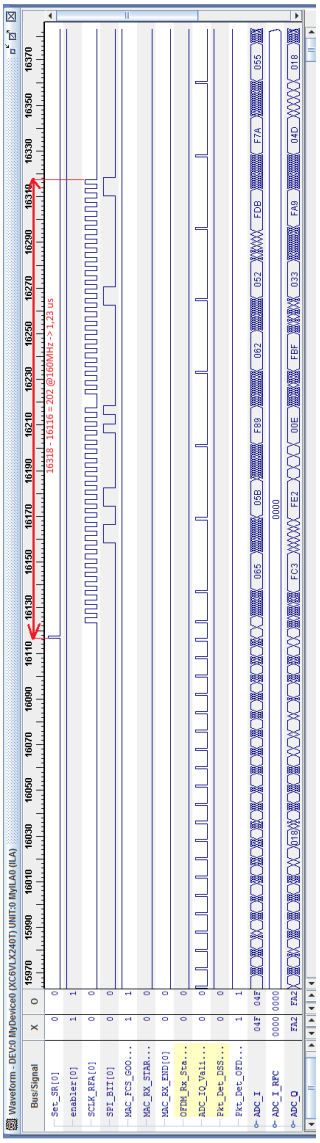


FIGURE B.6: ChipScope screenshot: latency for writing on a register of the AD9963.

B.2 Hopping Pilot Tones Implementation

At first, we decided to use GNU Radio, an open-source software development toolkit that provides signal processing blocks to implement software radios and it is used in order to support both wireless communications research and real world radio systems. Moreover, the GNU Radio Companion is a graphical UI used to develop GNU Radio applications. They provide some projects, including OFDM-based transmitter and receiver.

Unfortunately, we noticed that the implementation of the OFDM-based receiver was not performing enough. Indeed, for implementing the Hopping Pilot Tones system, we decided to write different scripts on MATLAB: (i) OFDM-based transmitter, (ii) jammers and (iii) OFDM-based receiver. In addition to the simulation, an important aspect is to test the system with a real wireless indoor channel. For this reason, we used the samples generated through MATLAB and the UHD driver in order to send the samples on the air.

The setup of all experiments includes two USRPs X310, as shown in Fig. B.7. The first one, acts both as transmitter and jammer: the transmitted samples are the result of the sum of the jammer samples and the data to be transmitted. Conversely, the second USRP acts as a receiver, recording traces. Then, the acquired traces are analyzed through MATLAB.

FIGURE B.7: Setup of all the Hopping Pilot Tones experiments.

B.3 Repeated Contention (ReCo) Implementation

For some evaluations of the ReCo mechanism we used WARPLab. WARPLab is a framework for rapid physical layer prototyping that allows for coordination of arbitrary combinations of single and multi-antenna transmit and receive nodes. The extensible framework gives users the flexibility to develop and deploy large arrays of nodes to meet any application or research need.

Conversely, for the implementation we used two of the tools adopted for the *Agile Receiver*: System Generator and ChipScope Pro. We created another flow in the receiver chain, shown in Fig. B.8, in addition to the one already present, in order to be able to receive tones transmitted from other stations and to perform the spectrum analysis. For maximizing the energy concentration in the main lobe, we multiply the received signal with a Kaiser window. Then, the spectrum analysis is made through an FFT. The real and imaginary part of the complex numbers are some of the FFT outputs. The detection algorithm analyzes the FFT result. More specifically, we performed the absolute value of the real and imaginary parts respectively. This result must be compared to a certain threshold value. Through WARPLab, we evaluated empirically the appropriate threshold (i.e. -35 dB).

The last change to make effective the new MAC mechanism was the implementation of various timers and a new simple state machine in addition to those already present, as shown in Figure B.9.

Finally, the ChipScope Pro tool was used for controlling the proper behaviour of some signals of interest, such as the FFT analysis and/or some values of certain registers.

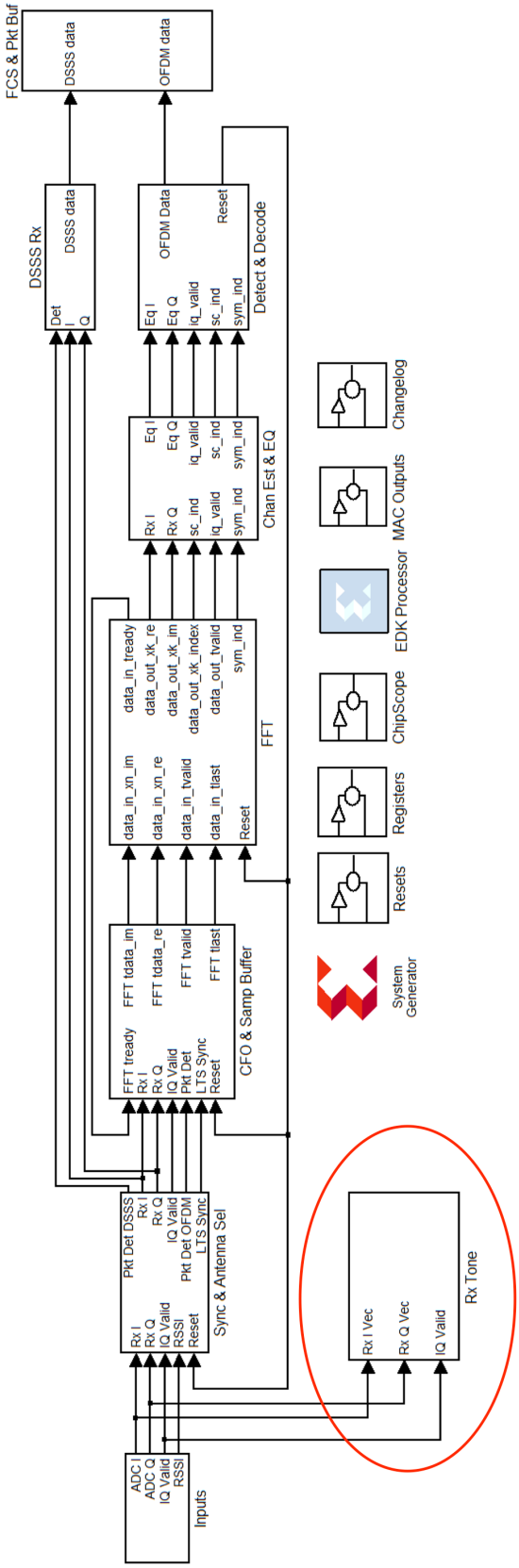


FIGURE B.8: Receiver chain of the ReCo implementation.

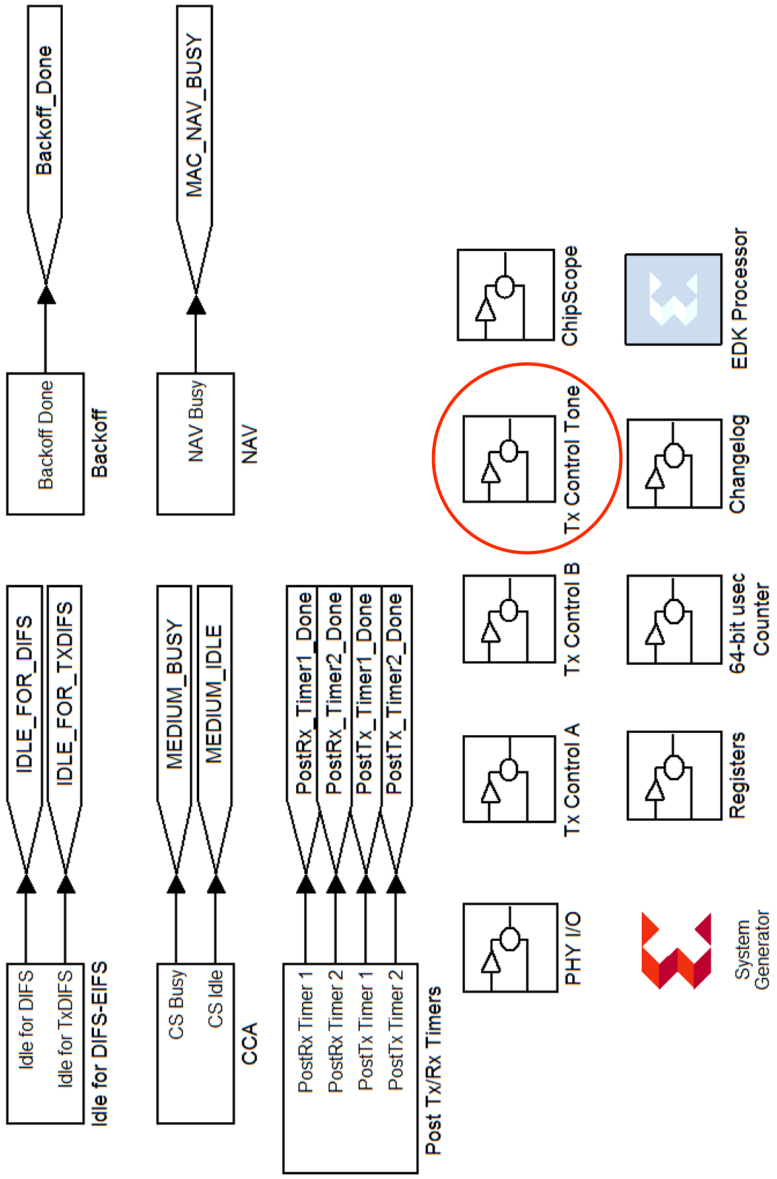


FIGURE B.9: MAC implementation of the ReCo mechanism.

Bibliography

[1] A. Polydros et al. "WIND-FLEX: de- veloping a novel testbed for exploring flexible radio concepts in an indoor environment". In: *IEEE Commun. Mag.* 41.7 (2003), pp. 116–122.

[2] A. J. Goldsmith and S.-G. Chua. "Variable-rate variable- power MQAM for fading channels". In: *IEEE Trans. Commun.* 45.10 (1997), pp. 1218–1230.

[3] T. Keller and L. Hanzo. "Adaptive modulation techniques for duplex OFDM transmission," in: *IEEE Trans. Veh. Technol.* 49.5 (2000), pp. 1893–1906.

[4] Wunder Gerhard et al. "5GNOW: Non-orthogonal, asynchronous waveforms for future mobile applications". In: *IEEE Commun. Mag.* 52.2 (2014), pp. 97–105.

[5] Joseph Mitola III. "The software radio". In: *IEEE National Telesystems Conference* (1992).

[6] J. R. Machado-Fernandez. "Software Defined Radio: Basic Principles and Applications". In: *Facultad de Ingeniería* 24.38 (2015), pp. 79–96.

[7] Eugene Grayver. "Implementing software defined radio". In: *Springer Science and Business Media* (2012).

[8] Bernard Sklar. *Digital communications*. Prentice Hall, 2001.

[9] K. VonEhr, W. Neuson, and B. E. Dunne. "Software Defined Radio: Choosing the Right System for Your Communications Course". In: *ASSE's 123rd Annual Conference and Exposition* (2016).

[10] Julien Herzen. "Flexible Spectrum Assignment for Local Wireless Networks". In: *Doctoral Thesis - École Polytechnique Fédérale de Lausanne* (2015).

[11] R. Chandra et al. "A Case for Adapting Channel Width in Wireless Networks". In: *SIGCOMM'08* (2008).

[12] A. Khattab et al. "WARP: A flexible platform for clean-slate wireless medium access protocol design". In: *ACM SIGMOBILE Mobile Computing and Communications Review* 12.1 (2008), pp. 56–58.

[13] V. Pejovic and E. M. Belding. "Whiterate: A context-aware approach to wireless rate adaptation". In: *IEEE Transactions on Mobile Computing* 13.4 (2014), pp. 921–934.

[14] M. Liechti, V. Lenders, and D. Giustiniano. "Jamming mitigation by randomized bandwidth hopping". In: *ACM CoNEXT 2015* (2015).

[15] P. Bahl et al. "White space networking with wi-fi like connectivity". In: *ACM SIGCOMM Computer Communication Review - SIGCOMM '09* 39.12 (2009), pp. 27–38.

[16] Michelle X Gong et al. "Channel bounding and MAC protection mechanisms for 802.11 ac". In: *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE. 2011, pp. 1–5.

[17] Won-Suk Kim and Sang-Hwa Chung. "Design and implementation of IEEE 802.11n in multi-hop over wireless mesh networks with multi-channel multi-interface". In: *High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (HPCC-ICESS), 2012 IEEE 14th International Conference on*. IEEE. 2012, pp. 707–713.

[18] Minyoung Park. "IEEE 802.11 ac: Dynamic bandwidth channel access". In: *Communications (ICC), 2011 IEEE International Conference on*. IEEE. 2011, pp. 1–5.

[19] Krishna Chintalapudi et al. "WiFi-NC: WiFi over narrow channels". In: *Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation*. USENIX Association. 2012, pp. 4–4.

[20] J. Fang et al. "Fine-Grained Channel Access in Wireless LAN". In: *IEEE/ACM Transactions on Networking*. Vol. 21. 3. 2013, pp. 772–787.

[21] Hariharan Rahul et al. "Learning to Share: Narrowband-friendly Wideband Networks". In: *Proceedings of the ACM SIGCOMM 2008 Conference on Data Communication*. SIGCOMM '08. Seattle, WA, USA: ACM, 2008, pp. 147–158. ISBN: 978-1-60558-175-0.

[22] L. Zheng et al. "Performance Analysis of Group-Synchronized DCF for Dense IEEE 802.11 Networks". In: *IEEE Transactions on Wireless Communications* 13.11 (2014), pp. 6180–6192. ISSN: 1536-1276. DOI: 10.1109/TWC.2014.2337315.

[23] V. Maglogiannis et al. "Impact of LTE Operating in Unlicensed Spectrum on Wi-Fi Using Real Equipment". In: *2016 IEEE Global Communications Conference (GLOBECOM)*. 2016, pp. 1–6. DOI: 10.1109/GLOCOM.2016.7841884.

[24] M. Heusse LSR-IMAG Lab. et al. "Performance Anomaly of 802.11b". In: *IEEE INFOCOM* (2003).

[25] C. Shahriar et al. "PHY-Layer Resiliency in OFDM Communications: A Tutorial". In: *IEEE Communications Surveys and Tutorials* 17.1 (2015), pp. 292–314.

[26] J. Grimes. "Commercial wireless metropolitan area network (WMAN) systems and technologies". In: *Memo* (2009), pp. 8–39.

[27] T. Schmidl and D. Cox. "Robust frequency and timing synchronization for OFDM". In: *IEEE Trans. Commun.* 45.12 (1997), pp. 1613–1621.

[28] M. Ozdemir and H. Arslan. "Channel estimation for wireless OFDM systems". In: *IEEE Commun. Surveys Tuts.* 9.2 (2007), pp. 18–48.

[29] R. Negi and J. Cioffi. "Pilot tone selection for channel estimation in a mobile OFDM system". In: *IEEE Transactions on Consumer Electronics* 44.3 (1998).

[30] T. C. Clancy. "Efficient OFDM denial: Pilot jamming and pilot nulling". In: *IEEE Int. Conf. Commun.* (2011), pp. 1–5.

[31] J. Luo, J. Andrian, and C. Zhou. "Bit error rate analysis of jamming for OFDM systems". In: *WTS* (2007), pp. 1–8.

[32] R. Poisel. "Jamming Techniques". In: *Modern communications jamming: principles and techniques 2nd Ed. Norwood, Artech House* (2011), pp. 467–511.

[33] J. Park et al. "Effect of partial band jamming on OFDM-based WLAN in 802.11g". In: *IEEE Int. Conf. Acoust.* 4 (2003), pp. 560–563.

[34] D. W. Chi and P. Das. "Effects of nonlinear amplifier and partial band jammer in OFDM with application to 802.11n WLAN". In: *IEEE Mil. Commun. Conf.* (2007), pp. 1–8.

[35] L. Lightfoot, L. Zhang, and T. Li. "Performance of QO-STBC-OFDM in Partial-Band Noise Jamming". In: *Information Sciences and Systems* (2010), pp. 1–6.

[36] M. K. Ozdemir and H. Arslan. "Channel Estimation for Wireless OFDM Systems". In: *IEEE Communications Surveys and Tutorials* 9.2 (2007), pp. 18–48.

[37] P. Fertl and G. Matz. "Channel Estimation in Wireless OFDM Systems With Irregular Pilot Distribution". In: *IEEE Trans. Signal Processing* 58.6 (2010), pp. 3180–3194.

[38] C. Patel, G. Stuber, and T. Pratt. "Analysis of OFDM/MC-CDMA under imperfect channel estimation and jamming". In: *IEEE Wireless Communications and Networking Conference (WCNC)* (2004).

[39] F. Guo and W. Chenggui. "A jamming scheme based on pilot assisted channel estimation of OFDM". In: *Journal of Electronic Warfare Technology* 23 (2008).

[40] C. Shahriar, T. Clancy, and R. McGwier. "Equalization Attacks against OFDM: Analysis and Countermeasures". In: *Wiley Wireless Communications and Mobile Computing* 16.13 (2016), pp. 1809–1825.

[41] J. A. Mahal and T. C. Clancy. "The BER analysis of OFDMA and SC-FDMA under pilot-assisted channel estimation and pilot jamming in rayleigh slow-fading channel". In: *Wireless Communications and Mobile Computing* 16.15 (2016), pp. 2315–2328.

[42] C. Shahriar and T. C. Clancy. "Performance impact of pilot tone randomization to mitigate OFDM jamming attacks". In: *IEEE CCNC* (2013), pp. 813–816.

[43] C. Mueller-Smith and W. Trappe. "Efficient OFDM denial in the absence of channel information". In: *IEEE Military Communications Conference* (2013), pp. 89–94.

[44] M. Han et al. "OFDM channel estimation with jammed pilot detector under narrow-band jamming". In: *IEEE Trans. Veh. Technol.* 57 (2008), pp. 1934–1939.

[45] S. Sodagari and T. C. Clancy. "Efficient jamming attack on MIMO channels". In: *IEEE ICC* (2012), pp. 852–856.

[46] C. Shahriar, S. Sodagari, and T. C. Clancy. "Performance of pilot jamming on MIMO channels with imperfect synchronization". In: *IEEE International Conference on Communications (ICC)* (2012), pp. 898–902.

[47] A. Bayesteh, M. Ansari, and A. K. Khandani. "Effect of jamming on the capacity of MIMO channels". In: (2004).

[48] Q.Liu, M.Li, and and N.Zhao X.Kong. "Disrupting MIMO communications with optimal jamming signal design". In: *IEEE Transactions on Wireless Communications* 14.10 (2015), pp. 5313–5325.

[49] M. Han et al. "An efficient channel estimation algorithm under narrowband jamming for OFDM systems". In: *IEEE Military Communications Conference* (2006), pp. 1–6.

[50] X. Lei et al. "Multipath Delay Estimation by Jammed Pilot in OFDM System". In: *Applied Mathematics and Information Sciences* 6.3 (2012), pp. 639–647.

[51] Richard A. Poisel. "Modern communications jamming principles and techniques". In: *Artech House Publishers* (2004).

[52] David L. Adamy. "EW 102: A Second Course in Electronic Warfare". In: *Artech House* (2004).

[53] Dinesh Bharadia, Emily McMilin, and Sachin Katti. "Full Duplex Radios". In: *SIGCOMM Comput. Commun. Rev.* 43.4 (2013), pp. 375–386.

[54] M. Wilhelm et al. "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" In: *Proceedings ACM Conference on Wireless Network Security (WiSec)* (2011), pp. 47–52.

[55] M. K. Simon et al. "Spread Spectrum Communications Handbook". In: *McGraw-Hill* (2002).

[56] C. Poepper, M. Strasser, and S. Capkun. "Anti-jamming broadcast communication using uncoordinated spread spectrum techniques". In: *IEEE Journal on Selected Areas in Communications* 28.5 (2010), pp. 703–715.

[57] E. Sourour, H. El-Ghoroury, and D. McNeil. "Frequency offset estimation and correction in the IEEE 802.11a WLAN". In: *IEEE Vehicular. Technology Conference* (2004), pp. 4923–4927.

[58] V. Jones and H. Sampath. "Emerging technologies for WLAN". In: *IEEE Communications Magazine* 53.3 (2015), pp. 141–149.

[59] Boris Bellalta et al. "Next generation IEEE 802.11 Wireless Local Area Networks: Current status, future directions and open challenges ". In: *Comp. Comm.* 75 (2016), pp. 1 –25.

[60] Dongkyu Kim, Haesoon Lee, and Daesik Hong. "A Survey of In-Band Full-Duplex Transmission: From the Perspective of PHY and MAC Layers". In: *IEEE Comm. Surveys & Tutorials* 17.4 (2015), pp. 2017–2046.

[61] Minkeun Chung et al. "Prototyping real-time full duplex radios". In: *IEEE Communications Magazine* 53.9 (2015), pp. 56–63.

[62] K.M. Thilina et al. "Medium access control design for full duplex wireless systems: challenges and approaches". In: *IEEE Comm. Mag.* 53.5 (2015), pp. 112–120.

[63] L. Song et al. "Cross-Layer Protocol Design for CSMA/CD in Full-Duplex WiFi Networks". In: *IEEE Communications Letters* 20.4 (2016), pp. 792–795.

[64] A. Mutairi and S. Roy. "An OFDM-Aware Reservation Random Access Protocol for Interference Mitigation in OFDMA Femtocells". In: *IEEE Transactions on Communications* 63.1 (2015), pp. 301–310.

[65] Souvik Sen, Romit Roy Choudhury, and Srihari Nelakuditi. "No Time to Countdown: Migrating Backoff to the Frequency Domain". In: *Proc. of ACM MOBICOM'11*. Las Vegas, Nevada, USA, 2011, pp. 241–252.

[66] L. Jiang and J. Walrand. "A Distributed CSMA Algorithm for Throughput and Utility Maximization in Wireless Networks". In: *IEEE/ACM Transactions on Networking* 18.3 (2010), pp. 960–972.

[67] Ilenia Tinnirello et al. "Wireless MAC processors: programming MAC protocols on commodity hardware". In: *INFOCOM, 2012 Proceedings IEEE*. IEEE. 2012, pp. 1269–1277.

[68] J. Lee et al. "Making 802.11 DCF Near-Optimal: Design, Implementation, and Evaluation". In: *IEEE/ACM Trans. on Networking* 24.3 (2016), pp. 1745–1758.

[69] J. Liu et al. "Towards Utility-optimal Random Access Without Message Passing". In: *Wirel. Commun. Mob. Comput.* 10.1 (2010), pp. 115–128.

[70] Martin Heusse et al. "Idle Sense: An Optimal Access Method for High Throughput and Fairness in Rate Diverse Wireless LANs". In: *SIGCOMM Comput. Commun. Rev.* 35.4 (2005), pp. 121–132.

[71] W. H. Wan Hassan et al. "WLAN Fairness with Idle Sense". In: *IEEE Communications Letters* 19.10 (2015), pp. 1794–1797.

[72] W. Zame, J. Xu, and M. van der Schaar. "Winning the Lottery: Learning Perfect Coordination With Minimal Feedback". In: *IEEE Journal of Selected Topics in Signal Processing* 7.5 (2013), pp. 846–857.

[73] Z. Abichar and J.M. Chang. "A Medium Access Control Scheme for Wireless LANs with Constant-Time Contention". In: *IEEE Transactions on Mobile Computing* 10.2 (2011), pp. 191–204.

[74] Mahanth Gowda et al. "Backing out of Linear Backoff in Wireless Networks". In: *Proceedings of the 1st ACM Workshop on Hot Topics in Wireless*. HotWireless '14. Maui, Hawaii, USA: ACM, 2014, pp. 7–12.

[75] Y. Mao and L. Shen. "A first-round-bye based priority scheme for WLANs with two access categories". In: *2015 Int. Conf. on Wireless Communications Signal Processing (WCSP)*. 2015, pp. 1–5.

[76] B. Zhou, A. Marshall, and T. H. Lee. "A k-Round Elimination Contention Scheme for WLANs". In: *IEEE Transactions on Mobile Computing* 6.11 (2007), pp. 1230–1244.

[77] Xiaojun Feng et al. "Use your frequency wisely: Explore frequency domain for channel contention and ACK". In: *INFOCOM, 2012 Proceedings IEEE*. 2012, pp. 549–557.

[78] Y. Zhang et al. "Multi-Channel Medium Access without Control Channels: A Full Duplex MAC Design". In: *IEEE Transactions on Mobile Computing* 16.4 (2017), pp. 1032–1046.

[79] Seyed K. Fayaz, Fatima Zarinni, and Samir Das. "Ez-Channel: A distributed {MAC} protocol for efficient channelization in wireless networks ". In: *Ad Hoc Networks* 31 (2015), pp. 34 –44.

[80] E. Magistretti, O. Gurewitz, and E.W. Knightly. "802.11ec: Collision Avoidance Without Control Messages". In: *IEEE/ACM Transactions on Networking* 22.6 (2014), pp. 1845–1858.

[81] Kun Tan et al. "Fine-grained Channel Access in Wireless LAN". In: *SIGCOMM Comput. Commun. Rev.* 40.4 (Aug. 2010), pp. 147–158.

[82] D. Betsekas and R. Gallager. *Data networks*. 2nd Ed., Prentice Hall, Englewood Cliffs, NJ, 1992.

[83] A. Baiocchi et al. "Random Access with Repeated Contentions for Emerging Wireless Technologies". In: *IEEE INFOCOM 2017*. Atlanta, GA, USA, 2017, pp. 1–9.

[84] G. Bianchi. "Performance analysis of the IEEE 802.11 distributed coordination function". In: *IEEE Journal on Selected Areas in Communications* 18.3 (2000), pp. 535–547.

[85] A. Kumar et al. "New Insights From a Fixed-Point Analysis of Single Cell IEEE 802.11 WLANs". In: *IEEE/ACM Trans. on Networking* 15.3 (2007), pp. 588–601.

[86] Souvik Sen, Romit Roy Choudhury, and Srihari Nelakuditi. "Listen (on the Frequency Domain) Before You Talk". In: *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*. Hotnets-IX. Monterey, California: ACM, 2010, 16:1–16:6. ISBN: 978-1-4503-0409-2.

[87] J. G. Andrews et al. "Are we approaching the fundamental limits of wireless network densification?" In: *IEEE Communications Magazine* 54.10 (2016), pp. 184–190.