Perspectives of Jamming, Mitigation and Pattern Adaptation of OFDM Pilot Signals for the Evolution of Wireless Networks

Raghunandan M. Rao

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Electrical Engineering

Jeffrey H. Reed, Chair
Vuk Marojevic
Michael R. Buehrer

September 15, 2016
Blacksburg, Virginia

Keywords: Multi-tone Pilot Jamming, Mitigation, OFDM systems, Long-Term Evolution (LTE)/LTE Cell-Specific Reference Signal (CRS) Jamming, Channel Quality Indicator (CQI) Spoofing, Pilot Pattern Adaptation

Perspectives of Jamming, Mitigation and Pattern Adaptation of OFDM Pilot Signals for the Evolution of Wireless Networks

Raghunandan M. Rao

(ABSTRACT)

Wireless communication networks have evolved continuously over the last four decades in order to meet the traffic and security requirements due to the ever-increasing amount of traffic. However this increase is projected to be massive for the fifth generation of wireless networks (5G), with a targeted capacity enhancement of $1000\times$ w.r.t. 4G networks. This enhanced capacity is possible by a combination of major approaches (a) overhaul of some parts and (b) elimination of overhead and redundancies of the current 4G. In this work we focus on OFDM reference signal or pilot tones, which are used for channel estimation, link adaptation and other crucial functions in Long-Term Evolution (LTE). We investigate two aspects of pilot signals pertaining to its evolution - (a) impact of targeted interference on pilots and its mitigation and (b) adaptation of pilot patterns to match the channel conditions of the user.

We develop theoretical models that accurately quantify the performance degradation at the user's receiver in the presence of a multi-tone pilot jammer. We develop and evaluate mitigation algorithms to mitigate *power-constrained multi-tone pilot jammers* in SISO- and full rank spatial-multiplexing MIMO-OFDM systems. Our results show that the channel estimation performance can be restored even in the presence of a strong pilot jammer. We also show that full rank spatial multiplexing in the presence of a synchronized pilot jammer (transmitting on pilot locations only) is possible when the channel is flat between two pilot locations in either time or frequency.

We also present experimental results of multi-tone broadcast pilot jamming (Jamming of Cell-Specific Reference Signal) in the LTE downlink. Our results show that full-band jamming of pilots needs $5\,\mathrm{dB}$ less power than jamming the entire downlink signal, in order to cause Denial of Service (DoS) to the users. In addition to this, we have identified and demonstrated a previously unreported issue with LTE termed 'Channel Quality Indicator (CQI) Spoofing'. In this scenario, the attacker tricks the user terminal into thinking that the channel quality is good, by transmitting interference transmission only on the data locations, while deliberately avoiding the pilots. This jamming strategy leverages the dependence of the adaptive modulation and coding (AMC) schemes on the CQI estimate in LTE.

Lastly, we investigate the idea of pilot pattern adaptation for SISO- and spatial multiplexing MIMO-OFDM systems. We present a generic heuristic algorithm to predict the optimal pilot spacing and power in a nonstationary doubly selective channel (channel fading in both time and frequency). The algorithm fits estimated channel statistics to stored codebook channel profiles and uses it to maximize the upper bound on the constrained capacity. We demonstrate up to a 30% improvement in ergodic capacity using our algorithm and describe ways to minimize feedback requirements while adapting pilot patterns in multi-band carrier aggregation systems. We conclude this work by identifying scenarios where pilot adaptation can be implemented in current wireless networks and provide some guidelines to adapt pilots for 5G.

Perspectives of Jamming, Mitigation and Pattern Adaptation of OFDM Pilot Signals for the Evolution of Wireless Networks

Raghunandan M. Rao

(GENERAL AUDIENCE ABSTRACT)

Wireless communications have evolved continuously over the last four decades in order to meet the ever-increasing number of users. The next generation of wireless networks, named 5G, is expected to interconnect a massive number of devices called the Internet of Things (IoT). Compared to the current generation of wireless networks (termed 4G), 5G is expected to provide a thousand-fold increase in data rates. In addition to this, the security of these connected devices is also a challenging issue that needs to be addressed. Hence in the event of an attack, even if a tiny fraction of the total number of users are affected, this will still result in a large number of users who are impacted.

The central theme of this thesis is the evolution of *Orthogonal Frequency Division Multiplexing (OFDM) pilot signals* on the road from 4G to 5G wireless networks. In OFDM, pilot signals are sent in parallel to data in order to aid the receiver in mitigating the impairments of the wireless channel. In this thesis, we look at two perspectives of the evolution of pilots: a) targeted interference on pilot signals, termed as 'Multi-tone pilot jamming' and b) adapting pilot patterns to optimize throughput.

In the first part of the thesis, we investigate the (a) impact of multi-tone pilot jamming and (b) propose and evaluate strategies to counter multi-tone pilot jamming. In particular, we propose methods that (a) have the potential to be implemented in the Third Generation Partnership Project Long-Term Evolution (3GPP LTE) standard, and (b) have the ability to maintain high data rates with a multi-antenna receiver, in the presence of a multi-tone pilot jammer. We also experiment and analyze the behavior of LTE in the presence of such targeted interference.

In the second half of the thesis, we explore the idea of adapting the density of pilots to optimize throughput. Increasing the pilot density improves the signal reception capabilities, but reduces the resources available for data and hence, data rate. Hence we propose and evaluate strategies to balance between these two conflicting requirements in a wireless communication system.

In summary, this thesis provides and evaluates ideas to mitigate interference on pilot signals, and design data rate-maximizing pilot patterns for future OFDM-based wireless networks.

Acknowledgements

I am indebted to a lot of people for helping me successfully jumpstart my career in the area of Wireless Communications. Firstly, I would like to thank my mentors Dr. Jeffrey H. Reed and Dr. Vuk Marojevic for giving me the opportunity, resources and the intellectual freedom to pursue interesting ideas. I am deeply honored to work with prolific researchers such as yourself, and your expert guidance in the right direction has enabled me to focus on concrete research problems, and helped me to formulate practical solutions in a timely manner.

I would also like to thank Dr. Michael R. Buehrer for serving on my thesis committee, and for his helpful technical inputs. His course on 'Multichannel Communications' solidified my concepts related to MIMO-OFDM, without which this thesis would have been difficult to accomplish.

I especially owe my gratitude to Dr. Harpreet Dhillon for motivating me during my first year of graduate study at Virginia Tech. His course on 'Advanced Digital Communications' introduced me to the exciting area of Communications, and led me to pursue research in Wireless Communications.

I would also like to thank the Institute of Critical Technology and Applied Science (ICTAS), Virginia Tech Foundation, Office of the Secretary of Defense (OSD), MS Technologies and Oceus Networks for funding my research and your support and cooperation.

To Dr. Eyosias Yoseph Imana: thanks for closely supervising my semester project in the course on 'Cellular Radios', which formed the basis for this thesis. It was a great time working with you during the Wireless@VT Symposium 2015. I learnt a lot from this single experience alone.

To Deven: I'm glad we got to work together the most during this year. It was a lot of fun working with you while preparing and presenting demos for visitors. You have been a great friend outside work, and I will always cherish the times I spent with you.

To Randall: You have been the most pleasant person I've ever worked with. Your knowledge on RF and Microwave measurements has helped me a great deal while working on the experimental part of my thesis. To my colleagues Abid, Aditya, Kaleb, Marc, Matt, Miao, Mina, Munnawar, Sean, Tad and Xiaofu: you guys are awesome! It has been an enriching experience being a part of this group, bouncing ideas off of you guys and getting useful feedback. I hope to build more collaborations with you guys in the future. Marc, Mina and Munnawar, it has been a pleasure collaborating with you on LTE jamming and spectrum sharing research. I would also like to thank

Sai Nisanth, Surabhi and Shankar for all your support and companionship.

To Hilda, Nancy and Joyce: thank you for constantly helping me navigate the logistics of grad school.

I would also like to thank my current and former roommates: Abhishek, Prakhar, Abdus, Ajai and Steve for all the camaraderie. Grad school would have been very difficult without the support of you guys.

To my dear Swati: this transition would've been very stressful without you. Your never-ending optimism and constant moral support has helped me remain strong during tough times. You have spread cheer everyday over these last two years. Thank you for everything.

To my beloved grandparents: you gave me the most beautiful childhood I could have ever wanted. Your absence will leave a void in my heart forever. I'll always remember you through your love for the family, and the things you've taught me.

To my uncles Gururaj, Vasudev and Venkatesh: your constant moral support and fatherly advice has always helped me believe in myself. I am blessed to have elders like you as a part of my family.

I am indebted to my parents and sister: I have missed home a lot, but am grateful for being just a phone call away. None of what I've accomplished would've been possible without your unconditional love and unquestioning support. You are, and always will be the pillars of my strength. Words aren't enough to thank you for the life you've provided me with.

To my Family

Contents

List of Figures xii

List of Tables xv

1 Introduction 1

1.1 Evolution of Wireless Networks . . . 1

1.2 Vulnerabilities of Wireless Networks . . . 2

1.3 Focus and Contributions of this Thesis . . . 3

1.3.1 Contributions . . . 3

1.4 Organization of this Thesis . . . 4

2 Theoretical Analysis of Multi-Tone Pilot Jamming in OFDM 6

2.1 Background . . . 6

2.2 Channel Model . . . 7

2.3 Channel Estimation . . . 9

2.4 Mean Square Error (MSE) Analysis . . . 12

2.4.1 Mean Square Error in the Absence of a Jammer . . . 13

2.4.2 Mean Square Error in the Presence of a Synchronous Multi-Tone Pilot Jammer . . . 16

2.4.3 Numerical Results . . . 19

2.5 Bit Error Rate Analysis . . . 19

2.5.1 BER in the Presence of a Synchronous Multi-Tone Pilot Jammer . . . 22

2.5.2 BER in the Absence of a Multi-Tone Pilot Jammer . . . 24
2.5.3 Numerical Results . . . 24
2.6 Conclusions . . . 27

3 Mitigation of Multi-Tone Pilot Jamming in SISO and MIMO-OFDM 28
3.1 Background . . . 28
3.2 Types of Multi-Tone Pilot Jammers . . . 29
3.3 Detection of Pilot Jamming . . . 30
3.4 Anti-Jamming for SISO-OFDM Systems . . . 31
3.4.1 Resource Element Blanking with Interference Cancellation . . . 31
3.4.2 Cyclic Frequency Shifting of Pilot Locations . . . 33
3.4.3 Numerical Results . . . 33
3.5 Spatial Multiplexing with MIMO-OFDM in the Presence of Multi-Tone Pilot Jamming . . . 35
3.5.1 Motivation . . . 35
3.5.2 Channel Equalization in MIMO-OFDM . . . 39
3.5.3 Multi-Tone Pilot Jamming Model for MIMO-OFDM . . . 42
3.5.4 Constant Channel Approximation (COCHAP) with Jammer Cancellation . 44
3.5.5 Numerical Results . . . 47
3.6 Conclusions . . . 52

4 Jamming of LTE's Cell-Specific Reference Signal (CRS) 53
4.1 Background . . . 53
4.2 The LTE Downlink . . . 54
4.3 Channel Quality and Adaptive Modulation and Coding . . . 56
4.4 Impact of CRS Jamming on the Performance of LTE . . . 56
4.4.1 Experimental Setup . . . 57
4.4.2 Throughput Measurement Results . . . 60
4.5 Conclusions . . . 64

5 Adaptation of Pilot Patterns for OFDM Systems **65**

5.1 Introduction . . . 65

5.2 Adaptation of Pilot Spacing and Power . . . 66

5.2.1 Problem Formulation . . . 67

5.2.2 Estimation of Channel Statistics . . . 71

5.2.3 Channel Statistics Codebook . . . 71

5.2.4 Optimal Pilot Spacing and Power . . . 72

5.2.5 Complexity . . . 73

5.3 Numerical Results . . . 73

5.4 Some Practical Considerations for Pilot Adaptation in Current and Future Wireless Networks . . . 81

5.5 Conclusions . . . 82

6 Conclusions and Future Work **83**

6.1 Thesis Summary and Conclusions . . . 83

6.2 Future Work . . . 84

6.2.1 Enhanced Mitigation Algorithms for Pilot Jamming . . . 84

6.2.2 Improving Resilience of LTE . . . 84

6.2.3 Cross-layer Optimization in Interference Channels . . . 85

6.2.4 Trust-Aware Protocol Design . . . 85

6.2.5 Pilot Pattern Adaptation . . . 85

A Additional Throughput Measurement Results **86**

Bibliography **88**

List of Abbreviations

3GPP	Third generation partnership project
AMC	Adaptive modulation and coding
BER	Bit error rate
BLER	Block error rate
CA	Carrier aggregation
CDF	Cumulative distribution function
COCHAP	Constant channel approximation
CoMP	Cooperative Multipoint
CQI	Channel quality indicator
CRS	Cell-specific reference signal
DoS	Denial of service
eNB	Evolved node B
FBMC	Filter-bank multicarrier
FDD	Frequency division duplex
FTN	Faster than Nyquist
HARQ	Hybrid automatic repeat request
ICI	Inter-carrier interference
ITU-T	International Telecommunication Union - Telecommunication standardization sector
JC	Jammer cancellation
JSR	Jammer to signal ratio
LDPC	Low density parity check
LS	Least squares
LTE/LTE-A	Long-term evolution/LTE advanced
MCS	Modulation and coding scheme
MIMO	Multiple input multiple output
MMSE	Minimum mean squared error
MSE	Mean square error
OFDM	Orthogonal frequency division multiplexing
PCFICH	Physical control format indicator channel
PCI	Physical Cell Identity
PDSCH	Physical downlink shared channel
PHY	Physical layer

PRACH	Physical random access channel
PSS	Primary synchronization signal
PUCCH	Physical uplink control channel
QAM	Quadrature amplitude modulation
QPSK	Quadrature phase shift keying
RB	Resource Block
RE	Resource element
RF	Radio frequency
S(I)NR	Signal to (interference and) noise ratio
SISO	Single input single output
SSS	Secondary synchronization signal
TDD	Time division duplex
TTI	Transmission time interval
UFMC	Universal filtered multicarrier
UAV	Unmanned aerial vehicle
UE	User equipment
ZF	Zero forcing

List of Figures

2.1 Mean Square Error analysis region for diamond-shaped pilot arrangement in OFDM. 10

2.2 Illustration of a Synchronous multi-tone pilot jammer. 18

2.3 Theoretical and simulated channel estimation Mean Square Error for $f_d = 100\,\text{Hz}$, $\tau_{rms} = 200\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer. 20

2.4 Theoretical and simulated channel estimation Mean Square Error for $f_d = 200\,\text{Hz}$, $\tau_{rms} = 400\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer. 20

2.5 Theoretical and simulated channel estimation Mean Square Error for $f_d = 500\,\text{Hz}$, $\tau_{rms} = 900\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer. 21

2.6 Analysis Region for BER derivations in the presence and absence of a multi-tone pilot jammer. 21

2.7 Theoretical and simulated BER performance of QPSK-OFDM for $f_d = 100\,\text{Hz}$, $\tau_{rms} = 200\,\text{ns}$,in the case of a synchronous pulsed multi-tone pilot jammer. 25

2.8 Theoretical and simulated BER performance of QPSK-OFDM for $f_d = 200\,\text{Hz}$, $\tau_{rms} = 400\,\text{ns}$,in the case of a synchronous pulsed multi-tone pilot jammer. 25

2.9 Theoretical and simulated BER performance of QPSK-OFDM for $f_d = 500\,\text{Hz}$, $\tau_{rms} = 900\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer. 26

3.1 Mitigation of asynchronous multi-tone pilot jamming by resource element blanking with interference cancellation. 32

3.2 Mitigation of synchronous multi-tone pilot jamming by cyclic frequency shifting of pilot locations. 32

3.3 Channel Estimation MSE performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$. 36

3.4 Channel Estimation MSE performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 400\,\text{ns}$, $f_d = 200\,\text{Hz}$. 36

3.5 Channel Estimation MSE performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 900\,\text{ns}$, $f_d = 500\,\text{Hz}$. 37

3.6 Bit Error rate performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$. 37

3.7 Bit Error rate performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 400\,\text{ns}$, $f_d = 200\,\text{Hz}$. 38

3.8 Bit Error rate performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 900\,\text{ns}$, $f_d = 500\,\text{Hz}$. 38

3.9 Diamond-shaped pilot pattern for 4×4 MIMO-OFDM. 41

3.10 Illustration of synchronous multi-tone pilot jamming in a 4×4 MIMO-OFDM block, for all spatial layers. 43

3.11 Schematic of the Constant Channel Approximation (COCHAP) assumption for pilots from transmit antenna 1 for $j = 1, 2, 3, 4$. 43

3.12 Comparison of Ergodic sum capacity for all scenarios, for $\tau_{rms} = 100\,\text{ns}$, $f_d = 50\,\text{Hz}$. 49

3.13 Comparison of Ergodic sum capacity for all scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$. 49

3.14 Comparison of Ergodic sum capacity for all scenarios, for $\tau_{rms} = 400\,\text{ns}$, $f_d = 200\,\text{Hz}$. 50

3.15 Comparison of Bit Error Rate for all scenarios, for $\tau_{rms} = 100\,\text{ns}$, $f_d = 50\,\text{Hz}$. . . . 50

3.16 Comparison of Bit Error Rate for all scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$. . . 51

3.17 Comparison of Bit Error Rate for all scenarios, for $\tau_{rms} = 400\,\text{ns}$, $f_d = 200\,\text{Hz}$. . . 51

4.1 A 1.4 MHz FDD-LTE downlink frame normal cyclic prefix, corresponding to antenna port 0 of the eNodeB. 54

4.2 Schematic of the experimental setup for throughput measurements of the LTE Downlink. 59

4.3 Schematic of the jamming strategies investigated for throughput performance of the LTE downlink. The number of REs affected are the same in CRS and data subcarrier jamming. 60

4.4 Measured throughput versus JSR per Resource Block for all considered jamming schemes. 61

4.5 Comparison of maximum theoretically achievable ($R_{max,MCS}$), and measured average ($\bar{R}_{meas}$) throughput values versus JSR per Resource Block, for (a) CRS jamming, (b) data subcarrier jamming (1 out of 3 data subcarriers above/below CRS frequencies), and (c) barrage jamming. 63

4.6 Comparison of achievable throughput efficiency ($\eta_{ach,th}$) for all considered cases. . 63

5.1 Illustration of pilot adaptation based on varying channel conditions. 68

5.2 Scenario of channel statistics variation for all cases. 76

5.3 Ergodic Capacity Performance in SISO-OFDM for all considered pilot configurations. 77

5.4 The CDF of Capacity for pilot adaptation versus LTE spacing, $\rho = -3\,\mathrm{dB}$ for SISO-OFDM. 77

5.5 Capacity gain of pilot adaptation versus the other considered fixed pilot configurations for SISO-OFDM. 78

5.6 Ergodic Capacity Performance in MIMO-OFDM for all considered pilot configurations. 78

5.7 The CDF of capacity for pilot adaptation versus LTE spacing, $\rho = -3\,\mathrm{dB}$ for MIMO-OFDM. 79

5.8 Capacity gain of pilot adaptation versus the other considered fixed pilot configurations for MIMO-OFDM. 79

List of Tables

2.1 Description of the most important parameters 8

2.2 Simulation Parameters 18

2.3 Relationship between JSR (dB) and ρ. 26

3.1 Important Symbols and Notation 40

4.1 Mapping from CQI to spectral efficiency for 3GPP LTE Release 8. Adapted from [1]. 57

4.2 Mapping from MCS to Maximum Throughput of Physical Downlink Shared Channel (PDSCH) for a FDD SISO 10MHz LTE Release 8 Downlink. Adapted from [2]. 58

4.3 Parameters of the LTE Downlink Throughput measurement setup. 59

5.1 Description of the most important parameters 69

5.2 Codebook of Channel Profiles, $\mathcal{R}_C$ 74

5.3 Capacity gains of pilot adaptation w.r.t. fixed pilot configurations: comparison against state of the art 81

A.1 Summary of statistics of measured throughput in the LTE jamming experiments. . . 87

Chapter 1

Introduction

1.1 Evolution of Wireless Networks

Wireless networks have evolved over the last four decades, from the first generation (1G) analog standards in the 1980s to the current digital fourth generation (4G) networks which saw worldwide deployment over the last couple of years. In each generation, there has been major upgrades over its predecessors in terms of coverage, speed, services etc. We are currently on the brink of the standardization of fifth generation (5G) wireless networks that are expected to provide $1000\times$ capacity w.r.t. 4G networks, along with other performance enhancements such as ultra-low latency; and interconnecting a massive number of devices to the Internet, called the Internet of Things (IoT).

The Third Generation Partnership Project (3GPP) has standardized the Long-Term Evolution (LTE) from Release 8 in 2009 to Release 13 in 2016 [3]. The next version (Release 14) is scheduled for completion by 2017. There have been addition of new features in the latest two releases of LTE compared to the initial releases. Some of the important features introduced in these are support for higher order modulation schemes (256QAM), higher number of spatial layers (up to 8×8 MIMO), throughput enhancements using Carrier Aggregation (CA), cell-edge coverage enhancements using Cooperative Multi-point (CoMP) etc. The wireless evolution from 4G to 5G is expected to happen through a combination of the following approaches: (a) major system overhaul of some aspects of 4G and (b) elimination of redundancies, and upgrades to LTE. Some of the promising technologies actively researched for 5G wireless networks are:

(a) Millimeter-wave (mmWave) communications [4],

(b) Massive MIMO [4],

(c) Alternatives to OFDM: Filter-bank Multicarrier (FBMC), Universal Filtered Multicarrier (UFMC), Faster than Nyquist (FTN) etc. [5],

(d) Machine-Type Communications (MTC), and many more.

Broadly, the recurrent theme in several 5G proposals is *support for parameter adaptation* in the system, be it subcarrier spacing, cyclic prefix, pulse shape or others [6]. This is meant to optimize the system performance based on the operating conditions of the network like channel statistics, traffic patterns.

Pilot signals have traditionally been designed to have a fixed pattern in order to avoid complexity. But they represent an essential overhead in the system since they do not carry data symbols. Because of the heterogeneity of the user mobilities and channel characteristics in a practical scenario, dense pilot patterns become an unnecessary overhead if the channel remains flat enough in time or frequency. In this regard, this thesis explores the idea of adaptation of downlink pilot pattern in order to maximize the capacity of the system based on feedback of channel statistics from the user to the base station.

In addition to performance enhancements, superior levels of reliability and security is also necessary since in 5G networks it is expected to support critical infrastructure, in addition to civilian and military user traffic.

1.2 Vulnerabilities of Wireless Networks

Security and privacy has always been an evolving problem in the area of wireless communications since the days of the analog 1G cellular network. Each cellular generation has undergone its share of research and development related to wireless network attacks and countermeasures because each new feature introduced can have a potential vulnerability can be exploited by an attacker. The importance of wireless security is and will be even more important in the future because critical systems such as public safety, national security, commercial and military communications will depend on the reliability of a wireless network.

The limits of wireless security will be tested in a 5G wireless network, simply because of the sheer volume and density of the devices that is expected to be served by the network. Affecting a tiny fraction of this number would result in the loss of functionality of a massive number of devices. Hence, the importance of making current and future wireless networks more robust to attacks and failures cannot be understated. Standardization of 5G networks is a couple of years away from taking form. Therefore, this thesis deals with the resilience of LTE networks and its downlink physical layer technology, *Orthogonal Frequency Division Multiplexing*. Prior research [7, 8] has shown that targeted interference on pilot signals is more efficient in degrading the Bit Error Rate performance than full-band jamming (also known as Barrage Jamming). Hence, this thesis will specifically be investigating and quantifying the impact of targeted interference on pilot signals, developing countermeasures against such attacks, and testing the resilience of the LTE downlink to such attacks.

1.3 Focus and Contributions of this Thesis

This thesis investigates the evolution of pilot signals, on the road from 4G to 5G wireless networks. The main ideas of focus are:

1. Vulnerability of OFDM downlink pilot signals to targeted interference, i.e. multi-tone pilot jamming.
2. Mitigation strategies to make OFDM systems more robust to multi-tone pilot jamming.
3. Study of the effect of targeted interference on LTE downlink pilots and (or) data resource elements.
4. Adaptation of OFDM downlink pilot pattern based on changing wireless channel characteristics

We provide important lessons learned from our investigation of OFDM systems in general, and LTE in particular. Our findings can help in the robust design of future 5G wireless networks to provide resilience against intentional and unintentional interference.

1.3.1 Contributions

The contribution of this thesis is divided into three parts. The first part develops a framework for analyzing multi-tone pilot jamming of downlink pilots in OFDM systems. OFDM is the underlying baseline communications technology for the LTE air interfaces. Hence, the second part applies the analysis to LTE-specific control channels and performance metrics. Finally, we propose an algorithm to adapt the pilot structure to optimize communications performance as a function of channel conditions.

1.3.1.1 Multi-Tone Pilot Jamming and Mitigation in OFDM Systems

Multi-tone pilot jamming refers to deliberate transmission of interference on top of pilot signals that degrade the process of equalization in coherent detection receivers. Prior research [9, 7, 8, 10, 11, 12, 13] has investigated pilot jamming and its mitigation in OFDM systems. This thesis builds on this body of work to quantify and demonstrate the level of degradation

(a) We develop a mathematical formulation and derive the Bit Error Rate (BER) and channel Estimation Mean Square Error (MSE) expressions for time and frequency fading channels (also known as *doubly dispersive/selective channels*).

(b) We introduce and evaluate mitigation strategies for *power-constrained pilot jammers* in SISO-OFDM systems. In contrast to prior work, the proposed mitigation strategies are more practical and simpler to be implemented in the widely deployed LTE networks.

(c) We devise and assess the performance of an approximate channel estimation algorithm in the presence of a power-constrained pilot jammer for MIMO-OFDM with full rank spatial multiplexing. As opposed to prior research in [13], we consider a the scenario where the pilots are broadcasted to the users of the cell and channel estimates are imperfect. The approximation is shown to yield satisfactory results in outdoor to indoor/indoor to indoor channels [14], and can be used for slow fading channels as well.

1.3.1.2 CRS Jamming and CQI Spoofing in LTE

Recently, research in [15, 16, 17, 18, 19] has looked at various control channel attacks in LTE. This thesis extends this body of research by analyzing the impact of CRS Jamming and CQI spoofing in the LTE downlink. Cell-Specific Reference Signals (CRS) are the downlink pilots in LTE, while Channel Quality Indicator (CQI) indicates the quality of the channel based on which the eNodeB (LTE Base Station) adapts its modulation scheme and rate of error control coding. To the best of our knowledge, we have demonstrated *'CQI Spoofing' in LTE for the first time*, wherein a jammer tricks the user into believing that the channel quality is good even though it isn't, by targeting interference on data subcarriers only. Experimental results pertaining to CRS Jamming and CQI spoofing are demonstrated, and its implications are discussed in this work.

1.3.1.3 Pilot Pattern Adaptation for Throughput Maximization

Current wireless networks use fixed pilot patterns, which lead to unnecessary overhead if the channel is flat in either time or frequency. Hence, it makes sense to adapt pilot patterns based on the channel flatness as seen by the user. Prior work has investigated and demonstrated pilot adaptation for MIMO-OFDM systems, and has compared its throughput performance with respect to that of LTE's fixed pilot pattern. Our work has built on this idea, and we have devised a simple codebook based approach to adapt pilot spacing in time and frequency in doubly dispersive channels. We show the throughput gains w.r.t. fixed pilot spacing, and provide insights for its extension into multi-band carrier aggregation systems with reduced feedback requirements. We also discuss the conditions which are necessary to implement pilot pattern adaptation.

1.4 Organization of this Thesis

Chapter 2 presents the system model and the mathematical derivation of the theoretical BER and channel estimation MSE in the presence of a multi-tone pilot jammer. Chapter 3 deals with mit-

igation techniques to counter a power-constrained multi-tone pilot jammer in SISO- and MIMO-OFDM systems. Chapter 4 demonstrates the impact of CRS Jamming and CQI Spoofing in the LTE downlink. Chapter 5 presents a heuristic algorithm to adapt pilot spacing in time and frequency based on estimated channel statistics, for SISO- and MIMO-OFDM scenarios. Finally, Chapter 6 provides the main conclusions, with a brief discussion of the research directions that can be spawned out of this work.

Chapter 2

Theoretical Analysis of Multi-Tone Pilot Jamming in OFDM

2.1 Background

Orthogonal Frequency Division Multiplexing (OFDM) is pervasive in today's wireless networks. The reason for its popularity is due to (a) its ability to achieve high data rates in mobile environments by effectively dealing with multipath propagation (b) tight channel packing (c) high area spectral efficiency (d) flexible resource allocation flexibility and scalability and (e) compatibility with multi-antenna techniques. It is employed in wireless commercial communications standards, such as IEEE 802.11 and LTE. It will be used for next-generation public safety networks and other mission critical communications systems [20].

OFDM waveforms and communications systems that use it have been analyzed in terms of robustness against radio frequency (RF) interference of various types. Research results have shown that OFDM-based systems are vulnerable to targeted RF interference [8, 9, 12, 21]. Although this kind of interference can be caused by an adversary that tries to disrupt communications, it can also be caused by other wireless systems in shared or unlicensed bands. Systems and technology need to adapt to the emerging scenario of shared, rather than exclusive use of spectrum for commercial wireless, including cellular communications. Hence, it is crucial to address the physical layer vulnerabilities of OFDM.

When the interferer has no prior knowledge about the signaling structure in the network, wideband barrage jamming is shown to be optimal [22]. The open access to wireless standards documentation makes it easy for an adversary to do better than wideband barrage jamming. Prior research [7], [8] has shown that OFDM reference signal or pilot-tone jamming is more efficient than wideband jamming. This is so because excessive interference on the reference signal corrupts the channel estimates, which are typically obtained by interpolating between the channel estimates of two or more reference symbols [23]. Hence, the equalization process is disrupted and the data demodula-

tion performance is degraded for relatively lower powers as compared to wideband jamming.

Patel et al. [9] derived closed form BER expressions to study the effect of imperfect channel estimation for OFDM/MC-CDMA systems in frequency-selective Rayleigh fading channels, in the presence and absence of a jammer. Han et al. [10] analyzed the mean squared error (MSE) of channel estimation in the presence of a narrowband pilot jammer and propose a jammed pilot detection and excision algorithm to mitigate the jammer. The damage that single-tone pilot jamming can cause is limited since only the adjacent data-carrying subcarriers would be affected.

Jun et al. [24] analyzed the BER performance under various partial-band, full-band and multi-tone jammer configurations for BPSK- and DBPSK-OFDM systems. Jasmin and Clancy [11] have derived closed-form expressions for PSK-OFDM and PSK-Single Carrier FDMA (PSK-SC FDMA) systems in the presence of jamming and imperfect channel estimation. These works assume a pilot-structure that requires time-only or frequency-only interpolation for channel estimation.

We extend on prior work and derive the MSE and BER for OFDM systems in doubly selective channels (strong fading in time and frequency), both in the presence and absence of a multi-tone pilot jammer. We assume a 'diamond-shaped' pilot arrangement for the OFDM block, because equal spacing of pilots in the block achieves the minimum MSE (MMSE) estimate of the channel [25]. This arrangement of pilots is used in modern communication systems, like 3GPP LTE/LTE-A. We assume least squares (LS) channel estimation along with linear interpolation for channel equalization because of its low complexity and good performance in the MSE sense, making it attractive for practical implementations [26].

Section 2.2 describes the system model for the wireless channel. Section 2.3 outlines the channel estimation algorithm in the presence and absence of a multi-tone pilot jammer. Section 2.4 presents the derivation and numerical simulation results of the MSE expressions for SISO-OFDM systems. Section 2.5 presents the derivation and numerical simulation results of the BER expressions. Section 2.6 concludes by summarizing the main results of this chapter.

Notation

The most important parameters and variables used in this chapter is introduced in Table 2.1.

2.2 Channel Model

The channel impulse response (CIR) $h(t,\tau)$ of a mobile wireless channel can be written as

$$h(t,\tau) = \sum_i \gamma_i(t)\delta(\tau - \tau_i), \tag{2.1}$$

where τ_i is the delay of the i^{th} resolvable multipath component, $\gamma_i(t)$ its corresponding complex amplitude and $\delta(t)$ the Dirac delta function. Due to relative motion in the channel, the $\gamma_i(t)$'s are

Table 2.1: Description of the most important parameters

Variable	Description
σ_H^2	Channel power gain factor
$R_t(\Delta t)$	Temporal correlation function of the wireless channel
$R_f(\Delta f)$	Frequency correlation function of the wireless channel
τ_{rms}	Root mean square delay spread of the wireless channel
f_d	Maximum Doppler Spread (Hz)
v_{tr}	Relative speed between the transmitter and the receiver
f_c	Center frequency of the OFDM signal
σ_w^2	Noise variance
σ_p^2	Pilot signal power
N	Total number of subcarriers per OFDM symbol
L	Pilot spacing in frequency on the same OFDM symbol
t_p	Pilot spacing in time between two consecutive pilot-bearing OFDM symbols
T	Pilot spacing in time between two odd/even-numbered pilot-bearing OFDM symbols
$H_k[n]$	Actual channel co-efficient of the k^{th} subcarrier on the n^{th} OFDM symbol
$\hat{H}_k[n]$	Channel estimate of the k^{th} subcarrier on the n^{th} OFDM symbol
$\mathcal{P}$	Set of pilot locations in the OFDM block. Its elements are of the form $\{n, k\} \in \mathcal{P}$
$\lvert\mathcal{P}\rvert$	Number of pilot locations in the OFDM frame
$\bar{\gamma}_b$	Average SNR per bit of QPSK symbols
$P_b(n, k)$	Probability of bit error at the k^{th} subcarrier on the n^{th} OFDM symbol

wide-sense stationary (WSS) narrowband complex Gaussian processes, and each $\gamma_i(t)$ is independent of the other multipath components $\gamma_j(t)$ for $i \neq j$ [27]. We model all $\gamma_i(t)$'s to have the same normalized correlation function $R_t(\Delta t)$ given by

$$r_{\gamma_i}(\Delta t) = \mathbb{E}[\gamma_i(t + \Delta t)\gamma_i^*(t)] = \sigma_i^2 R_t(\Delta t), \tag{2.2}$$

where $\mathbb{E}[\cdot]$ denotes the statistical expectation and σ_i^2 the average power of the i^{th} signal path. The channel frequency response (CFR) $H(t, f)$ is the Fourier transform of the CIR and is given by

$$H(t, f) = \int_{-\infty}^{+\infty} h(t, \tau) e^{-j2\pi f t} d\tau = \sum_i \gamma_i(t) e^{-j2\pi f \tau_i}. \tag{2.3}$$

The CFR can be used to compute the correlation function $R_H(\Delta t, \Delta f)$ that describes the second order statistics of the channel. It is defined as

$$R_H(\Delta t, \Delta f) \triangleq \mathbb{E}[H(t + \Delta t, f + \Delta f) H^*(t, f)]. \tag{2.4}$$

Using equations (2.1)-(2.4), we can rewrite (2.4) as [27]

$$\begin{aligned} R_H(\Delta t, \Delta f) &= \mathbb{E}\Big\{ \Big[\sum_i \gamma_i(t+\Delta t) e^{-j2\pi(f+\Delta f)\tau_i} \Big] \times \Big[\sum_i \gamma_i^*(t) e^{j2\pi f \tau_i} \Big] \Big\} \\ &= \sum_i \mathbb{E}[\gamma_i(t+\Delta t)\gamma_i^*(t)] e^{-j2\pi\Delta f\tau_i} \\ &= \sum_i \sigma_i^2 R_t(\Delta t) e^{-j2\pi\Delta f\tau_i} \\ &= R_t(\Delta t) \sum_i \sigma_i^2 e^{-j2\pi\Delta f\tau_i}. \end{aligned} \tag{2.5}$$

If we consider $\sigma_H^2 = \sum_i \sigma_i^2$, we can define the channel frequency correlation function $R_f(\Delta f)$ as

$$R_f(\Delta f) \triangleq \sum_i \frac{\sigma_i^2}{\sigma_H^2} e^{-j2\pi\Delta f\tau_i}. \tag{2.6}$$

Using this result, we can decompose the channel correlation function into its time and frequency correlation components:

$$R_H(\Delta t, \Delta f) = \sigma_H^2 R_t(\Delta t) R_f(\Delta f). \tag{2.7}$$

For simplicity, we assume a channel with $\sigma_H^2 = 1$ in this work. Equation (2.7) is widely known as the 'Wide Sense Stationary Uncorrelated Scattering' (WSSUS) approximation that enables the use of two 1-D estimators for channel estimation instead of the more complex 2-D estimators for joint time-frequency channel estimation in OFDM. The temporal correlation function $R_t(\Delta t)$ is given by the Jakes' model [28]

$$R_t(\Delta t) = J_0(2\pi f_d \Delta t), \tag{2.8}$$

where $J_0(\cdot)$ is the Bessel function of the first kind of zeroth order, $f_d = v_{tr} f_c / c$ with v_{tr} being the relative speed between the transmitter and the receiver, f_c the carrier frequency, and c the speed of light in free space.

2.3 Channel Estimation

Pilots are sent in parallel with data on dedicated time-frequency components of the OFDM block, called as a Resource Element (RE). We assume that the OFDM resource blocks have a 'diamond-shaped' arrangement of pilots because this arrangement achieves the MMSE estimate of the channel [25]. This pilot arrangement is used in the 3GPP LTE/LTE-A standard. Figure 2.1 shows the time-frequency resource grid, consisting of resource elements (REs) that form regular block structures. Each RE carries a modulation symbol (data) or a pilot symbol. Here, the pilot period is T seconds on the time axis and L subcarriers on the frequency axis with a cyclic frequency shift of $L/2$ between two consecutive pilot-bearing OFDM symbols. The *analysis region* is indicated

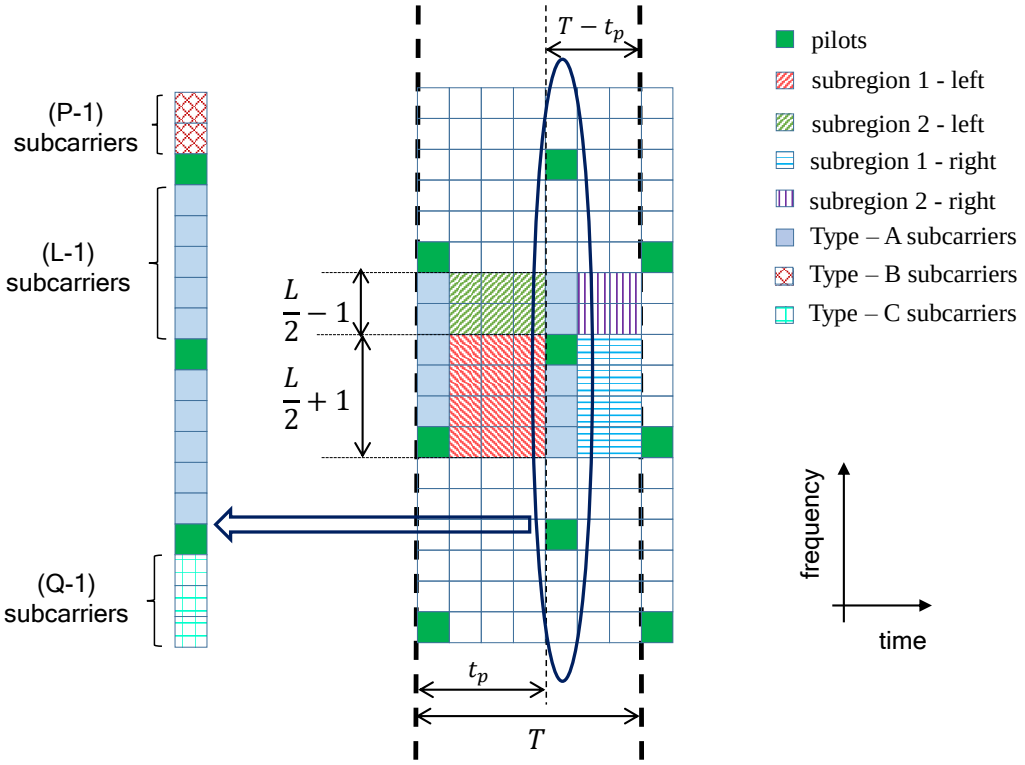

Figure 2.1: Mean Square Error analysis region for diamond-shaped pilot arrangement in OFDM.

by the colored REs in Figure 2.1, which periodically repeats in time and frequency to form the OFDM resource block. The analysis region forms a basis for the OFDM resource block, and hence the problem of MSE analysis of the OFDM block can be simplified to that of the analysis region. Sub-region 1 refers to the bottom $(L/2+1)$ subcarriers and sub-region 2 to the top $(L/2-1)$ subcarriers of the *analysis region*. Without loss of generality, we assume that L is an even number. To simplify the performance analysis, we divide the OFDM block into four distinct types of resource elements:

1. Pilots: Their channel estimates are obtained using Least Squares (LS) channel estimation, as shown in equation (2.10).

2. Type A: Resource Elements that lie between 2 pilot subcarriers. Their channel estimates are obtained by interpolation of channel estimates in frequency, between these two pilot subcarriers, as shown in equation (2.11) - (2.12), with $t = 0$.

3. Type B and C: Subcarriers that lie after the last pilot subcarrier (Type B), or before the first pilot subcarrier (Type C). Their channel estimates are obtained by extrapolation of channel estimates in frequency, using the ultimate and penultimate pilots (Type B) and the first and second pilots (Type C).

4. Sub-regions 1 and 2 : Resource elements that lie between two pilot-bearing OFDM symbols. Their channel estimates are obtained by linear interpolation in frequency and time, as given by (2.11) - (2.12), for $t \neq 0$.

Let $\mathcal{P}$ be set of pilot locations in an OFDM symbol. Let its elements form an ordered pair given by $(l, n) \in \mathcal{P}$, where l is the subcarrier index of the pilot at time n. For $(l, n) \in \mathcal{P}$, $H_l[n]$ is the frequency domain channel coefficient that is experienced by the pilot $P_l[n]$ on the l^{th} subcarrier and at time index $n = bt_p$, with $b \in \mathbb{Z}$.

2.3.0.1 Case 1: No Jamming

The received signal $Y_l[n]$ after removing the cyclic prefix can then be represented as

$$Y_l[n] = H_l[n]P_l[n] + w_l[n], \tag{2.9}$$

where $w_l[n] \sim \mathcal{CN}(0, \sigma_w^2)$ is circularly symmetric complex Gaussian noise. The least squares channel estimate $\hat{H}_l[n]$ of the l^{th} subcarrier at time n is given by

$$\begin{aligned} \hat{H}_l[n] &= Y_l[n]/P_l[n] \\ &= H_l[n] + w_l[n]/P_l[n]. \end{aligned} \tag{2.10}$$

For pilots, we have $w_l[n]/P_l[n] \sim \mathcal{CN}(0, \sigma_w^2/\sigma_p^2)$ for $l \in \mathcal{P}$, where σ_p^2 is the pilot signal power. Without loss of generality, we assume that $\sigma_p^2 = 1$ for the rest of the theoretical analysis in chapters 2 and 3.

Let $H_k[n]$ be the frequency domain channel of the k^{th} subcarrier in the n^{th} OFDM symbol, and $\hat{H}_k[n]$ its estimate. Suppose that for the n^{th} OFDM symbol, two consecutive pilots are located on the mL^{th} and $(m+1)L^{th}$ subcarriers for $m \in \mathbb{Z}$. Then for the $(n + t_p)^{th}$ OFDM symbol, the pilot-bearing subcarrier locations are at $(mL - L/2)$ and $(mL + L/2)$. The channel estimation in sub-region 1 can then be carried out using linear interpolation in time and frequency as follows:

$$\begin{aligned} \hat{H}_{mL+k}[n+t] = (1-\eta)\big[(1-\zeta)\hat{H}_{mL}[n] + \zeta\hat{H}_{(m+1)L}[n]\big] + \eta\Big[\Big(\frac{1}{2} - \zeta\Big)\hat{H}_{(m-1/2)L}[n+t_p] \\ + \Big(\frac{1}{2} + \zeta\Big)\hat{H}_{(m+1/2)L}[n+t_p]\Big], \end{aligned} \tag{2.11}$$

for $0 \leq t < t_p$ and $0 \leq k \leq L/2$, where $\eta \triangleq t/t_p$ and $\zeta \triangleq k/L$. Similarly, the channel estimates for sub-region 2 can be obtained using

$$\begin{aligned} \hat{H}_{mL+k}[n+t] = (1-\eta)\big[(1-\zeta)\hat{H}_{mL}[n] + \zeta\hat{H}_{(m+1)L}[n]\big] + \eta\Big[\Big(\frac{3}{2} - \zeta\Big)\hat{H}_{(m+1/2)L}[n+t_p] \\ + \Big(\zeta - \frac{1}{2}\Big)\hat{H}_{(m+3/2)L}[n+t_p]\Big], \end{aligned} \tag{2.12}$$

for $0 \leq t < t_p$ and $L/2 < k < L$. This interpolation method is commonly used in practical systems due to its low complexity and reasonably good performance [26].

2.3.0.2 Case 2: In the presence of a multi-tone pilot jammer

For the pilot on the l^{th} subcarrier at time n, the channel estimate in the presence of a jammer $\hat{H}_l^J[n]$ will be

$$\begin{aligned}\hat{H}_l^J[n] &= Y_l^J[n]/P_l[n] \\ &= H_l[n] + (w_l[n] + H_l'[n]J_l[n])/P_l[n],\end{aligned} \tag{2.13}$$

where $H_l'[n]$ is the channel coefficient between the jammer and the receiver for the l^{th} subcarrier at time n, and $J_l[n]$ the transmitted jamming signal. $H_l'[n]$ is a complex Gaussian random variable for typical Rayleigh fading wireless channels. For typical jammer signal types such as constant envelope digitally modulated, multi-tone continuous wave or i.i.d. AWGN. we get $H_l'[n]J_l[n] \sim \mathcal{CN}(0, \sigma_J^2)$, where σ_J^2 is the average jamming signal power per jammed RE.

Therefore, the error on the channel estimate at the pilots propagates into those of the data resource elements [1]. The channel estimates of the data resource element at the $(mL+k)^{th}$ subcarrier of the $(n+t)^{th}$ OFDM symbol is given by

$$\begin{aligned}\hat{H}_{mL+k}^J[n+t] = (1-\eta)\big[(1-\zeta)\hat{H}_{mL}^J[n] + \zeta\hat{H}_{(m+1)L}^J[n]\big] + \eta\Big[\Big(\frac{1}{2}-\zeta\Big)\hat{H}_{(m-1/2)L}^J[n+t_p] \\ + \Big(\frac{1}{2}+\zeta\Big)\hat{H}_{(m+1/2)L}^J[n+t_p]\Big],\end{aligned} \tag{2.14}$$

for $0 \leq t < t_p$ and $0 \leq k \leq L/2$, and

$$\begin{aligned}\hat{H}_{mL+k}^J[n+t] = (1-\eta)\big[(1-\zeta)\hat{H}_{mL}^J[n] + \zeta\hat{H}_{(m+1)L}^J[n]\big] + \eta\Big[\Big(\frac{3}{2}-\zeta\Big)\hat{H}_{(m+1/2)L}^J[n+t_p] \\ + \Big(\zeta-\frac{1}{2}\Big)\hat{H}_{(m+3/2)L}^J[n+t_p]\Big],\end{aligned} \tag{2.15}$$

for $0 \leq t < t_p$ and $L/2 < k < L$.

For REs in $t_p \leq t \leq T$, we can substitute $t \to (T-t)$ and $t_p \to (T-t_p)$ in equations (2.11)-(2.15) to find the appropriate channel estimates.

2.4 Mean Square Error (MSE) Analysis

We will describe the impact of multi-tone pilot jamming on the mean squared error (MSE) of the channel estimates in this section. Figure 2.1 shows the *analysis region* for the MSE analysis. To be more generic, we start with the case when $t_p \neq T - t_p$. Subcarriers of type A, B and C are shown

[1] Apart from this error the major threat from pilot-tone jamming is considered to be the fact that the channel on the data-carrying subcarriers can be quite different than assumed since it is not being jammed [7].

in Figure 2.1. To simplify our MSE analysis, we assume that $N \gg L$ where N is the total number of subcarriers per OFDM symbol, and L is the pilot spacing in frequency. This assumption is valid for modern OFDM-based communications systems, such as LTE or Wi-Fi and may not hold for narrowband-LTE (NB-LTE) or LTE MTC (LTE-M) suggested for IoT devices [29]. With this assumption, we can approximate the Mean Square Error of Type B and C subcarriers, with those of Type A subcarriers,. This is a reasonable approximation because Type A subcarriers will dominate the spectrum in such a scenario.

2.4.1 Mean Square Error in the Absence of a Jammer

2.4.1.1 MSE of Pilots

For pilots, the channel estimates are given as shown in equation (2.10). We have $w_l/P_l \sim \mathcal{CN}(0, \sigma_w^2/\sigma_p^2)$ for $l \in \mathcal{P}$, where σ_p^2 is the pilot signal power. Hence, the Mean Square error MSE_p of the channel estimates on pilot subcarriers becomes

$$\begin{aligned} MSE_p &= \frac{1}{|\mathcal{P}|}\sum_{l\in\mathcal{P}} \mathbb{E}[|H_l - \hat{H}_l|^2] \\ &= \sigma_w^2/\sigma_p^2, \end{aligned} \tag{2.16}$$

where $|\mathcal{P}|$ denotes the cardinality of $\mathcal{P}$. It is important to note here that w_l/P_l is uncorrelated with the channel term H_l. Hence, we make use of the fact that $\mathbb{E}\{H_l[n]w_l^*[n]\} = 0$ in the rest of the analysis presented in this work, where x^* denotes the complex conjugate of x.

2.4.1.2 MSE of Type-A REs

The Mean Square Error of the channel estimates for Type A REs, denoted by $MSE_{f,A}$, is derived in [30] and expressions using our symbols as

$$MSE_{f,A} = \left(\frac{5L-1}{3L}\right)R_f(0) + \left(\frac{2L-1}{3L}\right)\frac{\sigma_w^2}{\sigma_p^2} + 2\left(\frac{L+1}{6L}\right)\Re(R_f(L)) + \alpha, \tag{2.17}$$

where $\Re(x)$ denotes the real part of x and

$$\alpha = -\frac{2}{L-1}\sum_{i=1}^{L-1}\left[\left(\frac{L-k}{L}\right)\Re(R_f(k)) + \frac{k}{L}\Re(R_f(k-L))\right]. \tag{2.18}$$

where α represents the residual terms.

2.4.1.3 MSE of REs in Subregions 1 and 2

Once the channel estimates of pilot-bearing OFDM symbols are obtained, linear interpolation can be implemented in the time domain to obtain channel estimates for the OFDM symbols without pilots. Due to periodicity in the placement of the pilots as shown in Figure 2.1, the analysis can be carried out only in the colored sub-regions shown in Figure 2.1.

We further subdivide this region into two subregions for $0 \leq k \leq (L-1)$, i.e. subregion 1: $0 \leq k \leq L/2$ ($L/2+1$ REs) and Region 2: $L/2 < k < L$ ($L/2-1$ REs). The pilot-bearing OFDM symbol splits subregions 1 and 2 into left and right-hand sides, with the appropriate time-offset variable t ranging from $1 \leq t \leq t_p$ and $1 \leq t \leq (T-t_p)$ respectively. In the following analysis, t_p is the time-spacing between two adjacent pilot-bearing OFDM symbols in the grid, and $n = mT$ is the time variable that corresponds to the start of the OFDM block, for $m \in \mathbb{Z}$.

Due to symmetry in the analysis region, we present the analysis for the left half of subregions 1 and 2 only. Using these expressions, the analysis of the right hand side of subregions 1 and 2 can be derived by inverting the time-offset variable and and replacing t_p by $t_r = (T-t_p)$ in the resulting expressions.

2.4.1.4 Left Part of Subregion 1: $0 \leq k \leq L/2, 1 \leq t < t_p$

For this subregion, the MSE expression for linear interpolation using Least Squares $MSE_{1,l}$, is

$$MSE_{1,l} = C_1 \sum_{k=0}^{L/2} \sum_{t=1}^{t_p-1} \mathbb{E}\{|\hat{H}_{mL+k}[n+t] - H_{mL+k}[n+t]|^2\}, \tag{2.19}$$

where $C_1 \triangleq \frac{1}{(L/2+1)(t_p-1)}$. Using the interpolation equation for this region from equation (2.11), we get

$$MSE_{1,l} = C_1 \sum_{k=0}^{L/2} \sum_{t=1}^{t_p-1} \mathbb{E}\Big\{\Big|(1-\eta)\Big[(1-\zeta)\hat{H}_{mL}[n] + \zeta\hat{H}_{(m+1)L}[n]\Big] + \eta\Big[\Big(\frac{1}{2}-\zeta\Big)\hat{H}_{(m-\frac{1}{2})L}[n+t_p] + \Big(\frac{1}{2}+\zeta\Big)\hat{H}_{(m+\frac{1}{2})L}[n+t_p]\Big] - H_{mL+k}[n+t]\Big|^2\Big\}. \tag{2.20}$$

After expanding the terms and simplifying, we get

$$MSE_{1,l} = (1+\lambda\omega)R_f(0)R_t(0) + \lambda(2-\omega)R_t(0)\Re(R_f(L)) + (1-2\lambda)R_t(t_p)\Re\Big[\omega' R_f\Big(\frac{L}{2}\Big) + (1-\omega')R_f\Big(\frac{3L}{2}\Big)\Big] + \lambda\omega\left(\frac{\sigma_w^2}{\sigma_p^2}\right) - \varepsilon_{1,l}, \tag{2.21}$$

where

$$\lambda \triangleq \frac{2t_p-1}{6t_p}; \omega \triangleq \frac{4L+1}{3L}; \omega' \triangleq \frac{23L+2}{24L},$$

and

$$\varepsilon_{1,l} = 2C_1 \sum_{k=0}^{L/2} \sum_{t=1}^{t_p-1} \Big\{ (1-\eta) R_t(t) \Re\Big[(1-\zeta) R_f(k) + \zeta R_f(L-k) \Big] + \eta R_t(t-t_p) \Re\Big[\Big(\frac{1}{2} - \zeta \Big) \times R_f\Big(\frac{L}{2} + k \Big) + \Big(\frac{1}{2} + \zeta \Big) R_f\Big(k - \frac{L}{2} \Big) \Big] \Big\}. \tag{2.22}$$

where $\varepsilon_{1,l}$ are the cross terms.

2.4.1.5 Left part of Subregion 2: $L/2 < k < L, 1 \leq t < t_p$

For the left hand side of subregion 2, the mean square error is given by

$$MSE_{2,l} = C_2 \sum_{k=L/2+1}^{L-1} \sum_{t=1}^{t_p-1} \mathbb{E}\{ |\hat{H}_{mL+k}[n+t] - H_{mL+k}[n+t]|^2 \}, \tag{2.23}$$

where $C_2 = \frac{1}{(L/2-1)(t_p-1)}$. Using equation (2.12) in (2.23) and simplifying terms, we obtain

$$MSE_{2,l} = (1+\lambda\Omega) R_f(0) R_t(0) + \lambda(2-\Omega) \Re(R_f(L)) R_t(0) + (1-2\lambda) R_t(t_p) \Re\Big[\Omega' R_f\Big(\frac{L}{2} \Big) + (1-\Omega') R_f\Big(\frac{3L}{2} \Big) \Big] + \lambda\Omega \left(\frac{\sigma_w^2}{\sigma_p^2} \right) - \varepsilon_{2,l}, \tag{2.24}$$

where

$$\Omega \triangleq \frac{4L-1}{3L}; \Omega' \triangleq \frac{23L-2}{24L},$$

and

$$\varepsilon_{2,l} = 2C_2 \sum_{k=L/2+1}^{L-1} \sum_{t=1}^{t_p-1} \Big\{ (1-\eta) R_t(t) \Re\Big[(1-\zeta) R_f(k)) + \zeta R_f(k-L) \Big] + \eta R_t(t-t_p) \times \Re\Big[\Big(\frac{3}{2} - \zeta \Big) R_f\Big(k - \frac{L}{2} \Big) + \Big(\zeta - \frac{1}{2} \Big) R_f\Big(k - \frac{3L}{2} \Big) \Big] \Big\}. \tag{2.25}$$

where $\varepsilon_{2,l}$ are the cross-terms.

2.4.1.6 Right parts of Subregion 1 and 2: $t_p < t \leq (T-1)$

The MSE for the right part of subregions 1 and 2, $MSE_{1,r}$ and $MSE_{2,r}$ respectively, can be obtained by inverting the time offset variable t (i.e. by replacing t by $-t$) and t_p by $t_r = (T - t_p)$. The MSE expressions will be similar to that of the left part of subregions 1 and 2 because the only term that would get affected by time inversion is $R_t(t)$, which is an even function by the definition of $J_0(x)$. Hence, $R_t(t) = R_t(-t)$, implying that the MSE analysis of the left part of regions 1 and 2 applies to these parts as well.

2.4.1.7 Overall Mean Square Error

The overall Mean Square error MSE_{tot} is the weighted average of the MSEs of each sub-region and is given by

$$MSE_{tot} = \frac{1}{N_B}\left[\frac{MSE_{1,l}}{C_1} + \frac{MSE_{2,l}}{C_2} + \frac{MSE_{1,r}}{C_3} + \frac{MSE_{2,r}}{C_4} + 2\cdot(L-1)MSE_{f,A} + 2\cdot MSE_p\right], \tag{2.26}$$

where $N_B = L \cdot T$ is the total number of time-frequency elements in the OFDM block that repeats itself in time and frequency to yield the entire OFDM frame, $C_3 \triangleq \frac{1}{(L/2+1)(t_r-1)}$ and $C_4 \triangleq \frac{1}{(L/2-1)(t_r-1)}$. There are 2 special cases we would like to mention, where the expressions can be simplified further.

2.4.1.8 Special Case 1: The AWGN channel

For the special case of the AWGN channel, only noise-dependent terms exist, hence the MSE for this case can be written as

$$MSE_{tot,AWGN} = \frac{\sigma_w^2}{N_B\sigma_p^2}\left[\lambda\Big(\frac{\omega}{C_1} + \frac{\Omega}{C_2}\Big) + \Gamma\Big(\frac{\omega}{C_3} + \frac{\Omega}{C_4}\Big) + 2 + 2\cdot(L-1)\kappa\right], \tag{2.27}$$

where $\kappa = \frac{2L-1}{3L}$.

2.4.1.9 Special Case 2: Symmetric Pilot Spacing

When T is even and the pilot spacing is symmetric, we have $t_p = T - t_p$, in which case $C_1 = C_3$ and $C_2 = C_4$. Because the channel temporal correlation $R_t(\Delta t)$ is an even function, $MSE_{1,l} = MSE_{1,r}$ and $MSE_{2,l} = MSE_{2,r}$. Thus the resulting MSE $MSE_{tot,sym}$, can be written as

$$MSE_{tot,sym} = \frac{2}{N_B}\left[\frac{MSE_{1,l}}{C_1} + \frac{MSE_{2,l}}{C_2} + MSE_p + (L-1)\cdot MSE_{f,A}\right]. \tag{2.28}$$

2.4.2 Mean Square Error in the Presence of a Synchronous Multi-Tone Pilot Jammer

The MSE analysis we have derived so far can be extended to the case where a multi-tone pilot jammer is present. We assume the following about the jammer in the following analysis:

1. The jammer is synchronized with the target, and transmits only on the time slots and subcarriers that contain the pilot symbols, i.e. $J_l[n] \neq 0$ if and only if $(l, n) \in \mathcal{P}$.

2. The jammer satisfies $H'_l[n]J_l[n] \sim \mathcal{CN}(0, \sigma_J^2)$, where σ_J^2 is the average jamming signal power per jammed RE. This is possible for typical jammer signal formats such as constant envelope digitally modulated, multi-tone continuous wave or i.i.d. AWGN signals.

3. Jammer on all pilot locations have identical statistics, i.e. $\mathbb{E}[|H'_l[n]J_l[n]|^2] = \sigma_J^2$ for all $l \in \mathcal{P}$ at time n. Jammer signal on one pilot location is uncorrelated with that on every other pilot location, i.e. $\mathbb{E}\big[J_l[n]J_k^*[m]\big] = 0$ for $n \neq m$ or $l \neq k$.

4. Each multipath component goes through an uncorrelated scattering environment. Hence, $\mathbb{E}\big[H_l[n]H'^*_l[n]\big] = 0$. This is a consequence of the WSSUS approximation.

Assumption 3 makes the performance analysis more tractable, helping us derive very close approximations. Moreover, if the jammer signal is being tracked by the target the jammer symbol correlation across different pilot locations can be exploited for jammer cancellation. Assumption 1 represents the most power-efficient jammer possible in the absence of the jammer to receiver channel information. However, this is hard to achieve practically because such a jammer would need to be perfectly synchronized with the target receiver. Based on these assumptions, results derived in section 2.4.1 can be used for this scenario, with modifications in the noise power, as shown by the following lemma.

Lemma 2.4.1. *A synchronous multi-tone pilot jammer with the above characteristics has the same effect as AWGN on the MSE of channel estimation.*

Proof: From equation (2.13)-(2.15), we see that the channel estimate is a linear combination of the channel estimates on the pilot REs. Because of uncorrelated scattering, $\mathbb{E}\big[H_l[n]H'^*_l[n]\big] = 0$. Due to uncorrelated jammer signals on each pilot, i.e. $\mathbb{E}\big[J_l[n]J_k^*[m]\big] = 0$ for $n \neq m$ or $l \neq k$, the only non-zero terms that remain in the MSE expression are the σ_J^2 terms, which have the same coefficients as σ_w^2 terms, i.e. AWGN.

Therefore, a synchronous multi-tone pilot jammer with the assumed second-order statistics can be modeled to have the same effect on MSE as AWGN does.

By Lemma 2.4.1, the MSE expressions in the presence of the synchronous multi-tone jammer is obtained by replacing σ_w^2 with $(\sigma_w^2 + \sigma_J^2)$ in equations (2.16)-(2.28).

Table 2.2: Simulation Parameters

Parameter	**Value**
FFT-length	128
Number of OFDM subcarriers	72
Number of Guard Subcarriers	28 on each band edge
Center Frequency f_c	$2.0\,\mathrm{GHz}$
Subcarrier Spacing f_{sub}	$15\,\mathrm{kHz}$
OFDM symbol duration T_o	$71.875\,\mu\mathrm{s}$
Cyclic Prefix Duration	$5.21\,\mu\mathrm{s}$
Pilot spacing in time t_p	4
Pilot spacing in frequency L	6
Channel parameters:	Doubly selective: Jakes Doppler Spectrum with multipath fading.
Channel Estimation	Least Squares (pilots) 2D-Linear Interpolation (data REs)
Equalization	Zero Forcing (ZF)

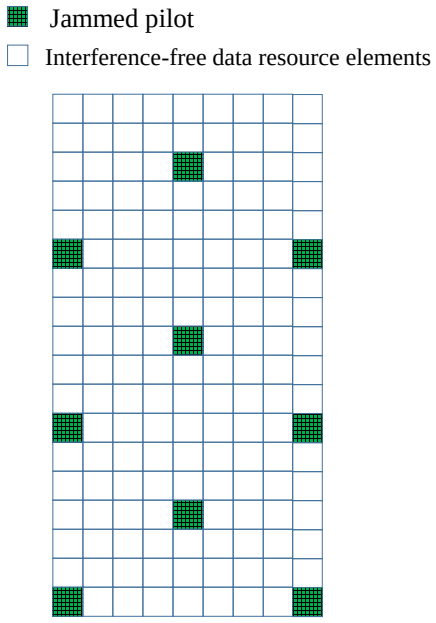

Figure 2.2: Illustration of a Synchronous multi-tone pilot jammer.

2.4.3 Numerical Results

This subsection presents the validation of derived MSE expressions by numerical simulations. Table 2.2 summarizes the parameters of the OFDM system. Each channel is chosen to be doubly selective: Jakes Doppler Spectrum models the mobility effects in the channel, with Rayleigh fading due to multipath modeled using a tapped delay-line model. The jammer is assumed to be synchronized with the target such that only pilot locations in the OFDM block are jammed, as shown in Figure 2.2.

We define the jammer-to-signal ratio per RE (JSR) to be the ratio between the received interference power and the received signal power on a target RE. Hence, $JSR = 0$ for interference-free REs (non-pilot REs) and non-zero otherwise (pilots). The simulations consider equal power allocation on all resource elements of the target OFDM signal, and equal jammer power allocations on all targeted pilot locations.

Figures 2.3, 2.4 and 2.5 show the comparison of theoretical and simulated MSE performance, for $(\tau_{rms}, f_d) = (200\,\text{ns}, 100\,\text{Hz})$, $(\tau_{rms}, f_d) = (400\,\text{ns}, 200\,\text{Hz})$ and $(\tau_{rms}, f_d) = (900\,\text{ns}, 500\,\text{Hz})$ respectively. The curves match very well, validating the derived MSE expressions in equations (2.26)-(2.28). The deviation between the curves at higher mobilities is due to Intercarrier Interference (ICI), which exhibits different statistical properties when compared to AWGN [31].

We observe that synchronous multi-tone pilot jamming significantly degrades the channel estimation performance of the OFDM system, as the MSE increases by three orders of magnitude. Hence, it is aptly referred to as an 'equalization attack' in the literature [12].

2.5 Bit Error Rate Analysis

For the BER analysis, we consider the symmetric pilot distribution case of $t_p = T - t_p$, shown in Figure 2.6. Due to symmetry, the region marked with upward diagonal lines has the same time and frequency correlation functions as the *analysis region*. Hence, the shaded region is excluded from the *analysis region* since it will statistically yield the same BER as the unshaded colored region.

For QPSK-modulated OFDM waveforms, the BER probability $P_b(t,k)$ for a resource element at the k^{th} subcarrier of the t^{th} OFDM symbol is given as [32]

$$P_b(t,k) = \frac{1}{2}\left[1 - \frac{1}{2\sqrt{2}}\frac{\theta_{t,k} + \theta'_{t,k}}{\sqrt{1 + \frac{1}{2\bar{\gamma}_b} - \frac{(\theta_{t,k} - \theta'_{t,k})^2}{2}}} - \frac{1}{2\sqrt{2}}\frac{\theta_{t,k} - \theta'_{t,k}}{\sqrt{1 + \frac{1}{2\bar{\gamma}_b} - \frac{(\theta_{t,k} + \theta'_{t,k})^2}{2}}}\right], \tag{2.29}$$

where $\bar{\gamma}_b$ is the average SNR per bit for the QPSK symbol and

$$\theta_{t,k} = \frac{\alpha'_{t,k}}{\beta_{t,k}\beta'_{t,k}}, \quad \theta'_{t,k} = \frac{\alpha''_{t,k}}{\beta_{t,k}\beta'_{t,k}}, \tag{2.30}$$

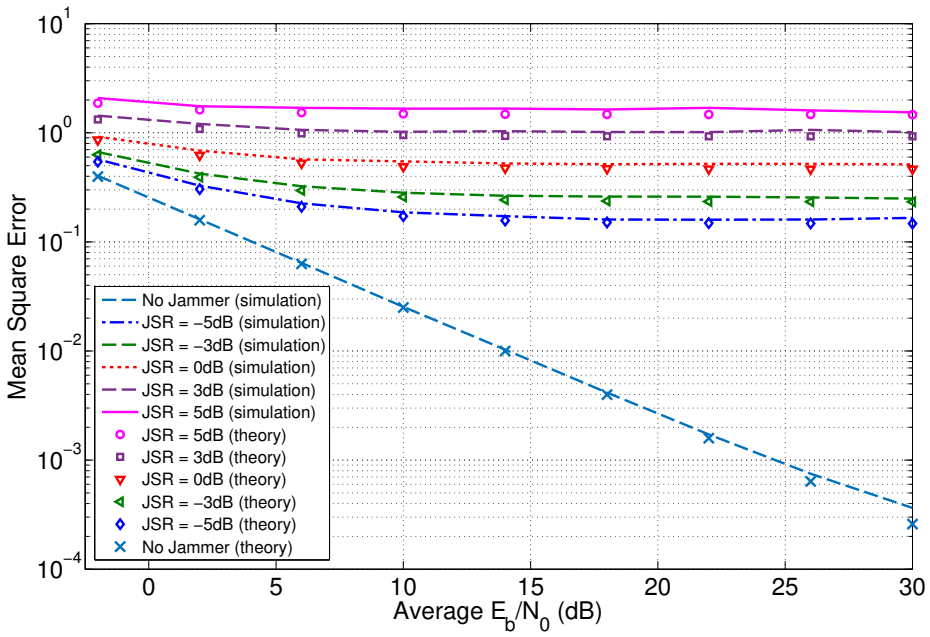

Figure 2.3: Theoretical and simulated channel estimation Mean Square Error for $f_d = 100\,\text{Hz}$, $\tau_{rms} = 200\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer.

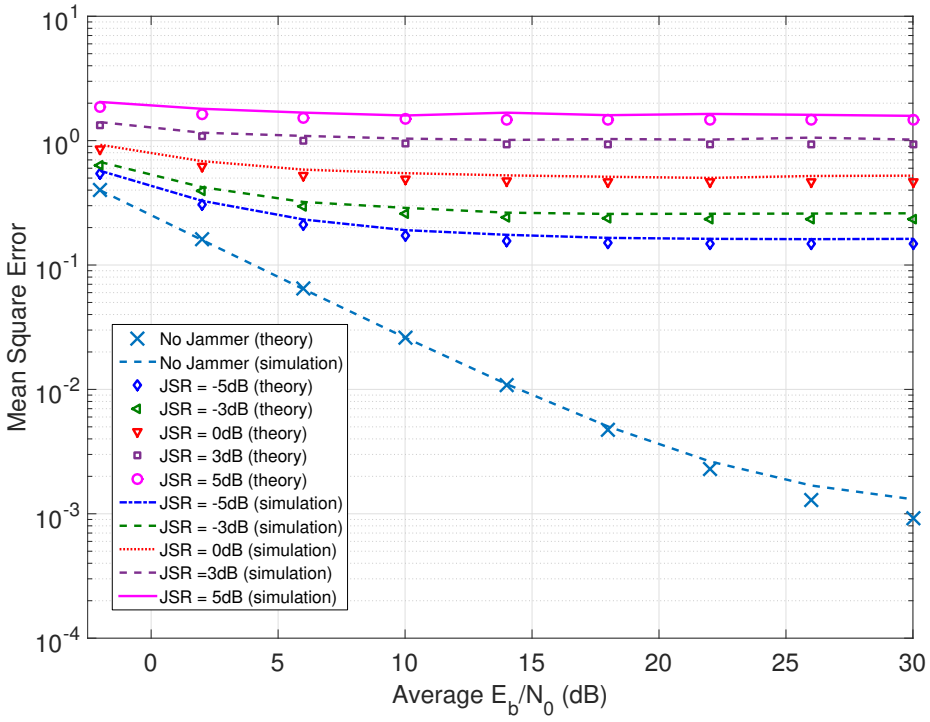

Figure 2.4: Theoretical and simulated channel estimation Mean Square Error for $f_d = 200\,\text{Hz}$, $\tau_{rms} = 400\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer.

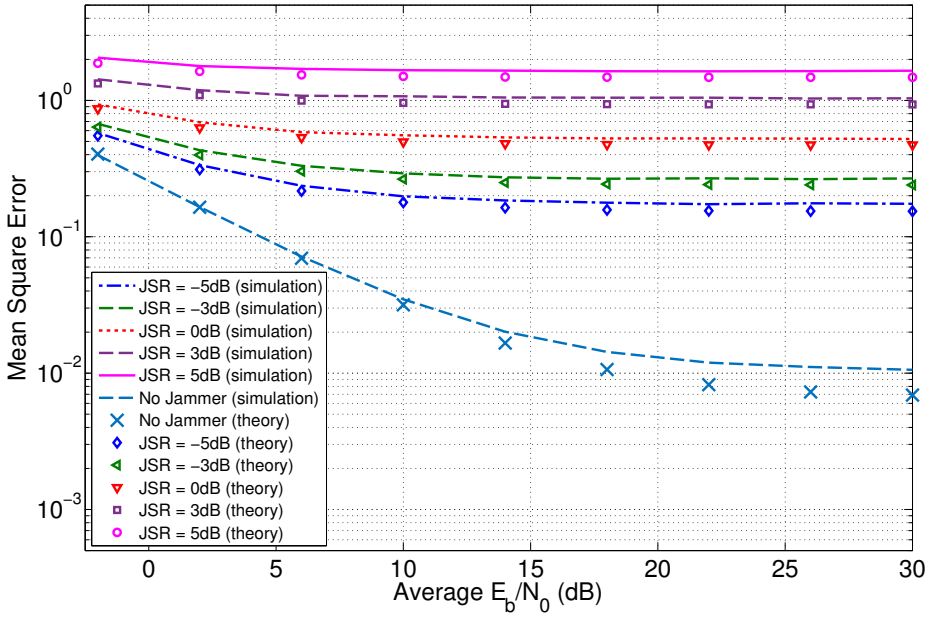

Figure 2.5: Theoretical and simulated channel estimation Mean Square Error for $f_d = 500\,\text{Hz}$, $\tau_{rms} = 900\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer.

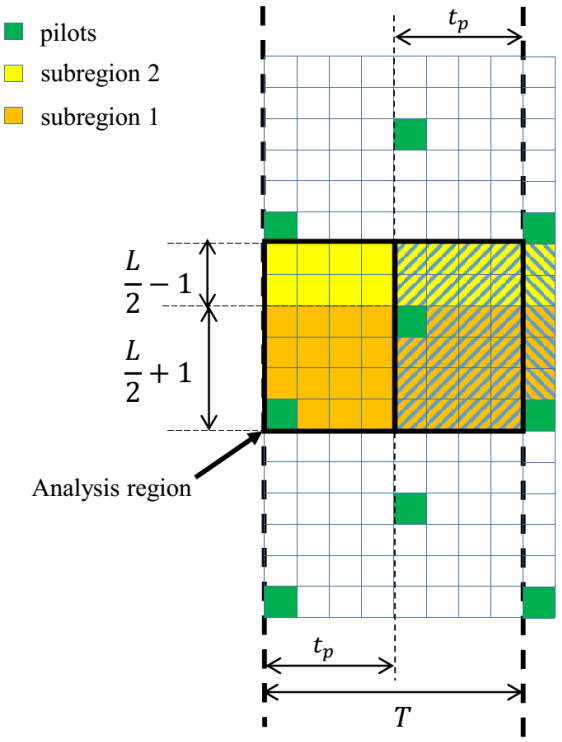

Figure 2.6: Analysis Region for BER derivations in the presence and absence of a multi-tone pilot jammer.

$$\beta_{t,k}^2 = \frac{1}{2}\mathbb{E}[|H_k[t]|^2], \quad \beta'^2_{t,k} = \frac{1}{2}\mathbb{E}[|\hat{H}_k[t]|^2]$$
$$\alpha_{t,k} = \frac{1}{2}\mathbb{E}\big[\hat{H}_k[t]H_k^*[t]\big] = \alpha'_{t,k} + j\alpha''_{t,k}, \tag{2.31}$$

where $\alpha'_{t,k}, \alpha''_{t,k} \in \mathbb{R}$. To derive the BER for the OFDM block with the diamond-shaped pilot pattern, we substitute (2.11) and (2.12) in (2.29)-(2.31) for each resource element in the *analysis region* and find the average. This is discussed in more detail in the next subsection.

2.5.1 BER in the Presence of a Synchronous Multi-Tone Pilot Jammer

In the presence of a multi-tone pilot jammer, the terms in (2.29) need to be calculated for sub-regions 1 and 2, shown in Figure 2.6. We will present the expressions for sub-region 1 in this section; the corresponding expressions for sub-region 2 can be derived from those of sub-region 1 by symmetry.

2.5.1.1 Lower REs of sub-region 1: $0 \le k \le L/2, 0 \le t < t_p$

We derive the BER expressions, with the same assumptions about the jammer as outlined in section 2.4. Because the *analysis region* forms a basis of the 2D resource grid, we can simplify notations by assuming $m = 0$ and $n = 0$ in (2.11) and (2.12), so that $0 \le k \le L/2$ and $0 \le t < t_p$ represent the equivalent ranges of subcarriers and time slots of sub-region 1. The corresponding channel estimate then becomes

$$\hat{H}_k^J[t] = (1-\eta)\big[(1-\zeta)\hat{H}_0^J[0] + \zeta\hat{H}_L^J[0]\big] + \eta\Big[\Big(\frac{1}{2}-\zeta\Big)\hat{H}_{-L/2}^J[t_p] + \Big(\frac{1}{2}+\zeta\Big)\hat{H}_{L/2}^J[t_p]\Big]. \tag{2.32}$$

For $\beta_{t,k}$ we then obtain

$$\beta_{t,k}^2 = \frac{1}{2}\mathbb{E}[|H_k[t]|^2] = \sigma_H^2/2. \tag{2.33}$$

Note that $R_f(0)R_t(0) = 1$ as a result from (2.6)-(2.8) and

$$\beta'^2_{t,k} = \frac{1}{2}\mathbb{E}[|\hat{H}_k^J[t]|^2] = \frac{1}{2}[\eta^2(1/2+2\zeta^2) + (1-\eta)^2(1+2\zeta^2-2\zeta)](\sigma_H^2+\sigma_w^2+\sigma_J^2) +$$
$$[(1-\eta)^2(\zeta-\zeta^2) + \eta^2(1/4-\zeta^2)]\Re[R_f(L)]R_t(0) + \eta(1-\eta)[(1-\zeta)+\zeta(1/2+\zeta)]\times$$
$$\Re[R_f(L/2)]R_t(t_p) + \eta\zeta(1-\eta)(1/2-\zeta)\Re[R_f(3L/2)]R_t(t_p). \tag{2.34}$$

Similarly,

$$\begin{aligned}\alpha_{t,k} &= \frac{1}{2}\mathbb{E}\big[\hat{H}_k^J[t]H_k^*[t]\big] \\ &= \frac{1}{2}\Big\{(1-\eta)[(1-\zeta)R_f(-k)+\zeta R_f(L-k)]R_t(t)+\eta\Big[\Big(\frac{1}{2}-\zeta\Big)R_f\Big(\frac{-L}{2}-k\Big) \\ &+ \Big(\frac{1}{2}+\zeta\Big)R_f\Big(\frac{L}{2}-k\Big)\Big]R_t(t_p-t)\Big\}. \end{aligned} \tag{2.35}$$

The BER of sub-region 1 REs $P_b(t,k)$ can be found with (2.29) using (2.33)-(2.35).

2.5.1.2 Lower REs of sub-region 1: $L/2 < k < L, 0 \le t < t_p$

The BER of sub-region 2 REs can be equivalently derived. Here, $L/2 < k < L$ and $0 \le t < t_p$. We define $k' = k - L/2$ and substitute it into equation (2.12) to obtain

$$\hat{H}_{k'}^J[t] = (1-\eta)\Big[\Big(\frac{1}{2}-\zeta'\Big)\hat{H}_0^J[n]+\Big(\frac{1}{2}+\zeta'\Big)\hat{H}_L^J[n]\Big]+\eta\big[(1-\zeta')\hat{H}_{L/2}^J[t_p]+\zeta'\hat{H}_{3L/2}^J[t_p]\big], \tag{2.36}$$

where $\zeta' \triangleq k'/L = \zeta + 1/2$. Noting the similarity of (2.36) with (2.32), and the fact that the temporal correlation $R_t(t)$ is an even function, we find the correlation terms of these resource elements by substituting $k' = k - L/2$ in (2.33)-(2.35). Therefore

$$\alpha_{t,k'} = \alpha_{t,k-L/2},\ \beta_{t,k'} = \beta_{t,k-L/2},\ \beta'_{t,k'} = \beta'_{t,k-L/2} \tag{2.37}$$

can be found using (2.33)-(2.35) and used in (2.29) to find the BER $P_b(t,k')$ of a resource element in sub-region 2.

2.5.1.3 Overall BER

The overall BER of the OFDM resource block with QPSK symbols in the presence of a multi-tone jammer $P_{b,QPSK}^J$ can finally be found by averaging the BER over all data resource elements in the analysis region:

$$P_{b,QPSK}^J = \frac{1}{L\cdot t_p - 1}\left[\sum_{k=L/2+1}^{L-1}\sum_{t=0}^{t_p-1}P_b(t,k-L/2)+\sum_{k=0}^{L/2}\sum_{t=0}^{t_p-1}P_b(t,k)-P_b(0,0)\right]. \tag{2.38}$$

Note that pilot symbols do not contribute to the BER of the OFDM resource block and are thus excluded for BER analysis.

2.5.2 BER in the Absence of a Multi-Tone Pilot Jammer

In the absence of the multi-tone jammer we have $\sigma_J^2 = 0$. Hence, only the term $\beta'^2_{t,k}$ changes, whereas the rest of the terms remain unchanged and can be computed in the same way as shown in (2.33)-(2.38).

This BER derivation can be extended to other modulation formats, such as QAM and higher order PSK [32], [33]. This is beyond the scope of the paper. Note, however that the correlation coefficients $\alpha_{t,k}, \beta_{t,k}, \beta'_{t,k}$ necessary for the BER calculations will remain the same for all these modulation formats.

2.5.3 Numerical Results

This subsection presents the validation of the accuracy of the derived BER expressions in the presence and absence of a synchronous multi-tone jammer. Table 2.2 summarizes the parameters of the OFDM resource block. We define the JSR to be the ratio between the received interference power and the received signal power on a target RE.

Figures 2.7, 2.8 and 2.9 show the theoretical and simulated performance of QPSK-OFDM in the case of a synchronous multi-tone pilot jammer, for $(\tau_{rms}, f_d) = (200\,\text{ns}, 100\,\text{Hz})$, $(\tau_{rms}, f_d) = (400\,\text{ns}, 200\,\text{Hz})$ and $(\tau_{rms}, f_d) = (900\,\text{ns}, 500\,\text{Hz})$ respectively. We have chosen these parameters in order to observe the accuracy of the derived expressions in (a) low frequency selectivity and mobility, (b) moderate frequency selectivity and mobility and (c) high frequency selectivity and mobility wireless channels. The theoretical and simulated BER curves closely match, thus validating the analysis presented in section 2.5.1. Note that the high inter-carrier interference (ICI) [31] results in a slight mismatch between theoretical and simulated BER curves at higher values of E_b/N_0, for higher f_d values.

Thus, it is clear from these figures that a synchronous pilot jammer causes massive degradation in BER at higher values of E_b/N_0 as well. Thus, it is a very effective attack that makes the jammer more energy-efficient. Once the BER increases beyond a value of 0.25, error correction codes of the system become ineffective. Thus, assuming that denial of service is caused for $BER > 0.25$, we see that the jammer can cause denial of service with a JSR of about $5\,\text{dB}$ for all values of E_b/N_0. This means that if the jammer perfectly localizes its power to the pilot locations of the target OFDM signal, it can cause denial of service with $2 \times 10^{0.5}/(6 \times 8) = 0.132$ or $\sim 9\,\text{dB}$ less power than the target signal for the parameters in Table 2.2. In general, if $1/\eta$ is the pilot density (number of pilots per OFDM block) and JSR (dB) the Jammer to Signal ratio of the *synchronous pilot jammer*, then the jammer requires a fraction ρ of the target OFDM signal power which can be computed using

$$\rho = \frac{10^{\frac{JSR(dB)}{10}}}{\eta}, \tag{2.39}$$

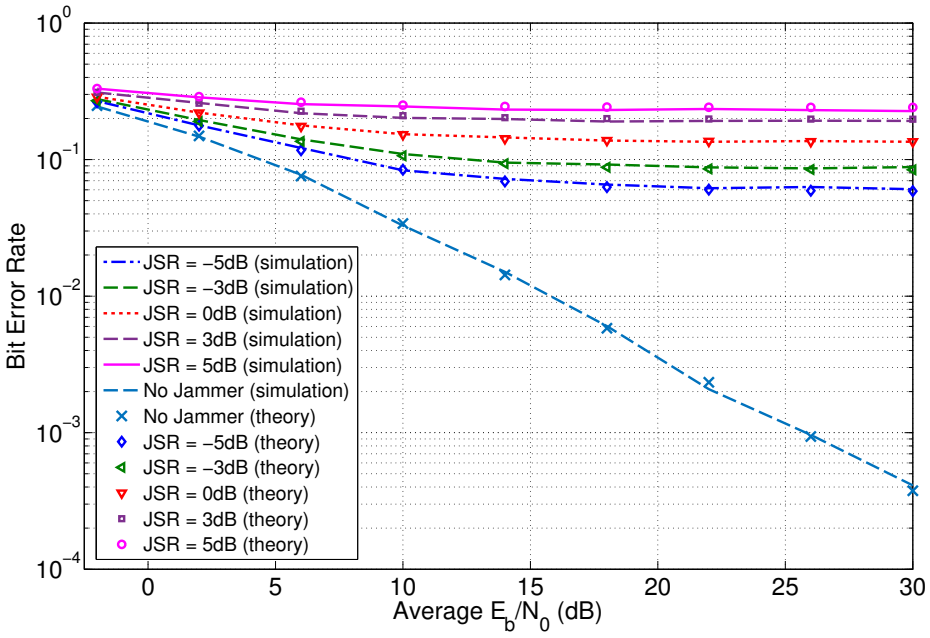

Figure 2.7: Theoretical and simulated BER performance of QPSK-OFDM for $f_d = 100\,\mathrm{Hz}$, $\tau_{rms} = 200\,\mathrm{ns}$,in the case of a synchronous pulsed multi-tone pilot jammer.

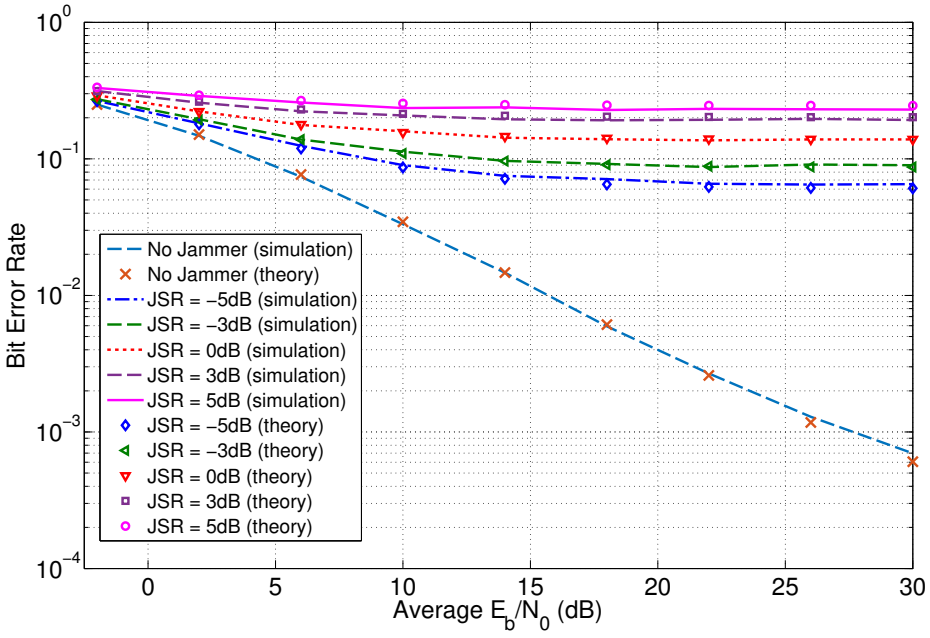

Figure 2.8: Theoretical and simulated BER performance of QPSK-OFDM for $f_d = 200\,\mathrm{Hz}$, $\tau_{rms} = 400\,\mathrm{ns}$,in the case of a synchronous pulsed multi-tone pilot jammer.

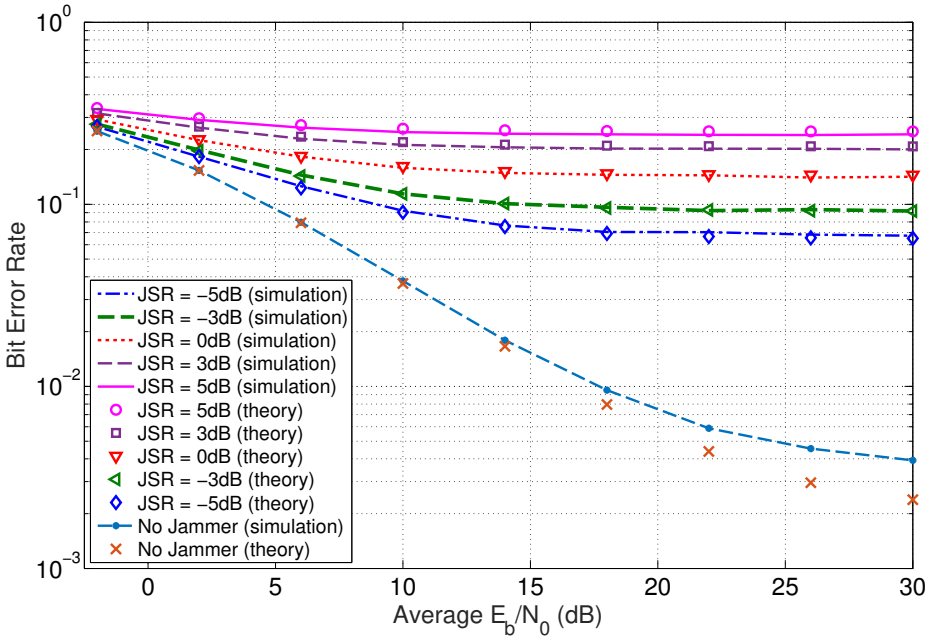

Figure 2.9: Theoretical and simulated BER performance of QPSK-OFDM for $f_d = 500\,\text{Hz}$, $\tau_{rms} = 900\,\text{ns}$, in the case of a synchronous pulsed multi-tone pilot jammer.

since the jammer transmits a power $JSR\ (dB)$ higher than that of the victim signal at pilot locations. Hence, ρ is *analogous to the overall average Signal to Interference Ratio (SIR)* at the receiver, which depends on the sparsity of the pilots $(1/\eta)$. The sparser the pilot density, the lower will be the value of ρ. Table 2.3 shows the relation between ρ and JSR for the simulation parameters in Table 2.2.

Table 2.3: Relationship between JSR (dB) and ρ.

JSR (dB)	ρ^*	ρ^* (dB)
-5	0.0132	-18.8021
-3	0.0209	-16.8021
0	0.0417	-13.8021
3	0.0831	-10.8021
5	0.1318	-8.8021

* assuming that the transmitter and jammer are located equidistant from the victim receiver. ρ will vary if the distances are different.

2.6 Conclusions

In this chapter, we derived the expressions for the MSE of the linear interpolation-based channel estimation and the BER for QPSK-OFDM. We derived these expressions using the WSSUS channel approximation, to model the system performance accurately, both in the presence and absence of a multi-tone pilot jammer.

These derivations and its validation through numerical simulations demonstrate that synchronous multi-tone pilot jamming is a very effective attack that can potentially cause DoS by transmitting a total of only about 10% of the power w.r.t. that of the OFDM transmitter in most cases. This power requirement will reduce for smaller pilot densities, making synchronous pilot jamming a threat to consider when the jammer is sophisticated. It is to be noted that reactive jamming would be necessary in order to carry out these attacks in practice, since the jammer needs to know exactly when the target is receiving the downlink OFDM blocks.

The primary factor causing the performance degradation is corrupted channel estimates and hence, can be countered by first restoring the channel estimation performance in the presence of the pilot jammer. These approaches are the focus of the next chapter.

Chapter 3

Mitigation of Multi-Tone Pilot Jamming in SISO and MIMO-OFDM

3.1 Background

Multi-tone pilot jamming, unlike other types of interference, spreads the effect of localized interference on the pilot REs to adjacent data REs by spoofing the channel estimation and equalization. Hence, degradation of performance to reach the point of Denial of Service (DoS), can be achieved with lesser powers w.r.t. wideband barrage jamming when pilot signals are targeted. In order to mitigate the multi-tone pilot jammer, firstly we would need to restore channel estimation performance in the presence of the jammer, which is the central goal of the work presented in this chapter.

For narrow-band interference on pilots, Han et al. [10] proposed a jammed pilot detection and excision algorithm to mitigate the narrow-band jammer. However, a narrowband jammer will have a limited impact on the target's throughput, because the system can still operate by not scheduling users on the affected resource elements. To cause DoS, multiple pilots of the OFDM block will need to be targeted.

Clancy [7, 8] analyzes pilot tone jamming and nulling and proposes pilot-tone randomization as a technique to evade the jammer. However, randomizing pilot tone locations leads to sub-optimal OFDM performance in the absence of a jammer [25] and requires higher layer protocols to communicate the pilot patterns to legitimate users, which makes initial access to the cell a time-consuming procedure.

Mitigation of pilot jamming in spatial multiplexing MIMO systems becomes challenging, as it would require channel estimation between each transmit antenna - receive antenna pair. In traditional beamforming systems, canceling out interference by null-steering or beam-steering using multiple antennas is possible because of the presence of a single spatial stream on all transmit

antennas [34, 35]. Mitigation of pilot jamming using beamforming algorithms is not possible in the case of spatial multiplexing, because it involves transmission of independent streams of data from each antenna. Moreover it is even more challenging due to the fact that the pilot jammer degrades Channel State Information (CSI) at the target, which are central to achieving capacity enhancements promised by spatial multiplexing.

Yan et al. [36] present a MIMO-based anti-jamming scheme utilizing MIMO interference cancellation and transmit precoding. They implement jammer cancellation using iterative jammer and transmitter channel tracking in the case of a reactive jammer. This solution comes at the cost of losing one spatial degree of freedom.

Sodagari et al. [37] propose randomizing pilot locations to mitigate pilot jamming in MIMO scenarios, in a similar manner as proposed in [7, 8]. Cole et al. [13] propose a new method of designing a MIMO antijamming communications system called 'Spatial Hiding Antijamming', which relies on making the transmit precoding vector orthogonal to the jammer channel matrix. The use of transmit precoding methods to mitigate the multi-tone pilot jammer is difficult to implement for broadcast pilot jamming, where each affected user will potentially need a different precoding matrix, in addition to perfect CSI to mitigate the pilot jammer. Most current wireless standards allow for choice of precoding matrices from a finite-sized codebook.

The aim of this chapter is to present and analyze methods that can restore channel estimation performance in the presence of a multi-tone pilot jammer for both SISO- and MIMO-OFDM case. In our proposed jammer mitigation algorithms for a SISO-OFDM system, we seek to preserve the optimal pilot configuration that minimizes the MSE [25]. For MIMO-OFDM systems, our focus is on methods that can achieve full rank spatial multiplexing in the presence of the jammer. We show that it is possible to mitigate a power-constrained multi-tone pilot jammer with little to no intervention from the base station.

Section 3.2 describes the most common jamming strategies, and outlines our definition of a *power-constrained pilot jammer*. Section 3.3 provides a brief overview about the detection of pilot jamming. Section 3.4 presents our proposed algorithms to mitigate the pilot jammer, its performance, and highlights the applicability of these methods in LTE. Section 3.5 presents a brief overview of spatial multiplexing in MIMO-OFDM, the jammer model, an approximate channel estimation algorithm to mitigate the power-constrained pilot jammer and its performance results. Section 3.6 concludes the chapter with a summary of the main results.

3.2 Types of Multi-Tone Pilot Jammers

The multitone pilot jammer can have power allocation strategies with varying levels of sophistication. The jammer can transmit continuously, or can allocate power based on its knowledge of the downlink signal [38]. In this work, we consider two broad classes of jammer strategies:

1. *Continuous Asynchronous Jammer*: Requires knowledge of the pilot subcarrier indices only.

Since it is an asynchronous continuous transmission, the jammer has less complexity, but lower energy efficiency.

2. *Pulsed Synchronous Jammer*: Requires tight synchronization with the target's receiver, but provides high energy efficiency at the cost of jammer complexity.

As discussed before, we consider power-constrained multi-tone pilot jammers in this work. The aim of such a jammer is to maximize its power efficiency while being constrained to the strategy it chooses to use.

Definition 3.1. A Power-constrained jammer

1. Transmits on all possible pilot subcarriers continuously at a *lower data rate than the target signal*, in the case of an asynchronous jammer.

2. Transmits only on pilot locations of the OFDM grid, in the case of a synchronous jammer. This is straightforward for SISO-OFDM, but it becomes slightly complicated for MIMO-OFDM where some pilot locations might be adjacent to each other. In this case, the jammer would need to transmit its modulation symbols at a *lower data rate* as compared to the target OFDM signal.

The reasoning for such a definition for the asynchronous jammer is as follows. If the asynchronous jammer intends to be power efficient, it needs to make sure that all of it power is aligned with pilot subcarriers. A potential issue with modulation symbols is spectral leakage of power into adjacent subcarriers. Spectral leakage can be minimized if the jammer has a lower symbol rate on each targeted subcarrier, than the target OFDM signal [39]. In addition to pulse shape and modulation of jammer data symbols, jammer mobility results in inter-carrier interference at the target receiver, as a result of shift in jammer spectra w.r.t. the pilot subcarrier due to Doppler. Hence, strong power localization on the pilot locations in a fast fading wireless channel is possible with lower data rates for the jammer digital modulated signal w.r.t. the target OFDM symbol.

Traditionally, narrowband interference is mitigated either by Interference Cancellation (IC) or jammer evasion strategies. Since multi-tone pilot jamming in OFDM consists of multiple narrowband signals, we propose two strategies to mitigate it for SISO scenarios: resource element blanking with interference cancellation and jammer evasion by cyclic shifting of pilot locations.

3.3 Detection of Pilot Jamming

Before mitigating pilot jamming, it is necessary to detect that the jamming has occurred. There are various types of detectors with varying complexities from simple energy detection [10] to sophisticated interference detection with modulation classification algorithms [40]. The methods presented in this chapter result in little to no degradation in the case of a false negative during the

jammer detection process. The rest of this chapter assumes that presence of the jammer on pilot tones is detected using any of the methods available in the literature. The focus of this chapter is more on interference-aware pilot jamming mitigation, rather than the detection of pilot jamming itself.

When it comes to wireless standards, a lot of channel quality parameters can be utilized to detect the presence of the pilot jammer. For the 3GPP LTE standard, these parameters include Channel Quality Indicator (CQI), Reference Signal Received Power (RSRP), Reference Signal Received Quality (RSRQ) and Received Signal Strength Indicator (RSSI) [41]. A description of few of these parameters will be discussed with more details in chapter 4.

3.4 Anti-Jamming for SISO-OFDM Systems

3.4.1 Resource Element Blanking with Interference Cancellation

Asynchronous multi-tone pilot jamming is simple to implement and would be suitable for jammers that do not have very tight power constraints. For this type of jammer we propose resource element blanking with interference cancellation as illustrated in Figure 3.1.

Suppose that a pilot symbol is carried over the l^{th} subcarrier during time interval n and that the l^{th} subcarrier is jammed over all OFDM symbols. The channel estimate $\tilde{H}_l[n]$ based on resource element blanking and interference cancellation can be obtained as

$$\tilde{H}_l[n] = H_l[n] + \frac{H'_l[n]J_l[n] - H'_l[n+1]J_l[n+1]}{P_l[n]} + \frac{(w_l[n] - w_l[n+1])}{P_l[n]}. \tag{3.1}$$

The underlying assumption here is that the channels and the jamming signal remain constant over the two consecutive OFDM symbols; that is, $H'_l[n] \approx H'_l[n+1]$ and $J_l[n] = J_l[n+1]$ due to definition 3.1. In practice, the channel estimation and BER performance depends on the relative mobility between the jammer and the target receiver. Higher mobility leads to lower temporal correlation, thus resulting in slightly degraded performance of the proposed approach. In either case, because $(w_l[n] - w_l[n+1]) \sim \mathcal{CN}(0, 2\sigma_w^2)$, this method enhances the additive complex Gaussian noise component on the pilot and reduces its average SNR per bit (E_b/N_0) by at least $3\,\mathrm{dB}$. Implementation of this approach in the 3GPP LTE standard is simple, because of the in-built blanking of REs adjacent to reference signal locations on all antenna ports to support MIMO operation [42].

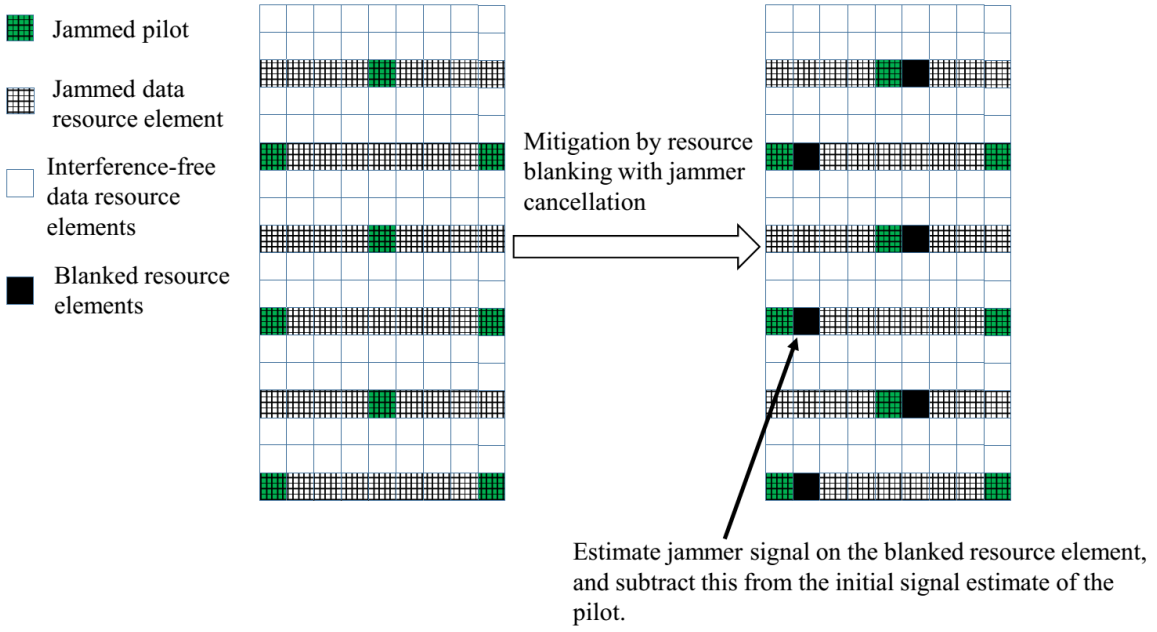

Figure 3.1: Mitigation of asynchronous multi-tone pilot jamming by resource element blanking with interference cancellation.

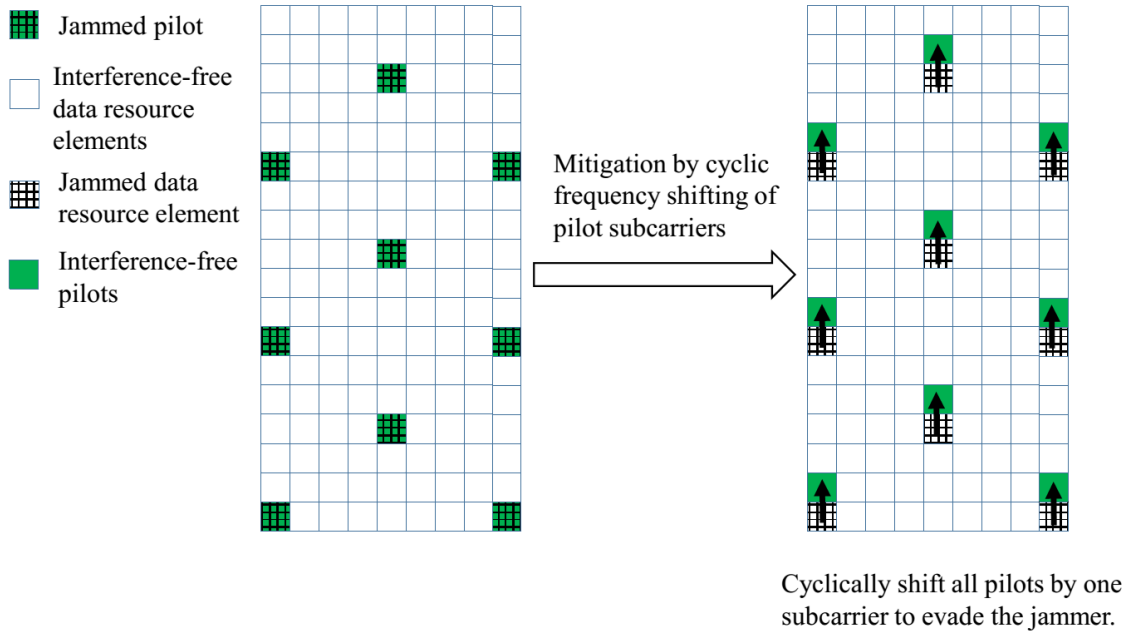

Figure 3.2: Mitigation of synchronous multi-tone pilot jamming by cyclic frequency shifting of pilot locations.

3.4.2 Cyclic Frequency Shifting of Pilot Locations

Interference cancellation is impossible without the knowledge of the jammer characteristics. If the jammer perfectly synchronizes with the receiver, and localizes its power on the pilot locations of the OFDM grid, tracking the jammer signal for cancellation becomes very hard in practice. In this case, the receiver can coordinate with the transmitter to cyclically shift all the pilot locations by one or more subcarriers to evade the jamming signal, as illustrated in Figure 3.2.

This feature is present in the 3GPP LTE/LTE-A standard where a cell-specific frequency shift is applied to the pilot locations based on a cell parameter, called the physical cell identity (PCI) of the network [42]. This mitigation strategy can be used with dynamic PCI planning approaches [43], to make provisions in the protocol for future releases of LTE to protect it against targeted interference. The advantage of this approach is that it would maintain optimal channel estimation performance due to equal pilot spacing in time and frequency [25], even in the presence of a multi-tone pilot jammer. This method is more suitable for cases where it is not feasible to use interference cancellation procedures to mitigate the pilot interference. However, the network implications of dynamic shifting of pilot locations in a cell need more analysis for network-wise solutions.

3.4.3 Numerical Results

Here we analyze the effectiveness of the proposed mitigation strategies. The simulation parameters are summarized in Table 2.2. We assume that the channels between the base station to the receiver, and jammer to the receiver have the same Doppler and rms delay spreads f_d and τ_{rms}. We compare the of the channel estimation and the BER performance in the following scenarios:

1. Synchronous and asynchronous multi-tone pilot jamming with no mitigation,
2. Asynchronous multi-tone pilot jamming with resource element blanking and jammer cancellation (JC),
3. Synchronous multi-tone pilot jamming with cyclic shifting of pilot locations,
4. No jammer.

We assume that the power allocated to pilot REs and data REs in the OFDM signal are the same. It is important to note that even though the jamming duration varies for an asynchronous pilot jammer w.r.t. a synchronous pilot jammer, we are interested in the interference power on the pilots. Hence we use the following definition of JSR for comparison between the different jammer strategies.

Definition 3.2. Jammer to Signal Ratio (JSR) is defined as

1. The ratio of jammer power to signal power for each jammed pilot *RE* in the case of a *synchronous multi-tone pilot jammer*.

2. The ratio of jammer power to signal power for each jammed *subcarrier* in the case of an *asynchronous multi-tone pilot jammer*.

Figures 3.3 - 3.5 show the channel estimation performance for all considered scenarios for $(\tau_{rms}, f_d) = (200\,\text{ns}, 100\,\text{Hz})$, $(\tau_{rms}, f_d) = (400\,\text{ns}, 200\,\text{Hz})$ and $(\tau_{rms}, f_d) = (900\,\text{ns}, 500\,\text{Hz})$. Among the two proposed mitigation methods we observe that cyclic shifting of pilot locations performs better than resource element blanking with interference cancellation. This is so because a) the mobility of the jammer with respect to the receiver and b) the noise enhancement due to imperfect noise cancellation result in residual errors that introduces an error floor on the MSE curve. This is pronounced at lower E_b/N_0 where the MSE performance is worse with than without mitigation. The MSE performance with cyclic shifting of pilot location, on the other hand, has the same performance with jamming as without it, thus perfectly restoring the channel estimation performance. Moreover, its performance is independent of the jammer power and thus is applicable for mitigating very high power pilot jammers.

Figures 3.6 - 3.8 illustrate the BER performance, for all considered scenarios for $(\tau_{rms}, f_d) = (200\,\text{ns}, 100\,\text{Hz})$, $(\tau_{rms}, f_d) = (400\,\text{ns}, 200\,\text{Hz})$ and $(\tau_{rms}, f_d) = (900\,\text{ns}, 500\,\text{Hz})$. We see that asynchronous jamming degrades the BER more than synchronous jamming. This behavior is expected because the asynchronous jammer continuously transmits on the pilot subcarrier, resulting in interference on top of some data resource elements, as shown in Figures 3.1 - 3.2. RE blanking with interference cancellation slightly improves the BER performance in the presence of an asynchronous jammer, due to interference on data resource elements, which cannot be mitigated, in addition to the issues of noise enhancement and imperfect jammer interference estimation. Cyclic shifting of pilot locations in the presence of a synchronous pilot jammer improves the BER performance by an order of magnitude and its performance approaches that of a jammer-free scenario. We also observe that higher root mean square delay spread and mobility characteristics of the wireless channel have very little effect on the BER, both in the presence as well as in the absence of our mitigation strategies. This is so because the relatively high interference power of the jammer sets the error floor of the BER curves in all channel scenarios. Therefore, most practical multi-tone pilot jamming scenarios can be analyzed as interference-limited systems.

It is simple to implement RE blanking with jammer cancellation in wireless standards since it does not change the structure of the OFDM block. However, implementing cyclic shifting of pilot locations in general will change the structure of the OFDM block. Therefore, in general,

1. Cyclic shifting of pilot locations maintains the optimal pilot pattern that minimizes the channel estimation MSE.

2. The pilot density before and after the cyclic shift, remains the same.

3. There needs to be a mechanism in the wireless standard to indicate the shift of cyclic locations to legitimate UEs. In LTE, the pilot locations can be altered by changing the cell ID [42].

4. In LTE, the cell IDs are chosen in order to minimize the interference on pilots of once cell from the others [1]. Hence, strategies such as dynamic PCI planning will be necessary to minimize the interference on the pilot signals of all surrounding cells [43].

The proposed mitigation methods help restoring the channel estimation performance in the presence of a multi-tone pilot jammer. However, neither of these mitigation techniques can protect data that is being jammed when the jammer transmits continuously. In this case, additional strategies, such as adaptive modulation and coding, resource blanking, adaptive bit loading and smart resource allocation, are needed to attain low BER values. These techniques alone would not be effective if the pilots are corrupted and cannot be restored in the first place. The protection of pilots is thus of most importance, because if pilots are compromised, the channel estimation and equalization for the data-carrying resource elements would be inaccurate resulting in low performance [7], [8]. Hence, this needs to be seriously addressed for protecting user equipment (UEs) and ensuring that future systems will be more robust.

3.5 Spatial Multiplexing with MIMO-OFDM in the Presence of Multi-Tone Pilot Jamming

3.5.1 Motivation

In the last few decades, wireless communication systems have utilized multiple antennas to accomplish either of the following [44]:

1. Enhance the SNR using antenna diversity.
2. Improve the SINR using a combination of beamforming, beam steering and null steering.
3. Scale the throughput linearly with the number of antennas, using MIMO spatial multiplexing.

Traditionally, interference cancellation has been accomplished by null steering or beam steering [34, 35], which is applicable for multiple antennas tramsmitting a single spatial stream. But in the current market environment and the road towards 5G, wireless carriers are more interested in increasing wireless capacity rather than signal quality exclusively. This is why transmission of multiple data streams using spatial multiplexing has been used to enhance the throughput of the current 4G technologies [1], as compared to its predecessors. It is expected to remain central to the design of the future 5G wireless networks [45]. Moreover, it is inefficient to give up spatial degrees of freedom to cancel out multi-tone pilot jamming, because the interference is sparse and targeted on specific subcarriers/REs of the OFDM blocks.

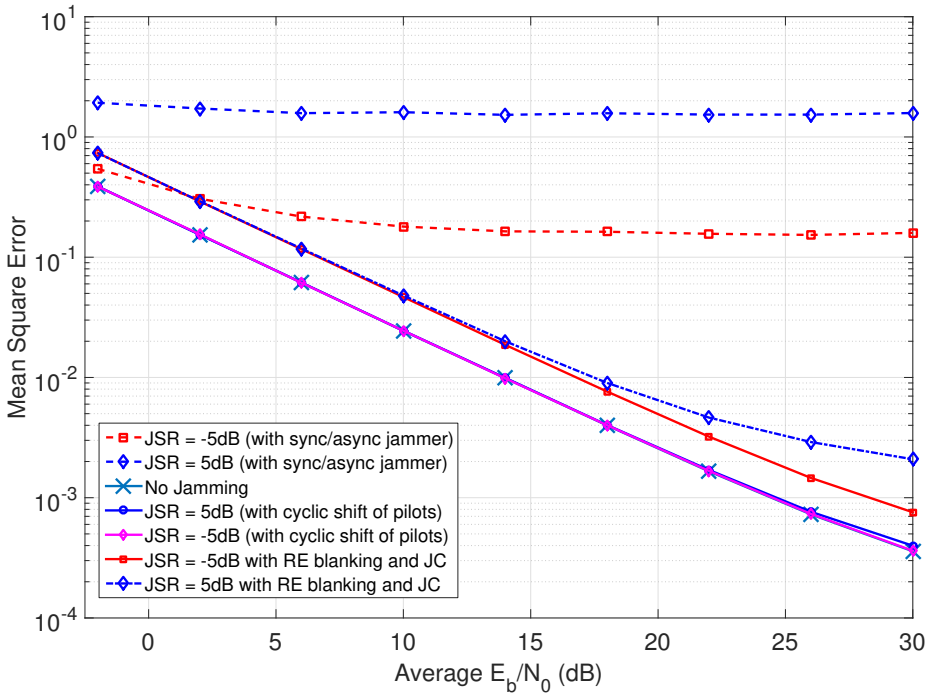

Figure 3.3: Channel Estimation MSE performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$.

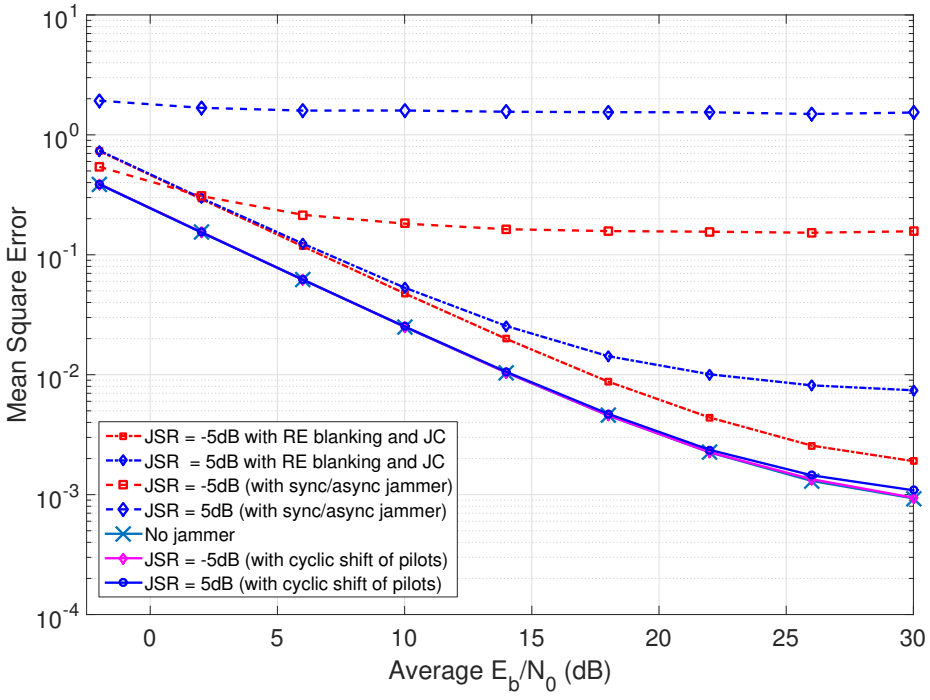

Figure 3.4: Channel Estimation MSE performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 400\,\text{ns}$, $f_d = 200\,\text{Hz}$.

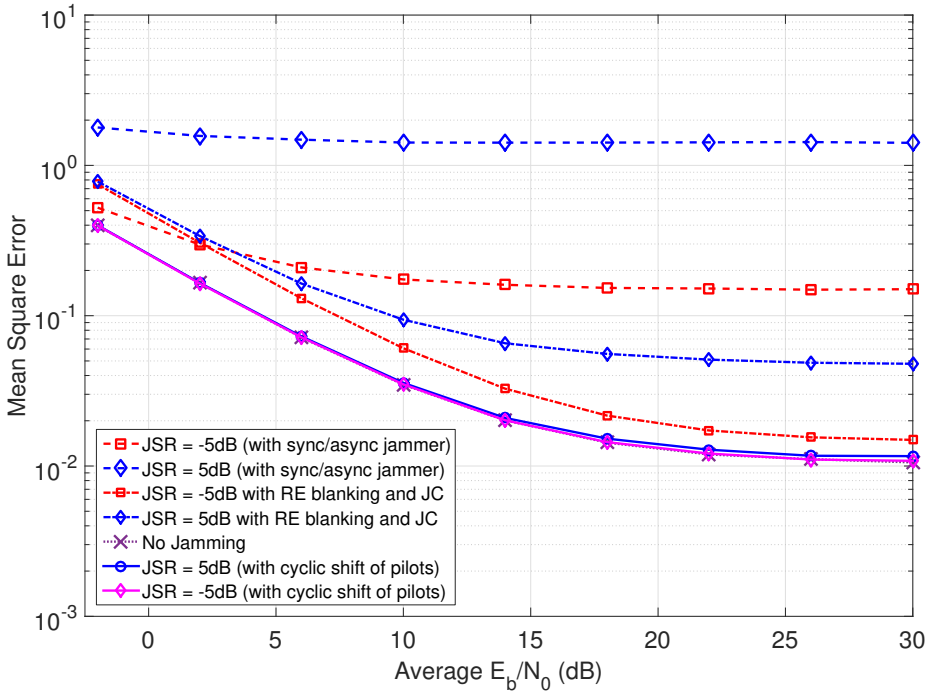

Figure 3.5: Channel Estimation MSE performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 900\,\text{ns}$, $f_d = 500\,\text{Hz}$.

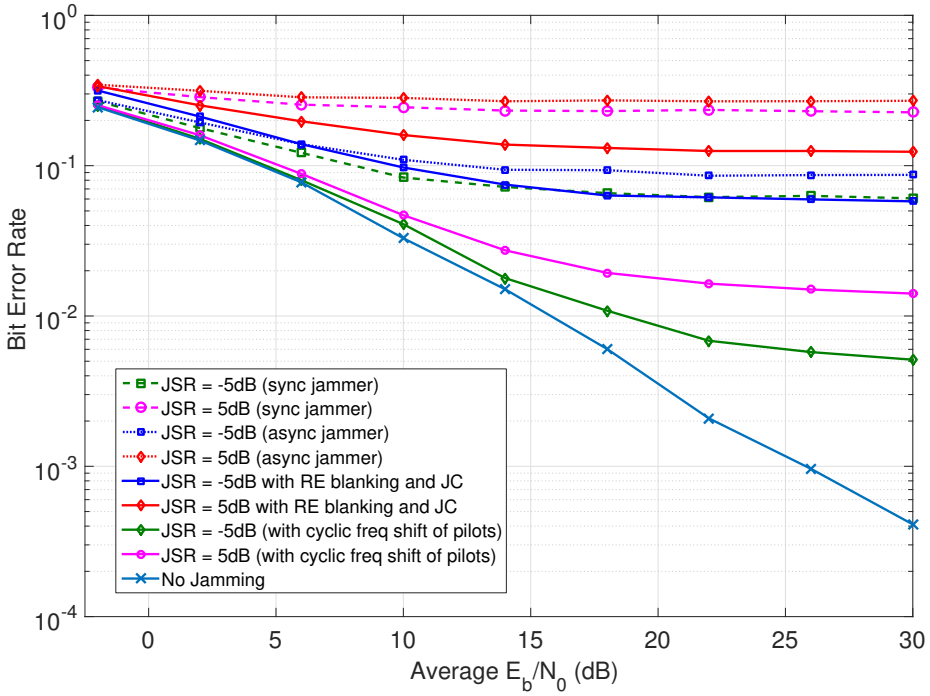

Figure 3.6: Bit Error rate performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$.

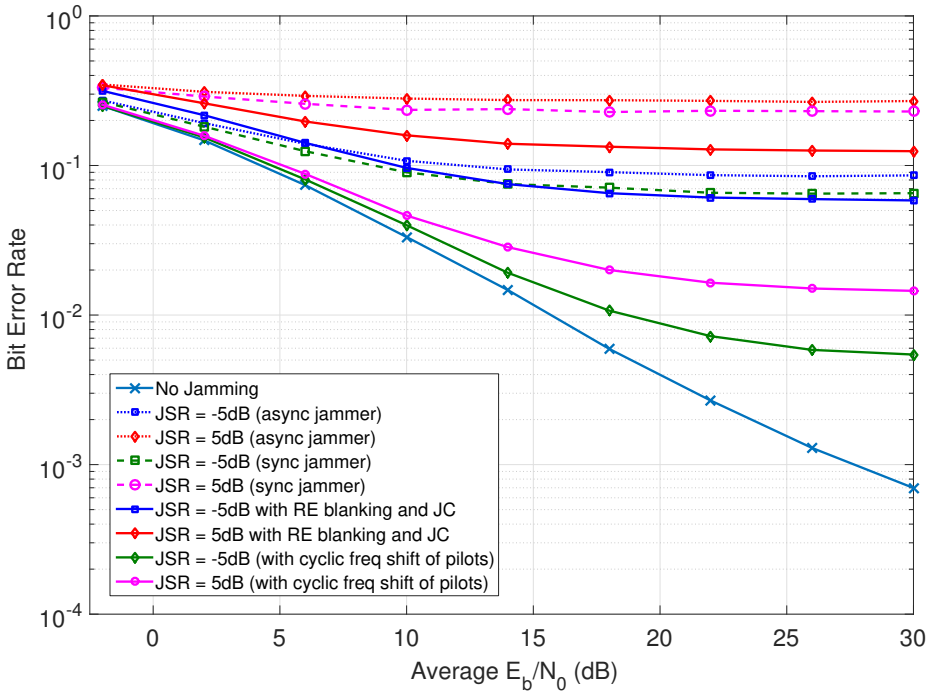

Figure 3.7: Bit Error rate performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 400\,\text{ns}$, $f_d = 200\,\text{Hz}$.

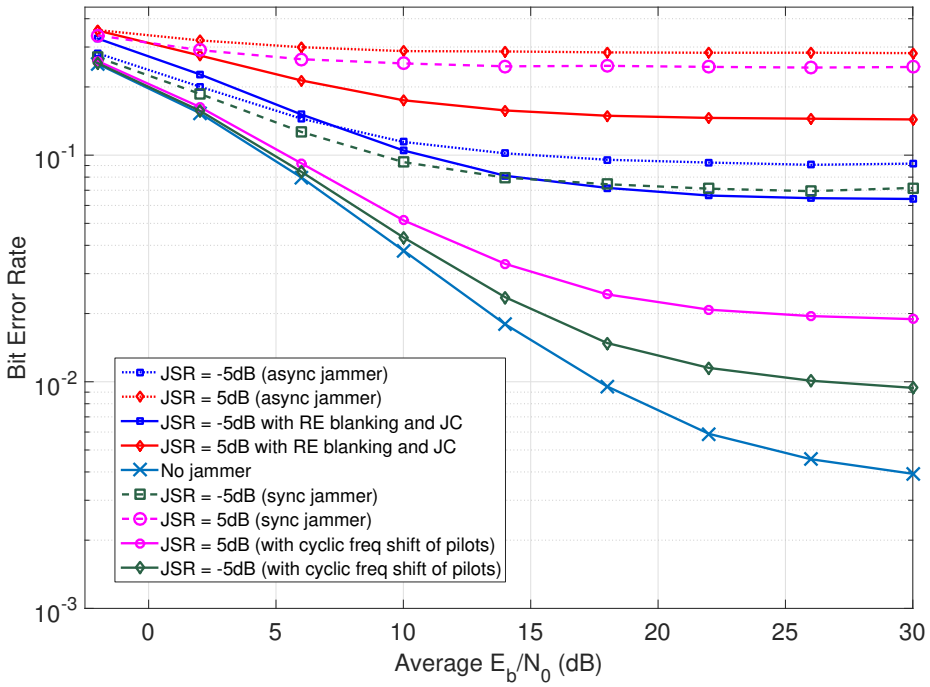

Figure 3.8: Bit Error rate performance of QPSK-OFDM in all considered scenarios, for $\tau_{rms} = 900\,\text{ns}$, $f_d = 500\,\text{Hz}$.

In the areas of MU-MIMO, techniques like precoding have been developed that can null multi-user interference. The authors of [13] have devised a method called *Spatial Hiding Precoding*, where transmit precoding vectors are chosen orthogonal to the channel vector of the jammer (with a single transmit antenna). However, this assumes perfect knowledge of the channels between the jammer and the receiver, and between the transmitter and receiver, which is hard to obtain if a) the jammer is persistently corrupting channel estimates, and b) either of the channels fades fast in a high mobility scenario. In addition, in the case of broadcast pilot jamming the transmit precoding vector will drastically vary for each and every user, which makes its implementation very challenging.

In this section, we show that a power-constrained multi-tone pilot jammer can be mitigated to some extent at each user independently of the other users without any assistance from the base station.

3.5.2 Channel Equalization in MIMO-OFDM

MIMO-OFDM systems use similar pilot-assisted methods as SISO systems to estimate the wireless channel. For $N_t \times N_r$ MIMO system, with N_t and N_r being the number of transmit and receive antennas respectively, equalization would require N_t different pilot patterns, one for each transmit antenna. Prior work [25] has shown equal pilot spacing in time and frequency to be optimal in the MMSE sense. Moreover, diamond-shaped pilots are used in the current 3GPP LTE/LTE-A standard for supporting MIMO operation. We have used a similar pilot pattern for our analysis, which is shown for a 4×4 MIMO-OFDM block in Figure 3.9. The RE nulls are present in the OFDM block of each antenna port to ensure that there is no interference due to antenna j on the pilot locations of transmit antenna port i, for $i \neq j$ and $i, j \leq N_t$. We consider least squares (LS) with linear interpolation as the channel estimator, with a zero forcing (ZF) equalizer [44] at the receiver.

Channel estimation is performed using the pilots from all N_t transmit antennas, using the algorithm presented in equations (2.9) - (2.12) of Section 2.3. After removing the cyclic prefix at the receiver and performing channel estimation, let $\hat{H}_k^{(ji)}[n]$ denote the frequency domain channel estimate for the channel between the i^{th} transmit and j^{th} receive antenna for the k^{th} subcarrier of the n^{th} OFDM symbol. The corresponding frequency domain channel coefficient is denoted by $\hat{H}_k^{(ji)}[n]$. The most important notations are summarized in Table 3.1

The overall MIMO-OFDM system can be represented by

$$\mathbf{Y}_k[n] = \mathbf{H}_k[n]\mathbf{X}_k[n] + \mathbf{W}_k[n], \tag{3.2}$$

where $\mathbf{Y}_k[n]$ is a $N_r \times 1$ vector denoting the received data vector, given by

$$\mathbf{Y}_k[n] = \begin{bmatrix} Y_k^{(1)}[n] & Y_k^{(2)}[n] & \cdots & Y_k^{(N_r)}[n] \end{bmatrix}^T. \tag{3.3}$$

The superscript $(.)^{(j)}$ refers to the index of the receive antenna and $[.]^T$ the matrix transpose, for

Table 3.1: Important Symbols and Notation

Variable	Domain†	Description
N_t	$\mathbb{Z}^+$	Number of transmit antennas
N_r	$\mathbb{Z}^+$	Number of receive antennas
$\mathbf{Y}_k[n]$	$\mathbb{C}^{N_r \times 1}$	Received data vector at the k^{th} subcarrier of the n^{th} OFDM symbol
$Y_k^{(j)}[n]$	$\mathbb{C}$	Received data at the j^{th} receive antenna on the k^{th} subcarrier of the n^{th} OFDM symbol, for $1 \leq j \leq N_r$
$\mathbf{X}_k[n]$	$\mathbb{M}^{N_t \times 1}$	Transmitted data vector at the k^{th} subcarrier of the n^{th} OFDM symbol
$X_k^{(i)}[n]$	$\mathbb{M}$	Transmitted data at the i^{th} transmit antenna on the k^{th} subcarrier of the n^{th} OFDM symbol, for $1 \leq i \leq N_t$
$\mathbf{H}_k[n]$	$\mathbb{C}^{N_r \times N_t}$	Channel matrix at the k^{th} subcarrier of the n^{th} OFDM symbol
$\hat{\mathbf{H}}_k[n]$	$\mathbb{C}^{N_r \times N_t}$	Estimated channel matrix at the k^{th} subcarrier of the n^{th} OFDM symbol
$\hat{H}_k^{(ji)}[n]$	$\mathbb{C}$	Estimated channel between the i^{th} transmit and the j^{th} receive antenna at the k^{th} subcarrier of the n^{th} OFDM symbol
$\mathbf{W}_k[n]$	$\mathbb{C}^{N_r \times 1}$	complex AWGN vector at the k^{th} subcarrier of the n^{th} OFDM symbol
σ_w^2	$\mathbb{R}$	Noise power
$W_k^{(j)}[n]$	$\mathbb{C}$	complex AWGN at the j^{th} receive antenna on the k^{th} subcarrier of the n^{th} OFDM symbol. $W_k^{(j)}[n] \sim \mathcal{N}(0, \sigma_w^2)$ for $1 \leq j \leq N_r$.
$H_k^{(j)'}[n]$	$\mathbb{C}$	Channel coefficient between the jammer and the j^{th} receive antenna of the target receiver on the k^{th} subcarrier of the n^{th} OFDM symbol, for $1 \leq j \leq N_r$.
$J_k[n]$	$\mathbb{C}$	Transmitted jammer symbol on the k^{th} subcarrier of the n^{th} OFDM symbol.

† $\mathbb{Z}^+$ denotes the set of all positive integers, $\mathbb{C}^{m \times n}$ denotes the set containing all possible $m \times n$ complex matrices, $\mathbb{R}^{m \times n}$ denotes the set containing all possible $m \times n$ matrices with real elements, $\mathbb{M}^{N_t \times 1}$ denotes a $N_t \times 1$ column vector containing modulation alphabets (we assume QPSK modulation in this chapter).

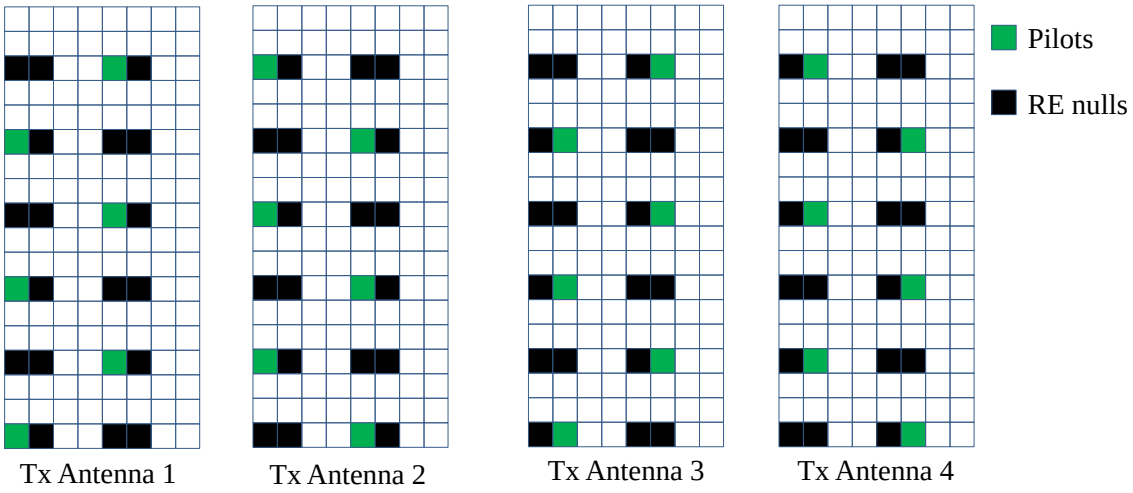

Figure 3.9: Diamond-shaped pilot pattern for 4×4 MIMO-OFDM.

$1 \leq j \leq N_r$. $\mathbf{X}_k[n]$ is a $N_t \times 1$ vector of the modulation symbols, given by

$$\mathbf{X}_k[n] = \begin{bmatrix} X_k^{(1)}[n] & X_k^{(2)}[n] & \cdots & X_k^{(N_t)}[n] \end{bmatrix}^T, \tag{3.4}$$

where the superscript $(.)^{(i)}$ refers to the index of the transmit antenna of the transmitter, for $1 \leq i \leq N_t$. $\mathbf{W}_k[n]$ is the $N_r \times 1$ vector denoting the complex AWGN component of the received signal, given by

$$\mathbf{W}_k[n] = \begin{bmatrix} w_k^{(1)}[n] & w_k^{(2)}[n] & \cdots & w_k^{(N_r)}[n] \end{bmatrix}^T, \tag{3.5}$$

where the superscript $(.)^{(j)}$ refers to the index of the receive antenna, for $1 \leq j \leq N_r$. $\mathbf{H}_k[n]$ is the $N_r \times N_t$ channel matrix, which is estimated by the LS/linear interpolation method presented in Section 2.3. The estimated channel matrix $\hat{\mathbf{H}}_k[n]$ can be written as

$$\hat{\mathbf{H}}_k[n] = \begin{bmatrix} \hat{H}_k^{(11)}[n] & \hat{H}_k^{(12)}[n] & \cdots & \hat{H}_k^{(1N_t)}[n] \\ \hat{H}_k^{(21)}[n] & \hat{H}_k^{(22)}[n] & \cdots & \hat{H}_k^{(2N_t)}[n] \\ \vdots & \vdots & \ddots & \vdots \\ \hat{H}_k^{(N_r1)}[n] & \hat{H}_k^{(N_r2)}[n] & \cdots & \hat{H}_k^{(N_rN_t)}[n] \end{bmatrix}. \tag{3.6}$$

The ZF equalizer inverts the effect of the channel by multiplying the received data vector $\mathbf{Y}_k[n]$ with the left pseudo-inverse of the estimated channel matrix $\hat{\mathbf{H}}_k[n]$

$$\begin{aligned} \hat{\mathbf{X}}_k[n] &= (\hat{\mathbf{H}}_k[n])^\dagger \mathbf{Y}_k[n] \\ &= (\hat{\mathbf{H}}_k[n])^\dagger \mathbf{H}_k[n]\mathbf{X}_k[n] + (\hat{\mathbf{H}}_k[n])^\dagger \mathbf{W}_k[n], \end{aligned} \tag{3.7}$$

where $\hat{\mathbf{X}}_k[n]$ is a $N_t \times 1$ vector denoting the estimated transmitted symbols. The pseudo-inverse matrix $(\hat{\mathbf{H}}_k[n])^\dagger$ is given by

$$(\hat{\mathbf{H}}_k[n])^\dagger = [(\hat{\mathbf{H}}_k[n])^H \hat{\mathbf{H}}_k[n]]^{-1} (\hat{\mathbf{H}}_k[n])^H, \tag{3.8}$$

where $(.)^H$ denotes the Hermitian-transpose operation. Equation (3.7) is applied for $0 \leq k \leq N-1$, $1 \leq i \leq N_t$, $1 \leq j \leq N_r$ and all OFDM symbol indices n. Further detection and decoding processes are carried out to recover N_t distinct spatial data streams from the transmitter.

3.5.3 Multi-Tone Pilot Jamming Model for MIMO-OFDM

At the receiver, the OFDM blocks on each antenna have the pattern shown in Figure 3.10. In the rest of this section, we consider a synchronous multi-tone pilot jammer with a single transmit antenna, which transmits only on the time-frequency locations of the MIMO-OFDM grid where all the pilots are located. As evident from Figure 3.9, the same pilot pattern will be used by all the N_r receive antennas for channel estimation. Hence, the jammer interferes with all the receive antennas by targeting the pilot locations of all N_t transmit antennas. We assume that the jammer is unaware of the channel between the itself and the receiver, in which case equal power allocation is optimal to degrade the Bit Error Rate at the receiver [46]. This strategy is applicable in broadcast pilot jamming where the jammer aims to interfere with all receivers of the cell.

In order to minimize spectral leakage of its power, it is beneficial to have a lower symbol rate on each subcarrier than the target OFDM signal, as explained in Definition 3.1. The jammer's transmitted symbols across different subcarriers can vary, even though it has been shown that transmitting the same sequence across all pilots causes more damage to the receiver post-equalization SINR [21]. This can also be inferred from the BER and MSE analysis presented in Chapter 2. If the jamming signal on one pilot location is correlated with that on every other pilot, then $\mathbb{E}\big[J_l[n] J_k^*[m]\big] > 0$ for $n \neq m$ or $k \neq l$, which results in higher MSE and BER values.

To summarize, the main assumptions about the pilot jammer are

1. The jammer has a single transmit antenna.
2. The jammer transmits only on the exact time-frequency locations of the target OFDM blocks.
3. Symbols transmitted by the jammer remain constant over adjacent OFDM symbols on the same subcarrier.
4. The jammer transmits equal power on all the pilot locations.

We now present a channel estimation algorithm to mitigate this jammer. This algorithm does not sacrifice full rank spatial multiplexing operation even in the presence of a power-constrained synchronous multi-tone pilot jammer.

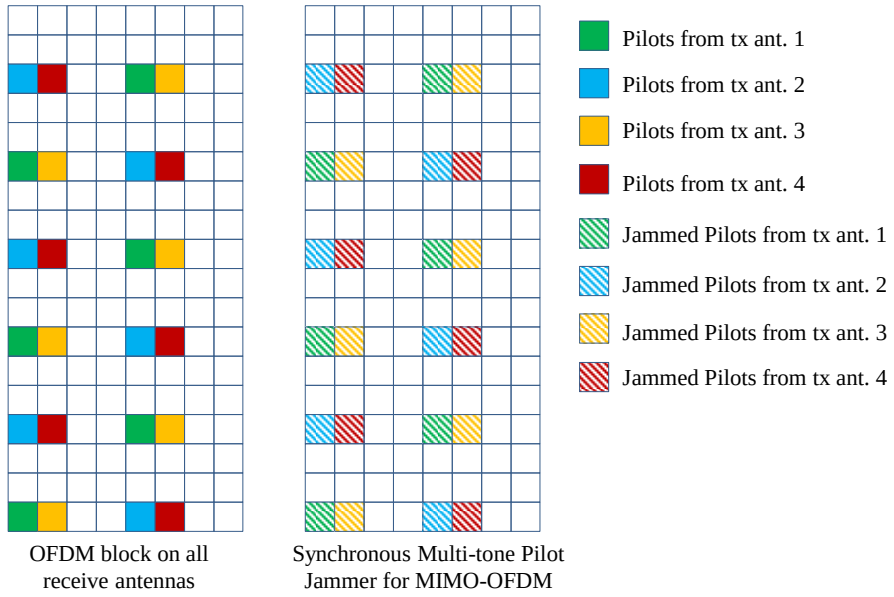

Figure 3.10: Illustration of synchronous multi-tone pilot jamming in a 4×4 MIMO-OFDM block, for all spatial layers.

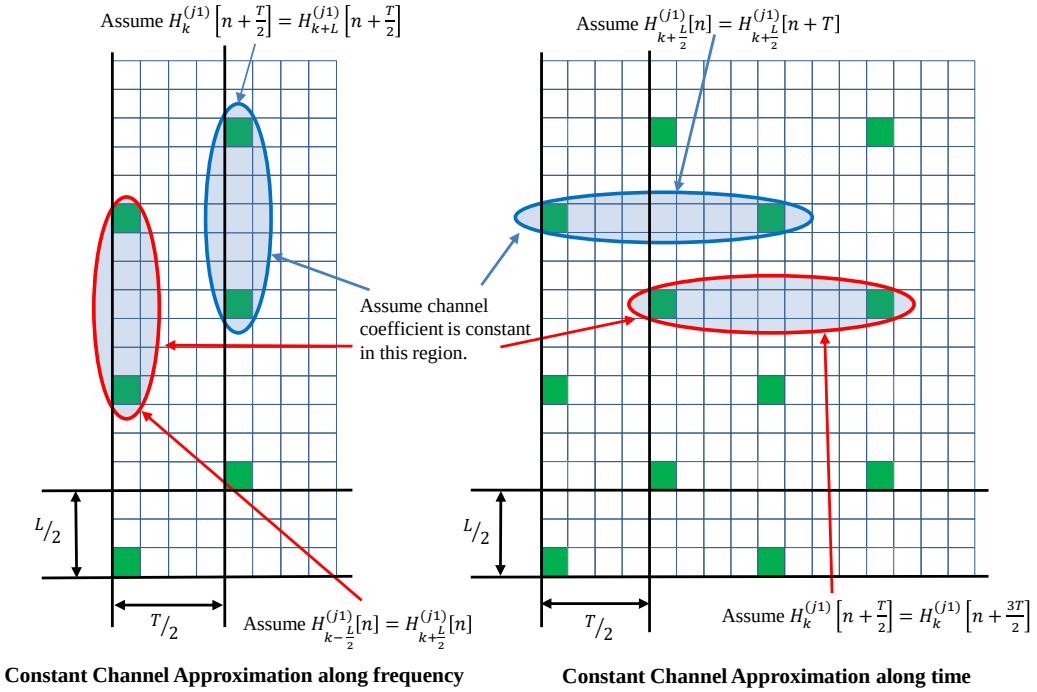

Figure 3.11: Schematic of the Constant Channel Approximation (COCHAP) assumption for pilots from transmit antenna 1 for $j = 1, 2, 3, 4$.

3.5.4 Constant Channel Approximation (COCHAP) with Jammer Cancellation

Wireless communications have become more reliable over the last few decades due to pioneering research carried out on Turbo codes, LDPC codes and Hybrid Automatic Repeat Request (HARQ) [1], among others. The presence of such schemes in the current wireless standards [42] gives us some flexibility to relax some of the accuracy requirements of the channel estimation and equalization procedures at the receiver.

In the proposed method, we relax the condition that the frequency domain channel coefficients vary with time and frequency over a small set of neighboring REs. Figure 3.11 illustrates the Constant Channel Approximation (COCHAP) method. Applying COCHAP along the frequency axis in the same OFDM symbol is appropriate for low root mean square delay spread wireless channels. The COCHAP can be used along the time axis as well, which is applicable for low mobility wireless channels. Even though it is an approximation and does not hold for general channel conditions, we use it as a starting point for jammer mitigation while performing spatial multiplexing. We describe the algorithm for the 4×4 MIMO-OFDM block shown in Figure 3.9. However, the method can be applied to other values of N_t by designing pilot patterns and/or nulls appropriately, to facilitate cancellation as described below.

The multi-tone pilot jammer is assumed to have a single transmit antenna. Let $H_k^{(j)'}[n]$ denote the frequency domain channel coefficient between the jammer and the j^{th} receive antenna of the targeted receiver at subcarrier k of the n^{th} OFDM symbol, $J_k[n]$ denote the corresponding jammer symbol. For the pilots on transmit antennas 1 and 3, the OFDM symbols received on the j^{th} receive antenna of the receiver will be

$$Y_k^{(j)}[n] = H_k^{(j1)}[n]P_k^{(1)}[n] + H_k^{(j)'}[n]J_k[n] + w_k^{(j)}[n], \tag{3.9}$$

$$Y_k^{(j)}[n+1] = H_k^{(j3)}[n+1]P_k^{(3)}[n+1] + H_k^{(j)'}[n+1]J_k[n+1] + w_k^{(j)}[n+1], \tag{3.10}$$

$$Y_{k+L}^{(j)}[n] = H_{k+L}^{(j1)}[n]P_{k+L}^{(1)}[n] + H_{k+L}^{(j)'}[n]J_{k+L}[n] + w_{k+L}^{(j)}[n], \tag{3.11}$$

$$Y_{k+L}^{(j)}[n+1] = H_{k+L}^{(j3)}[n+1]P_{k+L}^{(3)}[n+1] + H_{k+L}^{(j)'}[n+1]J_{k+L}[n+1] + w_{k+L}^{(j)}[n+1], \tag{3.12}$$

where $X_k^{(i)}[n] = P_k^{(i)}[n]$ correspond to the pilot symbols corresponding to the i^{th} transmit antenna of the legitimate transmitter mapped to the k^{th} subcarrier of the n^{th} OFDM symbol. Similarly, for the pilots from antennas 2 and 4, the received OFDM symbols on the j^{th} receive antenna of the receiver is given by

$$Y_{k-\frac{L}{2}}^{(j)}[n] = H_{k-\frac{L}{2}}^{(j2)}[n]P_{k-\frac{L}{2}}^{(2)}[n] + H_{k-\frac{L}{2}}^{(j)'}[n]J_{k-\frac{L}{2}}[n] + w_{k-\frac{L}{2}}^{(j)}[n], \tag{3.13}$$

$$Y_{k-\frac{L}{2}}^{(j)}[n+1] = H_{k-\frac{L}{2}}^{(j4)}[n+1]P_{k-\frac{L}{2}}^{(4)}[n+1] + H_{k-\frac{L}{2}}^{(j)'}[n+1]J_{k-\frac{L}{2}}[n+1] + w_{k-\frac{L}{2}}^{(j)}[n+1], \tag{3.14}$$

$$Y_{k+\frac{L}{2}}^{(j)}[n] = H_{k+\frac{L}{2}}^{(j2)}[n]P_{k+\frac{L}{2}}^{(2)}[n] + H_{k+\frac{L}{2}}^{(j)'}[n]J_{k+\frac{L}{2}}[n] + w_{k+\frac{L}{2}}^{(j)}[n], \tag{3.15}$$

$$Y_{k+\frac{L}{2}}^{(j)}[n+1] = H_{k+\frac{L}{2}}^{(j4)}[n+1]P_{k+\frac{L}{2}}^{(4)}[n+1] + H_{k+\frac{L}{2}}^{(j)'}[n+1]J_{k+\frac{L}{2}}[n+1] + w_{k+\frac{L}{2}}^{(j)}[n+1]. \tag{3.16}$$

Then, the constant channel approximation (COCHAP) is invoked along the frequency axis, for L OFDM subcarriers. Thus for each pilot-bearing OFDM symbol, we model the channel coefficient to be *constant for a region of L subcarriers* as shown in Figure 3.11. Hence for $\frac{L}{2} \leq k \leq N - \frac{L}{2}$ we assume that

$$\begin{aligned} H_k^{(j1)}[n] &\approx H_{k+L}^{(j1)}[n], \\ H_{k-\frac{L}{2}}^{(j2)}[n] &\approx H_{k+\frac{L}{2}}^{(j2)}[n], \\ H_k^{(j3)}[n+1] &\approx H_{k+L}^{(j3)}[n+1], \\ H_{k-\frac{L}{2}}^{(j4)}[n+1] &\approx H_{k+\frac{L}{2}}^{(j4)}[n+1]. \end{aligned} \tag{3.17}$$

The jammer channel does not vary appreciably between 2 consecutive OFDM symbols on the same subcarrier. Also, to minimize power leakage into data subcarriers, the jammer transmits digitally modulated symbols at a lower data rate than the target OFDM signal. Therefore, we have

$$\begin{aligned} H_k^{(j)'}[n] &\approx H_k^{(j)'}[n+1] \\ J_k[n] &= J_k[n+1]. \end{aligned} \tag{3.18}$$

Using equations (3.10)-(3.18), we get

$$\begin{aligned} \begin{bmatrix} Y_k^{(j)}[n] - Y_k^{(j)}[n+1] \\ Y_{k+L}^{(j)}[n] - Y_{k+L}^{(j)}[n+1] \end{bmatrix} \approx \begin{bmatrix} P_k^{(1)}[n] & -P_k^{(3)}[n+1] \\ P_{k+L}^{(1)}[n] & -P_{k+L}^{(3)}[n+1] \end{bmatrix} \begin{bmatrix} H_k^{(j1)}[n] \\ H_k^{(j3)}[n+1] \end{bmatrix} + \epsilon_k^{(\mathbf{13})}[n] + \\ \begin{bmatrix} w_k^{(j)}[n] - w_k^{(j)}[n+1] \\ w_{k+L}^{(j)}[n] - w_{k+L}^{(j)}[n+1] \end{bmatrix}, \end{aligned} \tag{3.19}$$

$$\begin{aligned} \begin{bmatrix} Y_{k-\frac{L}{2}}^{(j)}[n] - Y_{k-\frac{L}{2}}^{(j)}[n+1] \\ Y_{k+\frac{L}{2}}^{(j)}[n] - Y_{k+\frac{L}{2}}^{(j)}[n+1] \end{bmatrix} \approx \begin{bmatrix} P_{k-\frac{L}{2}}^{(2)}[n] & -P_{k-\frac{L}{2}}^{(4)}[n+1] \\ P_{k+\frac{L}{2}}^{(2)}[n] & -P_{k+\frac{L}{2}}^{(4)}[n+1] \end{bmatrix} \begin{bmatrix} H_{k-\frac{L}{2}}^{(j2)}[n] \\ H_{k-\frac{L}{2}}^{(j4)}[n+1] \end{bmatrix} + \epsilon_k^{(\mathbf{24})}[n] + \\ \begin{bmatrix} w_{k-\frac{L}{2}}^{(j)}[n] - w_{k-\frac{L}{2}}^{(j)}[n+1] \\ w_{k+\frac{L}{2}}^{(j)}[n] - w_{k+\frac{L}{2}}^{(j)}[n+1] \end{bmatrix}. \end{aligned} \tag{3.20}$$

Parameters $\epsilon_k^{(\mathbf{13})}[n]$ and $\epsilon_k^{(\mathbf{24})}[n]$ account for the residual terms due to temporal variations in the channel between the jammer and the target receiver. The subscripts $\epsilon_k^{(\mathbf{ij})}[n]$ denotes that these residual terms are a result of signal cancellation between the pilot symbols of antenna ports i and j. They are given as

$$\epsilon_k^{(\mathbf{13})}[n] = \begin{bmatrix} H_k^{(j)'}[n] - H_k^{(j)'}[n+1] & 0 \\ 0 & H_{k+L}^{(j)'}[n] - H_{k+L}^{(j)'}[n+1] \end{bmatrix} \begin{bmatrix} J_k[n] \\ J_{k+L}[n] \end{bmatrix}, \tag{3.21}$$

$$\epsilon_k^{(\mathbf{24})}[n] = \begin{bmatrix} H_{k-\frac{L}{2}}^{(j)'}[n] - H_{k-\frac{L}{2}}^{(j)'}[n+1] & 0 \\ 0 & H_{k+\frac{L}{2}}^{(j)'}[n] - H_{k+\frac{L}{2}}^{(j)'}[n+1] \end{bmatrix} \begin{bmatrix} J_{k-\frac{L}{2}}[n] \\ J_{k+\frac{L}{2}}[n] \end{bmatrix}. \tag{3.22}$$

$\mathbf{P}_k^{(\mathbf{13})}[n]$ and $\mathbf{P}_k^{(\mathbf{24})}[n]$ are defined as

$$\mathbf{P}_k^{(\mathbf{13})}[n] \triangleq \begin{bmatrix} P_k^{(1)}[n] & -P_k^{(3)}[n+1] \\ P_{k+L}^{(1)}[n] & -P_{k+L}^{(3)}[n+1] \end{bmatrix}, \tag{3.23}$$

$$\mathbf{P}_k^{(\mathbf{24})}[n] \triangleq \begin{bmatrix} P_{k-\frac{L}{2}}^{(2)}[n] & -P_{k-\frac{L}{2}}^{(4)}[n+1] \\ P_{k+\frac{L}{2}}^{(2)}[n] & -P_{k+\frac{L}{2}}^{(4)}[n+1] \end{bmatrix}. \tag{3.24}$$

We multiply equations (3.19) and (3.20) by $(\mathbf{P}_k^{(\mathbf{13})}[n])^{-1}$ and $(\mathbf{P}_k^{(\mathbf{24})}[n])^{-1}$ respectively, to get the channel estimates at the pilot locations:

$$\begin{aligned} \begin{bmatrix} \hat{H}_k^{(j1)}[n] \\ \hat{H}_k^{(j3)}[n+1] \end{bmatrix} &= (\mathbf{P}_k^{(\mathbf{13})}[n])^{-1} \begin{bmatrix} Y_k^{(j)}[n] - Y_k^{(j)}[n+1] \\ Y_{k+L}^{(j)}[n] - Y_{k+L}^{(j)}[n+1] \end{bmatrix} \\ &\approx \begin{bmatrix} H_k^{(j1)}[n] \\ H_k^{(j3)}[n+1] \end{bmatrix} + (\mathbf{P}_k^{(\mathbf{13})}[n])^{-1} \left\{ \epsilon_k^{(\mathbf{13})}[n] + \begin{bmatrix} w_k^{(j)}[n] - w_k^{(j)}[n+1] \\ w_{k+L}^{(j)}[n] - w_{k+L}^{(j)}[n+1] \end{bmatrix} \right\}, \end{aligned} \tag{3.25}$$

$$\begin{aligned} \begin{bmatrix} \hat{H}_{k-\frac{L}{2}}^{(j2)}[n] \\ \hat{H}_{k-\frac{L}{2}}^{(j4)}[n+1] \end{bmatrix} &= (\mathbf{P}_k^{(\mathbf{24})}[n])^{-1} \begin{bmatrix} Y_{k-\frac{L}{2}}^{(j)}[n] - Y_{k-\frac{L}{2}}^{(j)}[n+1] \\ Y_{k+\frac{L}{2}}^{(j)}[n] - Y_{k+\frac{L}{2}}^{(j)}[n+1] \end{bmatrix} \\ &\approx \begin{bmatrix} H_{k-\frac{L}{2}}^{(j2)}[n] \\ H_{k-\frac{L}{2}}^{(j4)}[n+1] \end{bmatrix} + (\mathbf{P}_k^{(\mathbf{24})}[n])^{-1} \left\{ \epsilon_k^{(\mathbf{24})}[n] + \begin{bmatrix} w_{k-\frac{L}{2}}^{(j)}[n] - w_{k-\frac{L}{2}}^{(j)}[n+1] \\ w_{k+\frac{L}{2}}^{(j)}[n] - w_{k+\frac{L}{2}}^{(j)}[n+1] \end{bmatrix} \right\}. \end{aligned} \tag{3.26}$$

It is to be noted here that for this method, a pilot sequence of symbols is required for which $\mathbf{P}_k^{(\mathbf{13})}[n]$ and $\mathbf{P}_k^{(\mathbf{24})}[n]$ is invertible for $0 \leq k \leq N-1$ and all n. From equations (3.25)-(3.26), we observe that the accuracy of the channel estimates depends on

1. The variation of the channel coefficient, for the channel between the transmit and receive antennas, across the L subcarriers, i.e. from subcarrier indices k to $k+L$, and $k - L/2$ to $k + L/2$.

2. The temporal variation of the channel between the jammer and the receiver, represented by the terms $\epsilon_k^{(\mathbf{13})}[n]$ and $\epsilon_k^{(\mathbf{24})}[n]$.

3. The jammer power, $\mathbb{E}[|J_k[n]|^2] = \sigma_J^2$.

4. The SNR on the pilot locations. In fact, the SNR increases by about $3\,\mathrm{dB}$ due to direct cancellation, even in the case of $\epsilon_k^{(\mathbf{13})}[n] = \epsilon_k^{(\mathbf{24})}[n] = [0 \;\; 0]^T$.

After we obtain the channel estimates on the pilot locations, the channel estimation method described in section 2.3 can be used to estimate the channel estimates on the data resource elements of each OFDM block on each spatial layer to obtain $\hat{\mathbf{H}}_k[n]$, for all OFDM symbols, subcarriers and antennas. Hence, it is possible to use multiple spatial layers for increasing throughput, even in the presence of a multi-tone pilot jammer. However, this comes at the cost of reduced SNR, due to (a) increased channel estimation MSE as a result of jammer mobility, (b) jammer power and (c) noise enhancement.

In this section we have described the application constant channel approximation along the frequency axis, which is applicable in the cases of channels with wide coherence bandwidth. It is also possible to apply this approximation along the time axis, which is applicable in the case of low mobility channels, like in the case pedestrian and low-speed vehicular scenarios.

3.5.5 Numerical Results

In this section we demonstrate the performance of the proposed *COCHAP with jammer cancellation* method for mitigating multi-tone pilot jamming. We use a 4×4 MIMO-OFDM system, with each spatial layer having OFDM block parameters as shown in Table 2.2. We have considered QPSK modulated symbols at each data resource element. For full rank spatial multiplexing, we have assumed the transmit and receive angle spreads to be 2π radians. We have assumed the transmitter and receiver antenna spacing to be $\mathbf{d_t} = [0 \;\; 3\lambda \;\; 6\lambda \;\; 9\lambda]$ and $\mathbf{d_r} = [0 \;\; \lambda \;\; 2\lambda \;\; 3\lambda]$ respectively, where $\lambda = c/f_c$ is the wavelength of the center subcarrier. The pilot pattern used for each spatial layer is shown in Figure 3.9.

We consider the following scenarios:

1. Synchronous multi-tone pilot jamming with no mitigation. The jammer does not transmit on resource elements other than the ones occupied by pilots.

2. No Jamming.

3. Mitigation of multi-tone pilot jamming using COCHAP with jammer cancellation along the frequency axis.

We evaluate the effectiveness of our mitigation scheme based on two metrics: BER and Ergodic Sum Capacity. Ergodic Sum Capacity C_s is indicative of the throughput achievable in the case of

a full spatial-multiplexing based MIMO-OFDM system, given by [47]

$$C_s = B_{sc} \sum_{i=1}^{N_t} \mathbb{E}_n \Big[\sum_{k \notin \mathcal{P}_i[n]} \log_2(1 + \gamma_{k,i}[n]) \Big], \tag{3.27}$$

where B_{sc} is the bandwidth per OFDM subcarrier, $\gamma_{k,i}[n]$ is the SINR of the resource element of the i^{th} spatial layer, k^{th} subcarrier and the n^{th} OFDM symbol. $\mathbb{E}_n[.]$ denotes the expectation w.r.t. the time variable n. $\mathcal{P}_i[n]$ denotes the set of pilot locations mapped to the i^{th} spatial layer at the n^{th} OFDM symbol. Note that pilot REs do not contribute to the capacity as they do not carry data.

Figures 3.12, 3.13 and 3.14 show the Ergodic Sum Capacity for all considered scenarios, for $(\tau_{rms}, f_d) = (100\,\text{ns}, 50\,\text{Hz}), (\tau_{rms}, f_d) = (200\,\text{ns}, 100\,\text{Hz})$, and $(\tau_{rms}, f_d) = (400\,\text{ns}, 200\,\text{Hz})$ respectively. We see that multi-tone pilot jamming reduces the channel capacity by a factor of $4-5$, at $E_b/N_0 = 30\,\text{dB}$ for all considered channel environments. With conventional beamforming, the capacity would scale by a maximum factor of $\log_2(N_r) = \log_2(4) = 2$ at a very high SINR [44]. On the other hand, when COCHAP with Jammer Cancellation is used along the frequency axis, it is able to achieve $\sim 50-90\%$ of the Ergodic Sum capacity w.r.t. that in the case of a 4×4 MIMO-OFDM system with full rank spatial multiplexing in absence of a jammer.

Figures 3.15, 3.16 and 3.17 show the BER comparison for all considered scenarios, for $(\tau_{rms}, f_d) = (100\,\text{ns}, 50\,\text{Hz}), (\tau_{rms}, f_d) = (200\,\text{ns}, 100\,\text{Hz})$, and $(\tau_{rms}, f_d) = (400\,\text{ns}, 200\,\text{Hz})$ respectively. Similar to what we observed in the SISO-OFDM case for QPSK-modulated data symbols, we observe a BER improvement by $1-2$ orders magnitude when COCHAP with JC is used.

An immediate consequence of direct cancellation of signals on adjacent pilot REs is the $3\,\text{dB}$ drop in the SINR, as seen in equation (3.19)-(3.20). This can be observed in Figures 3.12 and 3.15, where the *COCHAP with JC* curves are shifted to the right by $\approx 3\,\text{dB}$ w.r.t. the performance curves of the *no jamming* case. This is because of the low channel variation along the time and frequency axes, which yields very small values for $\epsilon_k^{(\mathbf{13})}[n]$ and $\epsilon_k^{(\mathbf{24})}[n]$ terms in equations (3.19)-(3.20). As one would expect, the effectiveness of our proposed mitigation strategy is sensitive to the channel characteristics between the transmitter and the receiver, and between the jammer and the receiver. The performance of this mitigation strategy is acceptable for $\tau_{rms} = 0 - 200\,\text{ns}$ and $f_d = 0 - 100\,\text{Hz}$, which translate to low root mean square delay spread and low mobility scenarios. The capacity scaling of spatial multiplexing is sensitive to angular spreads at the receive antenna. Low r.m.s. delay spreads of $\sim 50\,\text{ns}$ has been shown to be possible in outdoor to indoor channel environments [14]. Thus, in outdoor-to-indoor and some outdoor-to-outdoor scenarios, COCHAP with JC would be expected to enable full rank spatial-multiplexing operation with as low as 9% loss in throughput, in the presence of a multi-tone pilot jammer. Another approach to deal with channel variations in high r.m.s. delay spread and mobile channels, is to densify the pilot pattern. In this case, constant channel approximation becomes more accurate and can yield better performance even in such scenarios, but at the cost of a marginal reduction in throughput due to the additional pilot overhead.

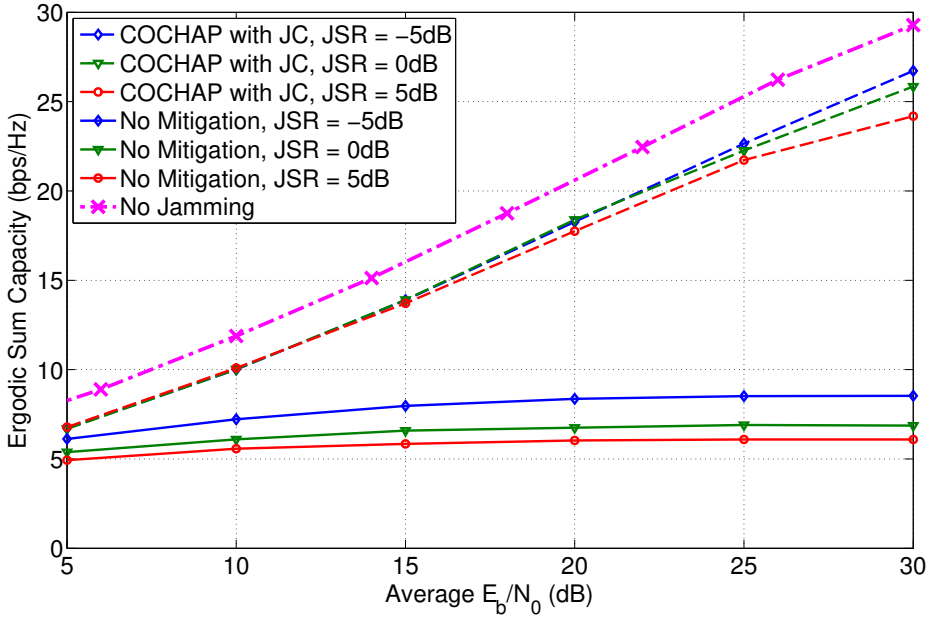

Figure 3.12: Comparison of Ergodic sum capacity for all scenarios, for $\tau_{rms} = 100\,\text{ns}$, $f_d = 50\,\text{Hz}$.

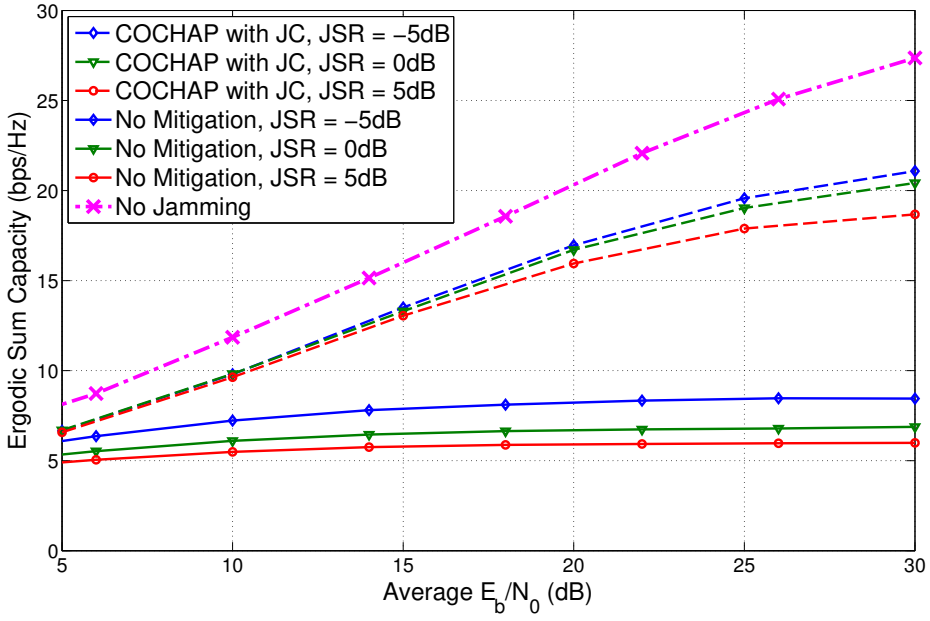

Figure 3.13: Comparison of Ergodic sum capacity for all scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$.

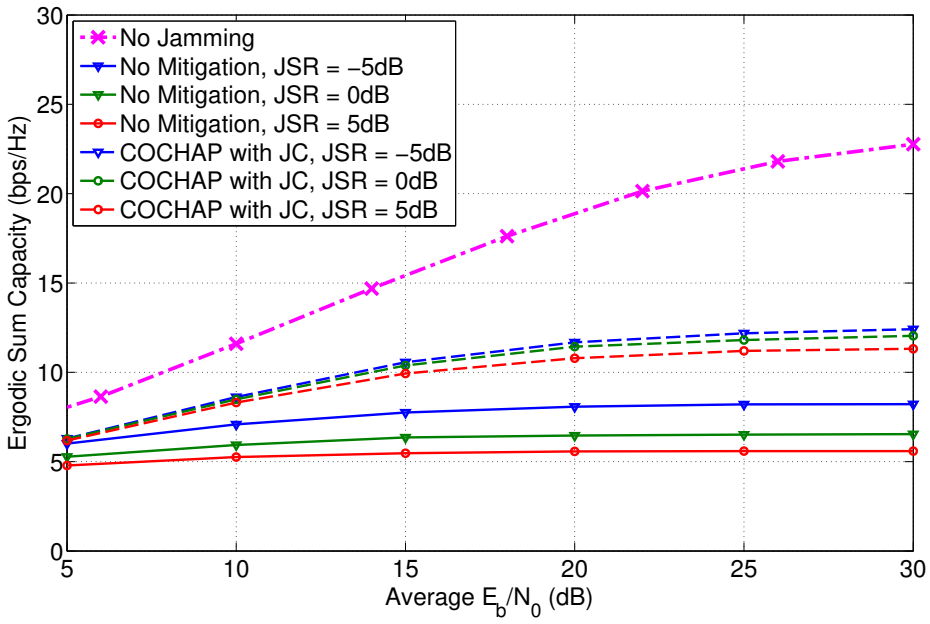

Figure 3.14: Comparison of Ergodic sum capacity for all scenarios, for $\tau_{rms} = 400\,\text{ns}, f_d = 200\,\text{Hz}$.

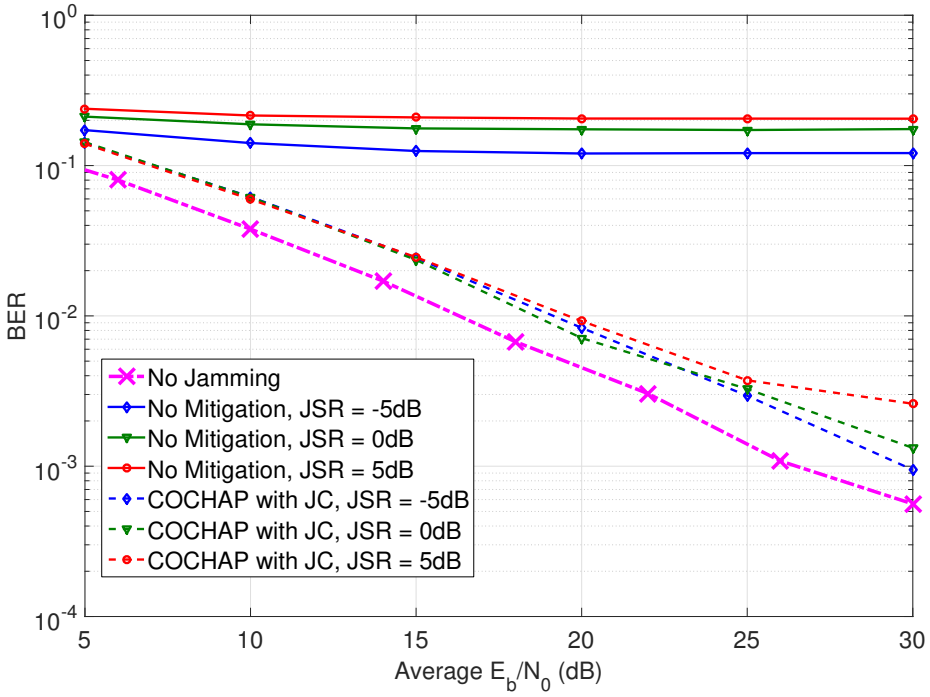

Figure 3.15: Comparison of Bit Error Rate for all scenarios, for $\tau_{rms} = 100\,\text{ns}, f_d = 50\,\text{Hz}$.

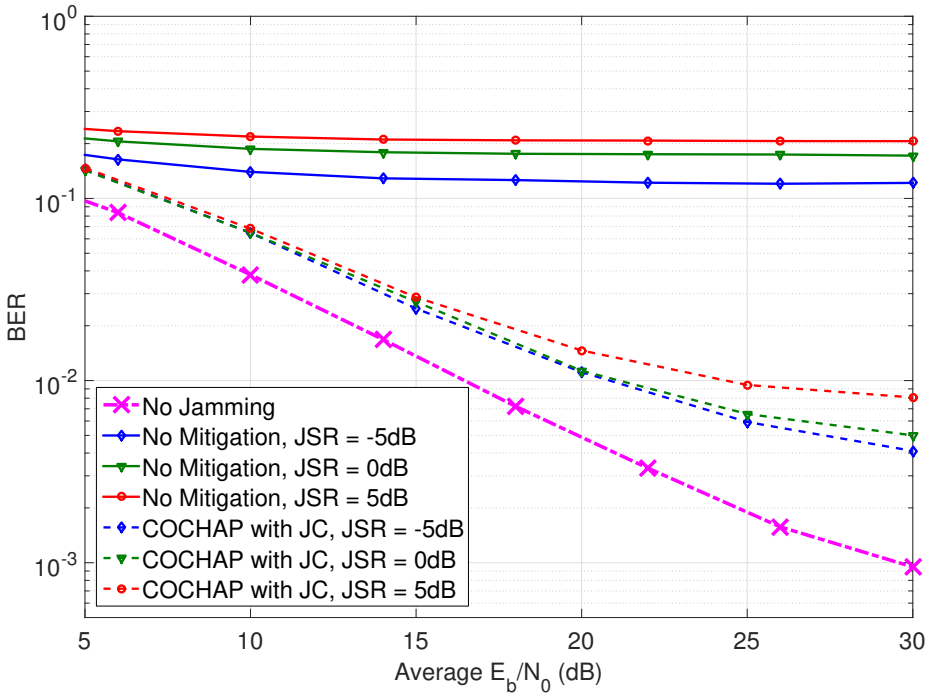

Figure 3.16: Comparison of Bit Error Rate for all scenarios, for $\tau_{rms} = 200\,\text{ns}$, $f_d = 100\,\text{Hz}$.

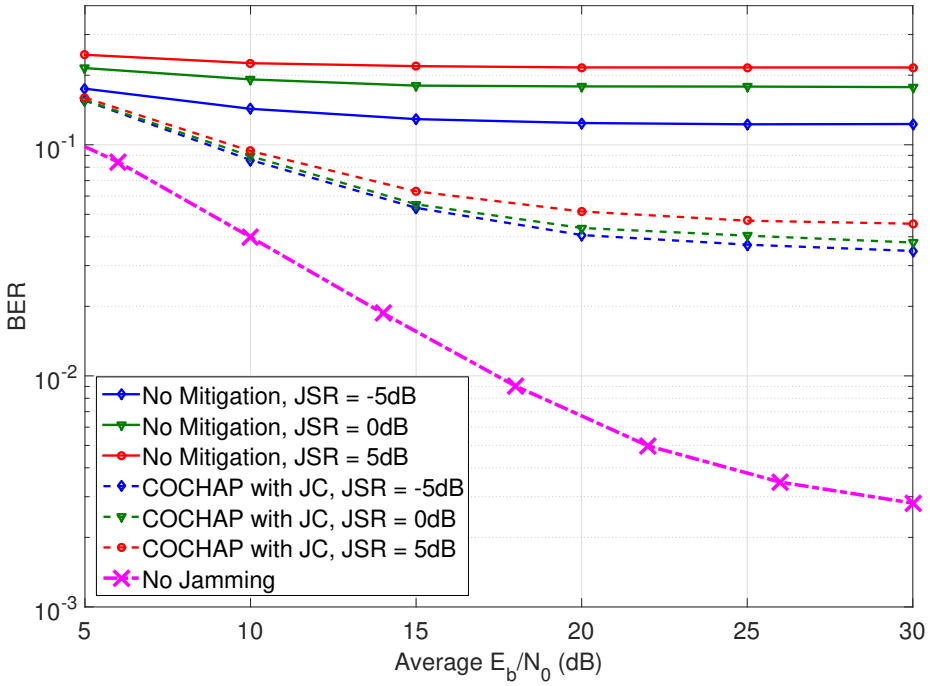

Figure 3.17: Comparison of Bit Error Rate for all scenarios, for $\tau_{rms} = 400\,\text{ns}$, $f_d = 200\,\text{Hz}$.

3.6 Conclusions

In this chapter, we proposed strategies to mitigate a power-constrained multi-tone pilot jammer in SISO- and MIMO-OFDM systems. The main goal of the mitigation strategies is to restore channel estimation performance in the presence of the jammer. We saw that for the case of SISO-OFDM systems:

1. Synchronous pilot jamming is a very efficient attack, but jammer evasion can restore the BER performance because the data REs being interfered constitute a small fraction of the total number of data REs.

2. Asynchronous pilot jamming is a very simple attack, but the data subcarriers on pilot frequencies are unnecessarily affected. In this case, schemes like Adaptive Modulation and Coding, Hybrid ARQ (HARQ), lower coding rates etc. are necessary to restore the BER performance. However, RE Blanking with JC helps in restoring the channel estimation performance, without which the aforementioned auxiliary schemes would be ineffective if implemented all by themselves.

We also investigated whether full rank spatial multiplexing operation is possible in a MIMO-OFDM system in the presence of a multi-tone pilot jammer. We devised and demonstrated a mitigation strategy called *Constant Channel Approximation (COCHAP) with Jammer Cancellation*. It is capable of restoring $\sim 50 - 90\%$ of the Ergodic Sum Capacity w.r.t. that of a full rank spatial multiplexing system, for 4×4 MIMO-OFDM. For very high r.m.s. delay spreads ($\tau_{rms} > 500\,\mathrm{ns}$) and low-mobility scenarios ($f_d = 0 - 100\,\mathrm{Hz}$ at $f_c = 2\,\mathrm{GHz}$), *COCHAP with JC* can be applied temporally to restore full rank spatial multiplexing operation.

In addition to these methods, it is evident that adaptation of pilot spacing and/or locations in the OFDM block, can intrinsically be a deterrent against pilot jamming. This aspect, in addition with the traditional benefits of throughput maximization is explored in Chapter 5.

Chapter 4

Jamming of LTE's Cell-Specific Reference Signal (CRS)

4.1 Background

The Long Term Evolution (LTE) was standardized by the Third Generation Partnership Project (3GPP), to address the rapid surge in cellular data traffic over the last decade. LTE provides tremendous performance enhancements over its predecessors in terms of data rate, latency, coverage and mobility management. Hence, LTE/LTE-A has received a lot of support from the R&D community and it promises to become the primary standard for a broad range of wireless networks, including public safety and military [48]. But, since it is openly documented and widely deployed, it becomes an easy target to intentional and unintentional interference. Hence, it is important to identify vulnerabilities of LTE and make future releases more resilient to targeted interference.

There has been prior work related to RF Jamming of LTE signals. Kakar et al. [15] investigate the performance of the Physical Control Format Indicator Channel (PCFICH) under harsh wireless conditions and propose strategies to mitigate interference on the PCFICH. Lichtman et al. [16] consider the problem of targeted interference on the Physical Uplink Control Channel (PUCCH) and propose detection and mitigation strategies to counter protocol-aware jammers. Labib et al. [17] introduce and demonstrate *LTE control channel spoofing*, which refers to spoofing by a fake eNodeB by transmission of a partial LTE downlink frame. Denial of Service (DoS) was found to be the result of transmission of the partial LTE downlink frames containing only the fake control channels, at a relatively higher power level w.r.t. the legitimate eNodeB. The authors also propose mitigation strategies that required simple modification to the cell selection process of LTE. In [18], a comprehensive threat assessment of LTE/LTE-A is provided, highlighting the vulnerabilities of various LTE physical channels and signals. A survey of mitigation techniques against various jamming/spoofing attacks is also provided. Jover et al. [19] focus on the jamming of LTE networks, and overviews power-efficient jamming attacks. They propose a series of security re-

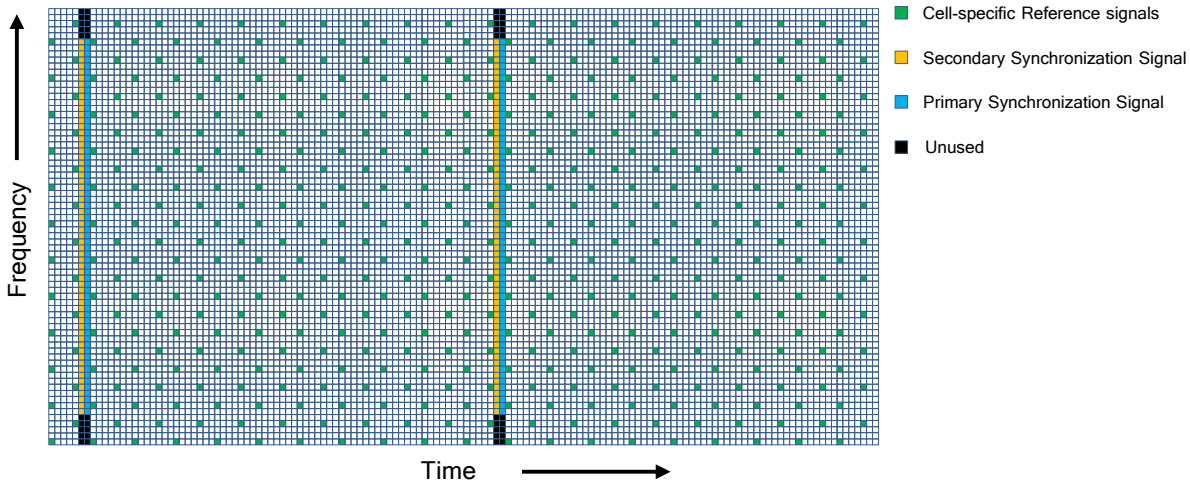

Figure 4.1: A 1.4 MHz FDD-LTE downlink frame normal cyclic prefix, corresponding to antenna port 0 of the eNodeB.

search directions to the LTE standard, which would force a jammer to resort to wideband jamming methods.

So far, this thesis has analyzed the impact of multi-tone pilot jamming of SISO- and MIMO-OFDM systems and proposed and evaluated mitigation strategies. In this chapter, we investigate the performance of the LTE Downlink in the presence of a multi-tone pilot jammer, and provide some insights into its behavior.

Section 4.2 briefly introduces the LTE Downlink structure. Section 4.3 describes the most important features of the LTE PHY layer that are relevant for this analysis. Section 4.4 provides the details of the experimental setup, throughput measurement results and some insights into the behavior of LTE. Section 4.5 concludes by summarizing the main results and the new insights gained.

4.2 The LTE Downlink

3GPP LTE uses Orthogonal Frequency Division Multiplexing (OFDM) as the multicarrier modulation scheme. The base station is called the evolved NodeB (eNodeB/eNB), and the Mobile Station or the User Terminal is called the User Equipment (UE). The 3GPP specifies a variety of system configurations [42]. The supported LTE system bandwidths range from $1.4 - 20\,\mathrm{MHz}$ for 3GPP Release 8 (LTE) and up to $100\,\mathrm{MHz}$ for Release 10 and beyond (LTE-A). Frequency-division and time-division duplexing, or FDD-LTE and TDD-LTE modes, are both specified, requiring paired and unpaired spectrum for the uplink and the downlink. The extended cyclic prefix, as opposed to

the normal cyclic prefix configuration, can account for longer root mean square delay spreads.

Figure 4.1 shows a simplified $1.4\,\mathrm{MHz}$ FDD-LTE downlink frame, highlighting the most important LTE physical control signals. Signals exist only at the physical layer, whereas physical channels are mapped to transport and logical channels. The frame structure in TDD-LTE is similar to that of FDD-LTE, except for the guard intervals between uplink and downlink frames. Of the many important downlink control channels of LTE, the control signals of interest in this work is the cell-specific reference signal (CRS). These are the pilot signals broadcasted in the downlink, and are used for channel estimation and equalization are carried out at the User Equipment (UE). In a single cell, up to 4 different groups of CRSs can be transmitted. Each of these patterns corresponds to a specific antenna port. This is to support up to 4×4 MIMO in the Downlink. The configuration in Figure 4.1 corresponds to the frame that would be transmitted out of antenna port 0 in a multi-antenna system [1]. This particular diamond shaped arrangement with homogeneous subcarrier spacing achieves the minimum mean square error (MMSE) of the channel estimate [25].

The CRS subcarriers are determined by the cell identity $N_{c,ID}$, which can take any integer value from 0 to 503. The pattern shown in Figure 4.1 corresponds to $N_{c,ID} = 0$. A cell-specific frequency shift of $\Delta f = [N_{c,ID} \pmod 6] \times \Delta f_{sc}$ is applied to the pattern in a cell with cell ID of $N_{c,ID}$, where $\Delta f_{sc} = 15\,\mathrm{kHz}$. In addition to aiding in channel estimation, CRS is also used to

1. Estimate channel quality parameters like Reference Signal Received Power (RSRP) and Reference Signal Received Quality (RSRQ). These are important parameters for cell selection and reselection (handover) [1].

2. Derive the channel state information (CSI) for its antenna port aiding in link adaptation, precoding selection, etc. [1].

In order to allow accurate estimation of the above parameters in low SINR environments, relative CRS power boosting (w.r.t. data symbols) of upto $6\,\mathrm{dB}$ is allowed in LTE [1]. Because of the fixed CRS positions in the LTE grid, it would be easy for a jammer to transmit interfering signals on (a) these subcarriers (asynchronous jammer), (b) the exact CRS locations (synchronous, most likely a reactive jammer), or (c) a combination of both with intermittent transmission. Moreover, in the case of frequency reuse factor of 1, the jammer can go to the cell-edge region of 3 adjacent cells, assume any value of $N_{c,ID}$ and target the appropriate CRS subcarriers in order to interfere with that cell. In this case, 1 out of the 3 cells will face network congestion or outage, based on the jammer power and the channel environment. Network congestion can occur in the case when (a) the jammer power is not strong enough to cause DoS or (b) DoS in one cell causes network congestion in adjacent cells due to load balancing. Hence, the PHY layer issues of the network in one cell can potentially translate into coverage and network congestion in the surrounding cells.

4.3 Channel Quality and Adaptive Modulation and Coding

In cellular systems, the measurement of channel quality is necessary in order to optimize the system performance in terms of coverage and throughput for a given transmit power. In LTE, channel quality is estimated using a parameter called the Channel Quality Indicator (CQI), which is fed back to the eNB/UE by the UE/eNB for the downlink/uplink adaptation respectively. Using this fed back CQI, the modulation and coding scheme (MCS) is updated. In LTE, MCS dictates the modulation order and coding scheme used by the UE/eNB in the uplink/downlink [41]. There are 32 possible values for the MCS in the uplink and the downlink [2]. Higher order modulation is more susceptible to interference while lower order modulation schemes are more robust. Similarly, higher code rates are more vulnerable to interference while lower code rates are more resilient against it. There is a tradeoff between throughput and resilience to noise and interference. In general, higher modulation orders and coding rates result in higher throughput, and vice versa.

If the reported CQI value is high, a higher order modulation and coding rate is chosen and vice versa. This is termed as *Link Adaptation*, where the reported CQI value is used to choose the MCS. Since the MCS is adapted based on varying channel quality, it is referred to as *Adaptive Modulation and Coding* in LTE. The CQI in 3GPP LTE is defined as follows [2]:

"A single PDSCH transport block with a combination of modulation scheme and transport block size corresponding to the CQI index, and occupying a group of downlink physical resource blocks termed the CSI reference resource, could be received with a transport block error probability not exceeding 0.1."

In other words, CQI maps to a MCS so that the transport blocks can be decoded with a Block Error rate (BLER) of 10% or less. In LTE, the CQI values vary from 0 to 15, and the MCS values vary from 0 to 31. The mapping from CQI to the spectral efficiency for 3GPP LTE Release 8 is shown in Table 4.1 [1]. 3GPP Release 12 supports 256QAM as well, resulting in much higher spectral efficiency of up to $7.4063\,\mathrm{bps/Hz}$ [2]. There are different types of CQI, with different definitions and reporting intervals. The interested reader is encouraged to refer to the 3GPP standardization documents [2] for more information. For the purpose of our understanding and analysis of pilot jamming in LTE, it is sufficient to understand that the fed back CQI dictates the modulation and coding scheme employed by the transmitter. The maximum theoretical throughput achievable by the downlink of $10\,\mathrm{MHz}$ FDD LTE in a SISO configuration, is shown in Table 4.2 for each MCS value. The interested user is referred to [2] to compute the maximum theoretical throughput for different configurations and 3GPP-LTE releases.

4.4 Impact of CRS Jamming on the Performance of LTE

Since CRS is the downlink pilots broadcasted to all the UEs, we will henceforth refer to multi-tone pilot jamming as *CRS jamming* in the context of LTE. The aim of this jammer could be to (a) throttle the throughput of the cell in order to degrade network performance or (b) cause DoS

Table 4.1: Mapping from CQI to spectral efficiency for 3GPP LTE Release 8. Adapted from [1].

CQI value	Modulation format	Modulation order (m)	Approximate code rate (r)	Spectral Efficiency $(m \cdot r)(\text{bps/Hz})$
0	'Out of Range'	–	–	–
1	QPSK	2	0.0762	0.1523
2	QPSK	2	0.1172	0.2344
3	QPSK	2	0.1885	0.377
4	QPSK	2	0.3008	0.6016
5	QPSK	2	0.4385	0.877
6	QPSK	2	0.5879	1.1758
7	16QAM	4	0.3691	1.4766
8	16QAM	4	0.4785	1.9141
9	16QAM	4	0.6016	2.4063
10	64QAM	6	0.4551	2.7305
11	64QAM	6	0.5537	3.3223
12	64QAM	6	0.6504	3.9023
13	64QAM	6	0.7539	4.5234
14	64QAM	6	0.8525	5.1152
15	64QAM	6	0.9258	5.5547

for legitimate UEs. In the presence of the CRS jammer, UE disconnection would happen when the CQI value is 0. In this case, the UE can (a) try to handover to another frequency on the same cell by requesting resources on the Physical Random Access Channel (PRACH) (b) handover to another cell with the same frequency, but with a better CQI [2] or (c) handover to a different RAT such as 2G/3G. Failure to connect/reconnect to a legitimate cell will cause the UE to experience DoS, or execute an inter-RAT handoff. The interested reader is directed to [2] to know more about cell search and random access procedures for a UE wanting to access the LTE network. For the sake of simplicity in the rest of this chapter we consider DoS to occur for a UE when its *CQI goes to 0* which implies that the UE is disconnected from a LTE cell.

4.4.1 Experimental Setup

In this section we present the impact of CRS jamming on a LTE downlink test system using throughput measurements. In chapter 3, cyclic shifting of pilot locations has been proposed to mitigate the multi-tone pilot jammer. In this section, we investigate its performance in the context of the LTE downlink by performing an experimental analysis with a 3GPP-compliant LTE system. Figure 4.2 shows the schematic of the experimental setup. For the eNodeB, an SDR-based software package called Amarisoft^{TM} LTE100 is used [49]. The CRS (multi-tone pilot) jammer is implemented using GNURadio [50] on another PC. An important factor to consider while designing the jammer, is the presence of a DC null in the OFDM signal of the LTE downlink. Therefore, the pilot

Table 4.2: Mapping from MCS to Maximum Throughput of Physical Downlink Shared Channel (PDSCH) for a FDD SISO 10MHz LTE Release 8 Downlink. Adapted from [2].

MCS value	Modulation order	I_{TBS}	Maximum Transport Block Size per TTI (bits/ms)	Maximum Theoretical Throughput (Mbps)
0	2	0	1384	1.384
1	2	1	1800	1.8
2	2	2	2216	2.216
3	2	3	2856	2.856
4	2	4	3624	3.624
5	2	5	4392	4.392
6	2	6	5160	5.16
7	2	7	6200	6.2
8	2	8	6968	6.968
9	2	9	7992	7.992
10	4	9	7992	7.992
11	4	10	8760	8.76
12	4	11	9912	9.912
13	4	12	11448	11.448
14	4	13	12960	12.96
15	4	14	14112	14.112
16	4	15	15264	15.264
17	6	15	15264	15.264
18	6	16	16416	16.416
19	6	17	18336	18.336
20	6	18	19848	19.848
21	6	19	21384	21.384
22	6	20	22920	21.774
23	6	21	25456	25.456
24	6	22	27376	27.376
25	6	23	28336	28.336
26	6	24	30576	30.576
27	6	25	31704	31.704
28	6	26	36696	36.696
29	2	'reserved'	–	–
30	4	'reserved'	–	–
31	6	'reserved'	–	–

spacing will be different in the middle of the LTE band, than that in the rest of the spectrum. To ensure that power localization on the intended subcarriers is maximum, a frequency-comb using equally spaced multiple sine waves was synthesized using GNURadio.

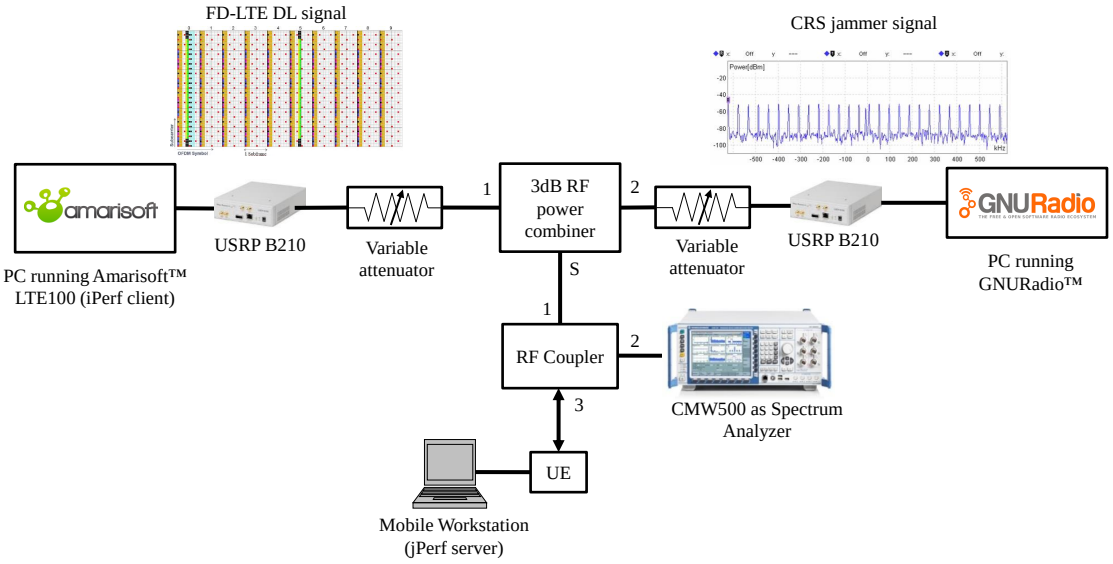

Figure 4.2: Schematic of the experimental setup for throughput measurements of the LTE Downlink.

Table 4.3: Parameters of the LTE Downlink Throughput measurement setup.

Parameter	Value
Frequency Band	Band 7 (UL/DL – 2560 MHz/2680 MHz)
LTE Bandwidth	10 MHz
LTE Release Version	LTE Release 11
Reference Signal Received Power (RSRP)	−72 dBm
JSR per Resource Block (JSR_{RB})	−15 to 10 dB
Maximum Theoretical Throughput	36.696 Mbps

Table 4.3 shows the experimental parameters for the throughput measurements. The variable attenuators are used to control the transmitted downlink and the jammer signal power. It can also be varied digitally on the SDRs using Amarisoft and GNURadio. iPerf [51] and jPerf were the tools used at the eNB and the UE respectively to measure the downlink data throughput. The device under test was a Sierra Wireless U330 LTE Dongle that is compatible with the experimental parameters shown in Table 4.3.

The throughput was measured for each of the following cases:

(a) CRS Jamming - Jammer transmits continuously on all CRS subcarriers of the LTE Downlink.

(b) Data Subcarrier Jamming - Jammer transmits on data subcarriers above/below each CRS subcarrier. The jammer is the same as (a), except that it is shifted up/down by one subcarrier.

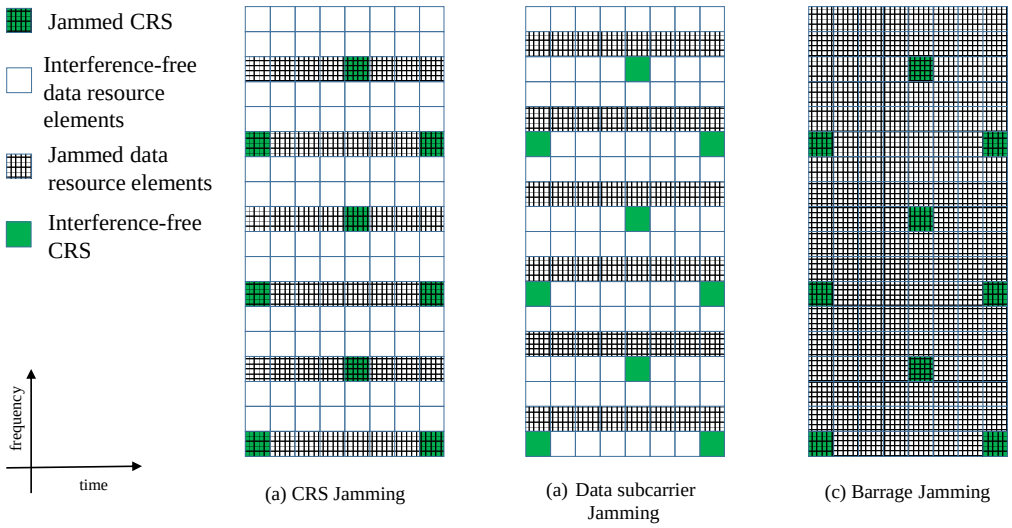

Figure 4.3: Schematic of the jamming strategies investigated for throughput performance of the LTE downlink. The number of REs affected are the same in CRS and data subcarrier jamming.

(c) Barrage Jamming - Jammer transmits on all LTE Downlink subcarriers.

Figure 4.3 shows the schematic of these jamming strategies.

4.4.2 Throughput Measurement Results

The transmit power of the eNB was kept constant and downlink data transfer was carried out using an iPerf client (at the eNB) and jPerf server (at the UE). iPErf and jPerf was configured to make sure that the data buffers were always full. The jammer power is held constant during a downlink data transfer duration of $100\,\mathrm{s}$ and the average throughput over this duration was measured for a fixed value of JSR per resource block (JSR_{RB}).

Definition 4.1. Jammer to Signal ratio per Resource Block (JSR_{RB}) is defined as

$$JSR_{RB} = \frac{P^J_{RB}}{\bar{P}_{LTE,RB}} \tag{4.1}$$

where $\bar{P}_{LTE,RB}$ is the average power of the LTE DL signal per Resource block, and P^J_{RB} is the jammer power per Resource block.

In cases (a) and (b), only one out of every three subcarriers of the LTE DL frame are targeted while in case (c) all subcarriers are targeted. JSR_{RB} was varied from -15 to +10dB while repeating the above procedure for each value of JSR_{RB}, which constitutes a single trial. For each of the

three considered jamming scenarios, four trials were performed and the statistics of the measured throughput values were computed to check the consistency of the measurements for each trial. The variance of measured throughput, averaged across all JSR_{RB} values over four trials were $\sigma_{CRS} = 0.36\,\text{Mbps}, \sigma_{data} = 0.541\,\text{Mbps}, \sigma_{barr} = 0.123\,\text{Mbps}$. The subscripts $CRS, data,$ and $barr$ refer to the cases of CRS, data and barrage jamming respectively. Hence, the throughput variation remains consistent within reasonable values for the considered range of JSR_{RB}, allowing us to gain insights about the behavior of the LTE DL under these three jamming scenarios. The reader is referred to Appendix A for more details regarding the throughput measurements.

In the rest of this section henceforth, all the figures are equipped with error bars. The height from the center to the top of error bar represents the variance of measured throughput for the corresponding JSR_{RB} value. Figure 4.4 shows the comparison between the throughput performance of all the above considered jamming scenarios. As expected, we see that barrage jamming needs $\sim 5\,\text{dB}$ more jammer power than the other 2 cases. However, it is interesting and somewhat counter-intuitive to see the following: a) jamming of 1 out of 3 data subcarriers (jamming scenario (b)) performs comparable to CRS jamming, and b) DoS, which essentially is the disconnection of the UE happens at around the same value of JSR_{RB} for both CRS and data subcarrier jamming. This behavior is the opposite of what was predicted in the theoretical results of Chapter 3. Since the CRS is not corrupted with interference the throughput performance would be expected to be better than that in CRS jamming. But the outcome of our experiments is opposite to our initial hypothesis.

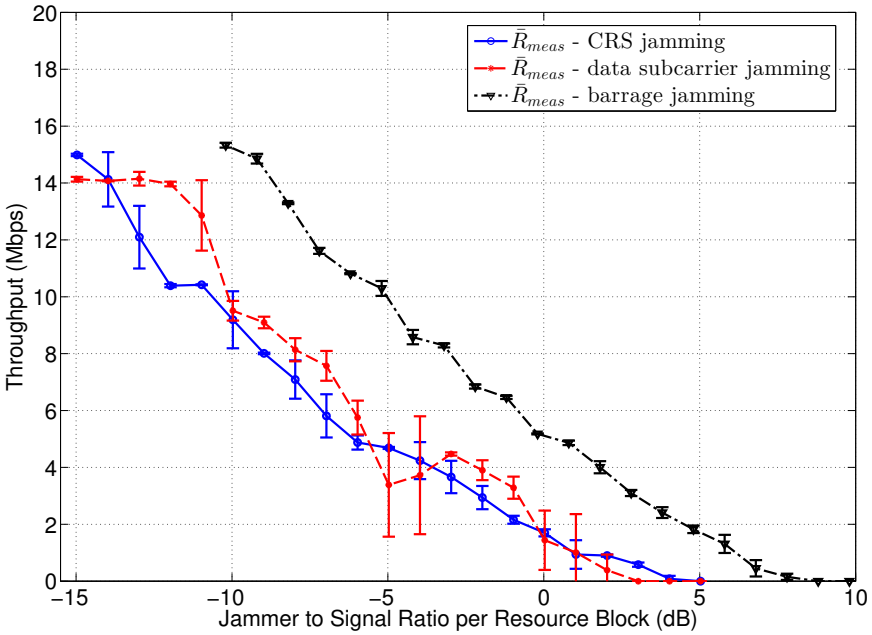

Figure 4.4: Measured throughput versus JSR per Resource Block for all considered jamming schemes.

To investigate this anomalous behavior, the CQI and MCS values were monitored throughout the duration of the throughput measurements. Using Tables 4.1 and 4.2, the maximum achievable throughput for the measured MCS was computed. Figure 4.5 shows the theoretical value of the maximum achievable throughput for the LTE downlink, computed using the monitored CQI and MCS values for each trial. At this point, we define a metric called the *achievable throughput efficiency* which is a measure of the throughput achieved w.r.t. the maximum throughput achievable in ideal conditions.

Definition 4.2. Achievable Throughput efficiency $(\eta_{ach,th})$ for a measured duration T_{meas} is given by

$$\eta_{ach,th} = \frac{\bar{R}_{meas}}{R_{max,MCS}} \tag{4.2}$$

where $\bar{R}_{meas}$ is the average measured throughput for the duration of T_{meas} seconds, and $R_{max,MCS}$ the maximum possible throughput achievable for the *median MCS value* chosen by the eNB during the same duration. $R_{max,MCS}$ can be computed for the corresponding measured MCS value using Table 4.2.

Figure 4.6 shows the throughput efficiency for all jamming scenarios, which shows the severe throughput degradation in data subcarrier jamming (1 in 3 subcarriers). For CRS and Barrage jamming, the throughput efficiency ranges from $80 - 90\%$ for low JSR_{RB} values. However, the efficiency for jamming of 1 in 3 data subcarriers is $10 - 50\%$ in the same range of JSR_{RB}. We define throughput efficiency as the ratio of the measured throughput to the maximum achievable throughput for the average MCS value chosen during the measurement duration.

The reason for the low throughput in case of data subcarrier jamming is revealed in Figures 4.5 and 4.6. It is due to the inability of the UE to accurately estimate the CQI in this jamming scheme. Typically the CQI estimation algorithm is left to the UE manufacturer, but the most common underlying approach is estimation of the noise and interference variance or the SINR [1]. Different methods have been suggested in the literature to estimate CQI, among which pilot-based noise variance estimation is popular [52, 53]. Pilot signals are known to the UE which simplifies the noise and interference variance estimation.

Hence in the case of CRS jamming, the interference on the pilots will result in accurate tracking of the CQI because the interference is aligned with the CRS subcarriers. However, in the case of localized multi-channel data jamming, the absence of interference on the CRS will lead to high CQI values which in return map to a high MCS value. It is well known that higher order modulation schemes (e.g. 16QAM, 64QAM) are not resilient to low SINRs, which result in a high percentage of retransmissions of $> 50\%$. A direct consequence of higher retransmissions and BLER, is degraded throughput performance. We term this phenomenon as 'CQI Spoofing', where the UE is tricked by the jammer into incorrectly estimating CQI values to be high, even in the presence of strong targeted interference. The impact of spoofing is severe when the jammer transmits almost the same power per targeted RE (note that only 1 out of 3 subcarriers are targeted) as the LTE signal, which is represented by the kinks near $JSR_{RB} = -5\,\mathrm{dB}$ in Figure 4.4. It is

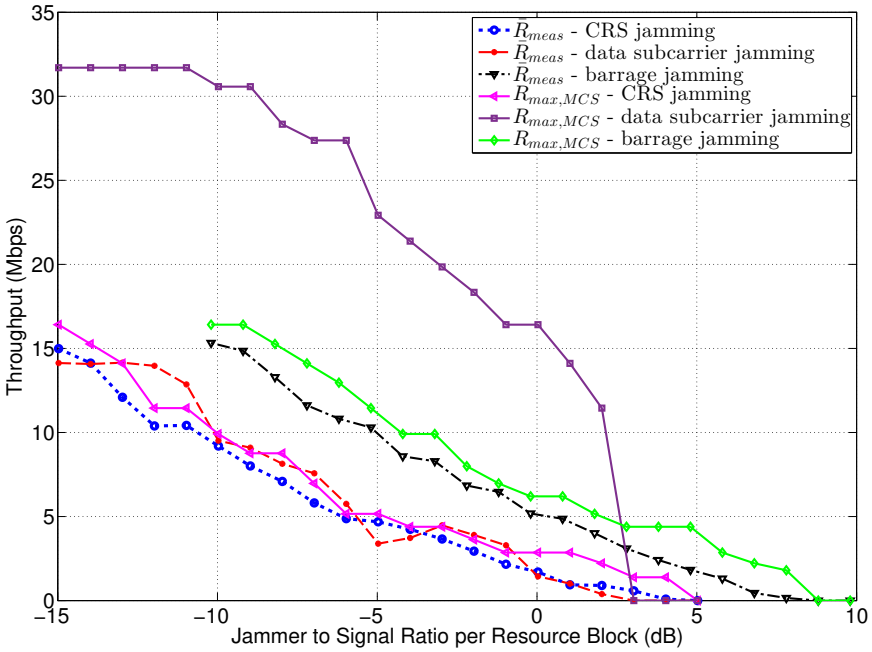

Figure 4.5: Comparison of maximum theoretically achievable $(R_{max,MCS})$, and measured average $(\bar{R}_{meas})$ throughput values versus JSR per Resource Block, for (a) CRS jamming, (b) data subcarrier jamming (1 out of 3 data subcarriers above/below CRS frequencies), and (c) barrage jamming.

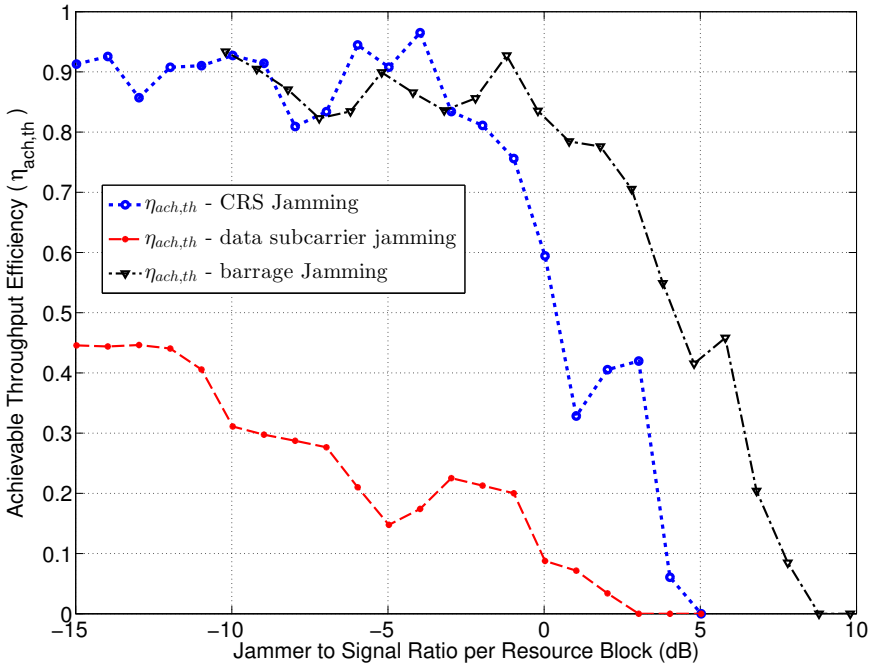

Figure 4.6: Comparison of achievable throughput efficiency $(\eta_{ach,th})$ for all considered cases.

clear from Figure 4.5 that a marginal reduction in the CQI value could enhance the throughput performance greatly.

CQI Spoofing needs to be addressed by 3GPP in order to minimize the damage caused by a jammer targeting only data subcarriers. Since public safety and military wireless networks have chosen LTE as their preferred standard for wireless communications, it becomes even more important to address this undesired behavior. Research into estimation of CQI correction terms, in the presence of such targeted interference will provide the LTE DL a means to balance throughput in the presence of strong targeted interference, so that the performance degradation is less severe.

4.5 Conclusions

In this chapter, we presented experimental results to understand the behavior of 3GPP LTE downlink in the presence of CRS and data-only jammers. The main results can be summarized as follows:

1. CRS Jamming has been shown to be an jamming effective method and needs $5\,\mathrm{dB}$ less power than Barrage Jamming to cause Denial of Service in the LTE Downlink.

2. An important new finding as a result of these experiments is the incorrect estimation of CQI in the presence of data-only jamming; we therefore call type of attack as 'CQI Spoofing'. CQI Spoofing leads to significant results in massive throughput degradation and results in similar downlink performance in the presence of both CRS and data-only jamming.

This can have severe consequences in cellular networks since the CRS jammer now has the potential to affect three or more cells simultaneously by moving to the intersecting area of the cells, and randomly picking any CRS pattern to interfere with. Therefore, considerable research effort is necessary to devise accurate CQI estimation/correction algorithms that maximize the throughput by optimizing link adaptation in the presence of such targeted interference.

Chapter 5

Adaptation of Pilot Patterns for OFDM Systems

5.1 Introduction

In current wireless standards based on OFDM, there is very little flexibility for adaptive signaling, such as support for multiple classes of frame structures, adaptive control channel overhead based on different operating conditions etc. In the evolution from 4G to 5G, there is interest in the research community to adopt multicarrier waveforms with adaptive transmission parameters [6] at the physical layer. Although not all control channels can be eliminated to reduce system overhead, one class of control signals whose overhead can be controlled are pilot signals. Most standards define a fixed number of pilots to be deployed, but it is a waste of resources when the channel remains flat in either time and/or frequency. This has motivated some work on adapting pilot spacing (also called pilot periods) in time and frequency based on varying channel conditions, where the aim is to vary pilot spacing to meet/maximize a particular target metric with minimal control overhead. An indirect benefit obtained by adapting the pilot spacing is an inherent resilience to multi-tone pilot jammers, whose impact has been discussed in previous chapters. This will lower the effect of a static jammer, since in such a scenario it would be necessary to track pilot locations of the downlink signal in real time.

There has been some research on adapting pilot density. The authors in [25] obtained pilot periods using Mean Square Error (MSE) of channel estimates as the criterion, and showed that equal powered and spaced pilot symbols lead to the least MSE. In [54], the pilot spacing was designed with Bit Error Rate (BER) as the cost function. The paper proposed a new pilot-pattern which had the potential of reducing the noise power on the pilot subchannel estimate by half. The authors in [55] demonstrated pilot arrangements based on Kalman channel estimators, by limiting the effective Signal to Noise Ratio (SNR) within a desired bound. The problem with these approaches are that they result in conservative pilot periods and these cost functions do not capture the bottom

line of a cellular communication system: throughput.

In this regard, the authors of [56] proposed OFDM frames with adaptive pilot spacing and pilot power to enhance throughput performance in the system. The authors have considered a general linear channel estimator and provide numerical insights on the channel estimation Mean Square Error (MSE). For pilot adaptation, they propose a feedback mechanism using metrics like Channel Quality indicator (CQI) that it is used in the 3GPP LTE standard. In this work, we provide a generic algorithm to adapt the pilot spacing based on the feedback of the estimated channel statistics. As compared to the state of the art, our proposed method offers an advantage in terms of applicability in multi-band Carrier Aggregation with less feedback requirements, as we will elaborate later.

For pilot adaptation, the availability of accurate channel statistics is necessary to adjust pilot density in order to meet the targeted system performance. However, estimation of channel statistics over a finite duration of time will rarely be accurate enough, especially in low SNR conditions. To overcome this problem we use a codebook-based approach, where the receiver fits the channel statistics estimates to one of multiple stored channel profiles. These "fitted" channel statistics are then used to predict the likely Mean square error (MSE) for the desired pilot configuration. These MSE values are used to calculate the post-equalization SINR, which is used by the receiver to maximize the upper bound of the constrained channel capacity to find the optimal pilot spacing and power [56]. The parameters of the pilot configuration that maximizes this bound are fed back to the transmitter through the uplink and the process is repeated. We demonstrate the performance gain due to pilot adaptation in SISO- and MIMO-OFDM systems through simulation results. We highlight the benefit of using pilot adaptation for cognitive radios and emerging wireless applications like unmanned aerial systems, vehicular to vehicular networks etc. A method for reducing the feedback for multi-band Carrier Aggregation systems utilizing adaptive pilot patterns is also outlined.

Some pilots are meant for specific users, while others are broadcasted. We also discuss the viability of pilot adaptation for each of these pilot types, and provide insights and approaches for introducing adaptive pilots in 5G.

This chapter is organized as follows. Section 5.2 provides the problem formulation, our proposed algorithm and its computational complexity. Section 5.3 presents the numerical simulation results demonstrating the capacity gain achievable using pilot spacing. Section 5.4 highlights the issues that need to be addressed and points out areas where pilot adaptation can be utilized in LTE and emerging wireless applications. Section 5.5 concludes this chapter by summarizing our main findings.

5.2 Adaptation of Pilot Spacing and Power

Wireless channels exhibit different characteristics based on the terrain, propagation environment, obstructions, mobility of users etc. For low mobility and strong line of sight channels, the channel

is flat in time and frequency, while for high mobility with a strong scattering environment, the channel exhibits strong frequency selectivity and fast fading in time. Most wireless standards are designed to operate in the worst channel conditions. For this reason the pilot spacing in LTE is designed to satisfactorily capture channel variations for root mean square delay spread $\tau_{rms} = 991\,\mathrm{ns}$ and a user velocity of $500\,\mathrm{km/h}$ at $f_c = 2\,\mathrm{GHz}$ [1]. But the wireless channel might be better or worse based on the operating environment. Therefore, there is interest in the wireless community to adapt the spacing of pilots in future wireless standards to match the channel conditions [6]. The central idea of pilot adaptation is shown in Figure 5.1 where:

(a) Increase the pilot spacing along the time axis when the coherence time of the channel is high and vice versa.

(b) Increase the pilot spacing along the frequency axis when the coherence bandwidth of the channel is high and vice versa.

In this section, we describe an algorithm to adapt pilot spacing and power in a non-stationary doubly selective fading channel with the aim of maximizing the throughput of the link for a particular channel scenario. There is wide agreement that instantaneous channel capacity is the best indicator of the throughput that can be achieved [57, 56]. Since it is not possible to know the instantaneous capacity beforehand, we maximize the upper bound of the constrained channel capacity based on estimation of necessary operating parameters [56]. Nonstationary channels that vary very rapidly in time and frequency can be modeled as locally stationary [58]. This assumption allows us to pose and solve an optimization problem to find the throughput-maximizing pilot configuration. The formulation of this problem and an algorithm to solve it are described in the rest of this section.

5.2.1 Problem Formulation

In order to find an optimal pilot configuration for a particular channel scenario, we formulate an optimization problem to maximize the upper bound of the constrained channel capacity as a function of the data to pilot power ratio ρ, the pilot period in frequency $\Delta_p f$ and the pilot period in time $\Delta_p t$. As the name suggests, the 'data to pilot power ratio' is defined as $\rho = \sigma_d^2/\sigma_p^2$, where σ_d^2 is the transmitted power for data symbols and σ_p^2 the transmitted pilot power. For ease of analysis, we are not considering adaptive bit loading in our algorithm. The constraints we impose on the cost function are

(a) average transmitted power per resource element $\bar{P}_t$,

(b) pilot spacing in time $\Delta_p t$,

(c) pilot spacing in frequency $\Delta_p f$,

(d) data to power pilot ratio ρ.

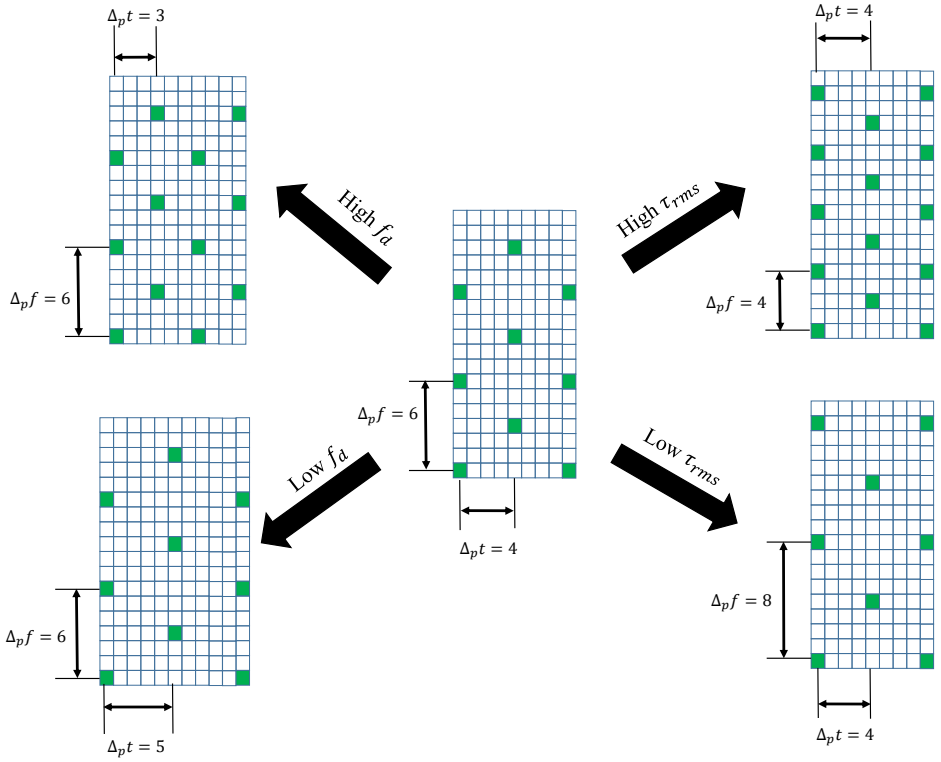

Figure 5.1: Illustration of pilot adaptation based on varying channel conditions.

The optimization problem can be mathematically represented as

$$\{\rho_o, (\Delta_p f)_o, (\Delta_p t)_o\} = \underset{\rho, \Delta_p f, \Delta_p t}{\text{argmax}} \; S(\Delta_p f, \Delta_p t) \cdot \log_2(1 + \overline{\gamma}) \tag{5.1}$$

$$\begin{aligned} \text{subject to} \quad & \overline{P}_t(\Delta_p t, \Delta_p f, \rho) \leq 1 \\ & \Delta_p t \leq T_{max} \\ & \Delta_p f \leq F_{max} \text{ and } \Delta_p f \; (mod\; 2) = 0 \\ & \rho \leq \rho_{max}, \end{aligned}$$

where $\overline{\gamma}$ is the post-equalization SINR for a ZF equalizer under imperfect channel knowledge, $S(\Delta_p f, \Delta_p t)$ is the spectrum utilization function as a function of pilot spacing for OFDM, $\overline{P}_t$ is the average power per resource element, and T_{max} is the maximum tolerable latency by the receiver due to channel estimation. F_{max} is the maximum allowable pilot spacing, which is dictated by the number of channel taps. ρ_{max} is the maximum allowable data to pilot power ratio, that is dictated by PAPR considerations and is dependent on the transmitter power amplifier (PA) characteristics. The post equalization SINR $\overline{\gamma}$ is given as [56]

Table 5.1: Description of the most important parameters

Variable	Description
ρ	The data to pilot power ratio
σ_d^2	Average power of data symbols
σ_p^2	Average power of pilot symbols
$\Delta_p t$	Pilot spacing in time
$\Delta_p f$	Pilot spacing in frequency
$\bar{\gamma}$	Post-equalization SINR
σ_{ICI}^2	Inter-carrier interference power
σ_n^2	Noise power
MSE_d	Channel estimation MSE of data resource elements
N_t	Number of transmit antennas
N_r	Number of receive antennas
N	Number of subcarriers per OFDM symbol
T	Number of OFDM symbols used for channel statistics estimation
$\mathbf{H}$	The $N \times T$ channel matrix for each transmit-receive antenna pair
T_s	OFDM symbol duration
f_d	Maximum Doppler Spread
τ_{rms}	Root mean square delay spread
$\hat{R}_t$	Estimated temporal channel correlation function
$\hat{R}_f$	Estimated spectral channel correlation function

$$\overline{\gamma} = \frac{\sigma_d^2}{\sigma_n^2 + \sigma_{ICI}^2 + \sigma_d^2 \cdot MSE_d} \sigma_{ZF}, \tag{5.2}$$

where σ_n^2 is the average noise power, σ_{ICI}^2 is the average power of Intercarrier Interference, MSE_d is the MSE of the channel estimates for data resource elements, and $\sigma_{ZF} = N_r - N_t + 1$ is the equalizer allocation function when neglecting antenna correlation [59]. N_t and N_r are the number of transmit and receive antennas respectively. Hence for the SISO- and $N \times N$ MIMO-OFDM cases, $\sigma_{ZF} = 1$. The intercarrier interference power can be bounded using [31]

$$\left[\frac{\sigma_d^2}{12}(2\pi f_d T_s)^2 - \frac{1}{360}(2\pi f_d T_s)^2\right] \leq \sigma_{ICI}^2 \leq \left[\frac{\sigma_d^2}{12}(2\pi f_d T_s)^2\right], \tag{5.3}$$

where f_d is the maximum Doppler frequency shift, and T_s the symbol duration. The expression forming the lower bound will have to be used in equation (5.1) because we are optimizing the

upper bound on the constrained channel capacity. The MSE for data resource elements MSE_d can be obtained by ignoring the contribution from pilots in equation (2.28) to get

$$MSE_d = \frac{2}{N_B - 2}\left[\frac{MSE_{1,l}}{C_1} + \frac{MSE_{2,l}}{C_2} + (L-1)\cdot MSE_{f,A}\right]. \tag{5.4}$$

The spectral utilization function depends on the number of data resource elements N_d and pilots N_p, which in turn depend on the pilot spacing $\Delta_p t$ and $\Delta_p f$. For N subcarriers per OFDM symbol with the diamond-shaped pilot arrangement, there will be N_{f1} and N_{f2} pilots in alternate pilot-bearing OFDM symbols. Therefore $N_p = N_{f1} + N_{f2}$ where $N_{f1} = \lceil N/\Delta_p \rceil$ and

$$N_{f2} = \begin{cases} \lceil N/\Delta_p f \rceil & \text{if } N \ (mod\ \Delta_p f) > \Delta_p f/2 \\ \lfloor N/\Delta_p f \rfloor & \text{if } N \ (mod\ \Delta_p f) \leq \Delta_p f/2, \end{cases}$$

and $\lceil . \rceil$ and $\lfloor . \rfloor$ refer to the ceiling and floor operations. The spectrum utilization function is given as

$$S(\Delta_p f, \Delta_p t) = \frac{N_d}{N_d + N_p}, \tag{5.5}$$

where N_d can be obtained by seeing that among $N = (2 \cdot N \cdot \Delta_p t)$ resource elements, N_p of them are occupied by pilots. If it is a MIMO system, then RE nulls would be necessary to transmit pilot from other antennas, as shown in Figure 3.9 of chapter 3. Therefore, for a $N_t \times N_r$ MIMO system, $N_d = (2 \cdot N \cdot \Delta_p t - N_t \cdot N_p)$ and

$$S(\Delta_p f, \Delta_p t) = \frac{2N\Delta_p t - N_t \cdot (N_{f1} - N_{f2})}{2N\Delta_p t}. \tag{5.6}$$

When we have a constraint on the average unit power per resource element, we have that $N_d\sigma_d^2 + N_p\sigma_p^2 = 2N\Delta_p t = N_{tot}$. For a fixed ρ, the data and pilot powers can be obtained as

$$\sigma_d^2 = \frac{N_{tot}}{N_p/\rho + N_d} \tag{5.7}$$

$$\sigma_p^2 = \frac{N_{tot}}{N_p + \rho N_d}. \tag{5.8}$$

The only quantity left that is necessary to compute the upper bound of the constrained capacity is the channel estimation MSE. The next subsection describes a method to compute MSE_d.

5.2.2 Estimation of Channel Statistics

To compute the MSE for data, the receiver needs the second order channel statistics $R_t(\Delta t)$ and $R_f(\Delta f)$. In the absence of feedback, the receiver would need to estimate the channel statistics $\hat{R}_t(\Delta t)$ and $\hat{R}_f(\Delta f)$ on its own, which can be done by temporal averaging assuming local stationarity of the channel for the averaging duration [60]. For a $N \times T$ channel matrix $\mathbf{H}$ with N rows corresponding to frequency subcarriers, and T columns corresponding to OFDM symbols, the statistics can be estimated using

$$\begin{aligned} \hat{R}_t(-i) &= \frac{1}{T-|i|} \sum_{t=1}^{T-|i|} \left\{ diag_i \left[\mathbf{H}^H \mathbf{H} \right] \right\}_t \\ \hat{R}_f(-j) &= \frac{1}{N-|j|} \sum_{f=1}^{N-|j|} \left\{ diag_j \left[\mathbf{H}\mathbf{H}^H \right] \right\}_f, \end{aligned} \tag{5.9}$$

where $diag_i[\mathbf{X}]$ is the vectorized i^{th} diagonal of matrix $\mathbf{X}$ and $\left\{ diag_i[\mathbf{X}] \right\}_k$ its k^{th} element. Because $\mathbf{H}\mathbf{H}^H$ and $\mathbf{H}^H\mathbf{H}$ are Hermitian-symmetric matrices, the other elements can be found using $\hat{R}_t(-i) = \hat{R}_t^*(i)$ and $\hat{R}_f(-j) = \hat{R}_f^*(j)$, where $(.)^*$ denotes the complex conjugate operation. This follows from the properties of Hermitian symmetric matrices.

In practical scenarios where the channel statistics are estimated over a finite duration of time, the accuracy will be poor. This occurs due to (a) interpolation error, and (b) addition of noise. In the worst case, the estimated channel statistics can violate the properties of an autocorrelation function. This is probably especially in high noise, low mobility and/or flat fading scenarios. Hence, utilizing these estimated channel statistics directly can result in inconsistent and, sometimes absurd values for the MSE. To overcome these limitations, we opt for a codebook-based approach where the receiver stores the power delay profile and maximum Doppler Frequency values of typical channels it expects to encounter. A cognitive radio can update the codebook over time as it learns more about its channel environment. The receiver calculates the channel estimates using equation (5.9) for a finite duration of time and fits it to a channel profile that best matches the estimated statistics.

5.2.3 Channel Statistics Codebook

Let the codebook be denoted by set $\mathcal{R}_C$ with 2 disjoint subsets $\mathcal{R}_{C,t} \subseteq \mathcal{R}_C$ and $\mathcal{R}_{C,f} \subseteq \mathcal{R}_C$, with $|\mathcal{R}_{C,f}| = M_f$ and $|\mathcal{R}_{C,t}| = M_t$. $\mathcal{R}_{C,f}$ is the set of channel frequency correlation profiles, with elements $R_{fc,l} \in \mathcal{R}_{C,f}$ for $1 \leq l \leq M_f$. Likewise, $\mathcal{R}_{C,t}$ is the set of channel temporal correlation profiles, with elements $R_{tc,m} \in \mathcal{R}_{C,t}$ for $1 \leq m \leq M_t$. Here, assuming a classic Doppler spectrum $R_{tc,m}(\Delta t) = J_0(2\pi f_{d,m}\Delta t)$ from equation (2.8), where $f_{d,m}$ is the maximum Doppler spread for the m^{th} channel temporal correlation profile. Such a definition of the codebook channel profiles is motivated by the WSSUS approximation.

Initially, the profiles that comprise the codebook would correspond to the most common type of channels that the wireless radios would be expected to encounter, based on reported field measurements in the literature. Examples would be the channel profiles from ITU-T [61] and the 3GPP channel models [62]. In the case of a cognitive radio, these profiles can be updated over time, when it learns more about its operating environment. The codebook can be designed to match the typical scenarios encountered, for e.g. vehicular to vehicular networks would have a large variation in Doppler spreads due to vehicular movement, UAV to UAV systems might have very low root mean square delay spread due to strong line of sight.

5.2.4 Optimal Pilot Spacing and Power

We assume that both transmitter and receiver know and share a common $\mathcal{P}, \mathcal{D}_f$ and $\mathcal{D}_t$, the sets that contain allowable values for $\rho, \Delta_p f$ and $\Delta_p t$, respectively. With the bounds for each parameter predefined, the algorithm to find the optimal pilot spacing and power can be applied for every N_{OFDM} symbols as shown in Algorithm 1. This algorithm is executed once using the most recent N_{OFDM} symbols. Upon its completion, it uses the subsequent N_{OFDM} symbols for the next cycle of pilot adaptation, and so on.

Algorithm 1 Optimal pilot spacing and power allocation using codebook of channel profiles.

1: Estimate channel statistics $\hat{R}_t$ and $\hat{R}_f$ from equation (5.9) using channel estimates from the most recent N_{OFDM} OFDM symbols across N subcarriers.
2: Find the frequency and time domain channel profiles from the codebook, $R_{fc,l'}$ and $R_{tc,m'}$ closest to the estimated statistics by evaluating

$$\begin{aligned} l' &= \underset{1 \le l \le M_f}{\arg\min} \quad \mathbb{E}\{|\hat{R}_f - R_{fc,l}|^2\} \\ m' &= \underset{1 \le m \le M_t}{\arg\min} \quad \mathbb{E}\{|\hat{R}_t - R_{tc,m}|^2\}. \end{aligned} \tag{5.10}$$

For $N_t \times N_r$ MIMO-OFDM, there will be $N_t \cdot N_r$ channel matrices of dimension $N \times N_{OFDM}$. If $\mathbf{l}'$ and $\mathbf{m}'$ represent the $N_t N_r \times 1$ vectors of codebook indices found using equation (5.10), then $l' = mode(\mathbf{l}'), m' = mode(\mathbf{m}')$. Here, $mode(.)$ represents the 'mode' operation.
3: For $\rho \in \mathcal{P}, \Delta_p f \in \mathcal{D}_f, \Delta_p t \in \mathcal{D}_t$, compute channel estimation MSE MSE_d assuming channel statistics $R_{fc,l'}$ and $R_{tc,m'}$ using equation (5.4).
4: Using the values of MSE for each tuple $\{\rho, \Delta_t f, \Delta_t t\}$, solve the optimization problem by solving equation (5.10) by calculating all the other necessary terms using equations (5.2)-(5.8). Let the resulting optimal tuple be $\{\rho_o, (\Delta_p f)_o, (\Delta_p t)_o\}$.
5: Feed back $\{\rho_o, (\Delta_p f)_o, (\Delta_p t)_o\}$ to the transmitter.
6: End.

5.2.5 Complexity

5.2.5.1 SISO and MIMO-OFDM systems

Based on the above algorithm for pilot adaptation, the receiver needs to feed back the indices of the corresponding channel profile from the codebook. There are a total of $M_t M_f$ possible values that can be sent to the transmitter. Therefore, the receiver would need to feed back $b_f = \lceil \log_2(M_t M_f) \rceil$ bits. Estimation of channel statistics involve matrix multiplication, which can be accomplished with a complexity of $O(N^2 T)$ for $\hat{R}_f$, and $O(T^2 N)$ for $\hat{R}_t$. Values chosen for T and N have to be chosen to fit the statistics from the codebook more accurately. If we only need $N_{\Delta t}$ terms of $\hat{R}_t$ and $N_{\Delta f}$ terms of $\hat{R}_f$, then the complexity becomes $O(T^2 N_{\Delta f})$ and $O(N^2 N_{\Delta t})$. Here $\hat{R}_t$ and $\hat{R}_f$ will be computed by summing along the central $N_{\Delta f}$ and $N_{\Delta t}$ diagonals respectively. Since these operations are similar to those used in an MMSE receiver [23], its implementation does not consume additional computing resources in modern wireless receivers.

5.2.5.2 Multi-Band Carrier Aggregation

In non-contiguous carrier aggregation, the resource blocks can be allocated to a user across two or more frequency bands. In such a case, pilots will be sent on all N_b allocated bands $(f_1, f_2, \cdots f_{N_b})$ and the pilot spacing can be varied on each frequency band based on its channel statistics. In this case, some of the properties of Doppler spread can be exploited to reduce the computation and feedback requirements for the channel profile in the codebook. We assume that the OFDM symbol duration, subcarrier spacing and all other parameters except for the pilot spacing and power, are the same across all frequency bands. Since the Doppler frequency scales linearly with the center frequency f_c, only 1 codebook index specifying the temporal pilot spacing needs to be fed back for any one of the N_b bands. The temporal codebook index m' for the other $N_b - 1$ bands can be estimated at the receiver by back calculations using equations (2.8) and (5.1) - (5.8). Even in the case when each frequency band experience different root mean square delay spreads, the total number of bits needed for feedback will be $b'_f = \lceil \log_2(M_t M_f + (N_b - 1) \times M_f) \rceil$. Hence with this method, at least $\log_2 \left(\frac{N_b M_t M_f}{M_t M_f + (N_b - 1) \times M_f} \right)$ bits of feedback can be saved.

5.3 Numerical Results

This section presents the numerical simulation results showing the gains of adaptive pilot spacing and power. The two important channel statistics descriptors are the root mean square delay spread τ_{rms} and the Doppler spread f_d. Figure 5.2 shows the variation of these two parameters over time and corresponds to the channel scenario chosen to test the performance of Algorithm 1. The range of parameters are $25\,\text{ns} \leq \tau_{rms} \leq 1\,\mu\text{s}$ and $4\,\text{Hz} \leq f_d \leq 980\,\text{Hz}$. For a duration of $100\,\text{ms}$, we assume stationarity of the channel statistics. For a total scenario duration of about $160\,\text{s}$, the

Table 5.2: Codebook of Channel Profiles, $\mathcal{R}_C$

A: Channel profiles for Doppler Spread $(\mathcal{R}_{C,t})$

Codebook Index (m)	Mobility Type/Velocity	$f_d^{\dagger}$ (Hz)
1	Pedestrian (3km/hr)	5.6
2	Urban Vehicular (32km/hr)	60
3	Highway Vehicular (120km/hr)	222.22
4	High Speed Train/UAV low (300km/hr)	555.56
5	High Speed Train/UAV medium (400km/hr)	750
6	High Speed Train/UAV high (500km/hr)	925

B: Channel profiles for Frequency Selectivity $(\mathcal{R}_{C,f})$

Codebook Index (l)	Normalized PDP	Delay taps*	τ_{rms} (ns)
1	[0.9310, 0.3425, 0.126]	[0,1,2]	221.5
2	[0.8882, 0.3152, 0.2809, 0.158, 0.0888]	[0,1,2,3,5]	476.4
3	[0.778, 0.4426, 0.3097, 0.3169, 0.0497]	[0,1,2,4,7]	791.2
4	[0.5795, 0.4745, 0.3885, 0.318, 0.2604, 0.213, 0.1745, 0.143, 0.117, 0.096]	[0,1,2,3,4,5,6,7,8,9]	1440

*Normalized tap coefficients for a sampling duration of $T_s = 520.833\,\text{ns}$.
† For a center frequency of $f_c = 2\,\text{GHz}$.

following cases are evaluated for SISO- and 4×4 MIMO-OFDM cases:

(a) Adaptive pilot spacing and power, $2 \leq \Delta_p t \leq 10, 2 \leq \Delta_p f \leq 8, -8\,\text{dB} \leq \rho \leq 0\,\text{dB}$.

(b) LTE Pilot spacing as shown in Figure 4.1, $\rho = -3\,\text{dB}$.

(c) Fixed pilot spacing and power, $\Delta_p t = 6, \Delta_p f = 6, \rho = -3\,\text{dB}$.

(d) Fixed pilot spacing and power, $\Delta_p t = 8, \Delta_p f = 8, \rho = -3\,\text{dB}$.

The diamond-shaped pilot patterns shown in Figure 3.9 are used for simulation of 4×4 MIMO-OFDM with full-rank spatial multiplexing. The other simulation parameters are presented in Table 2.2. We have used QPSK modulation on each data subcarrier of the OFDM symbol. For each case, the channel parameters τ_{rms} and f_d were held constant for $N_{OFDM} = 1500$ OFDM symbols. Using Algorithm 1, the channel scenario for case (a) was simulated using the codebook of Table 5.2.

5.3.0.1 Performance of Pilot Adaptation in SISO-OFDM

Figure 5.3 shows the ergodic capacity versus SNR for all considered pilot configurations (a)-(d). We see that pilot adaptation outperforms the other configurations for almost all values of SNR. We also see that the increase in channel capacity of pilot adaptation w.r.t. other fixed configurations improves with increasing E_b/N_0. This can be attributed to better estimation of channel statistics with higher SNR values. Figure 5.5 shows the channel capacity gain achieved by adapting pilot spacing and power. The capacity gain w.r.t. LTE spacing saturates at $\sim 10\%$ for higher values of SNR. The capacity gain w.r.t. other pilot configuration shows an almost linear increase with SNR.

Figure 5.4 shows the comparison of Cumulative Distribution Function (CDF) $F_C(C_s)$ of the capacity C for pilot adaptation versus LTE spacing. The CDF is given by

$$F_C(C_s) = \mathbf{P}[C \leq C_s] \tag{5.11}$$

where $\mathbf{P}[X \leq x]$ is the probability that the random variable X is less than or equal to x. We see that there is a significant performance improvement in the CDF, even at low SNR values. The non-existence of crossovers between the Cumulative Distribution Functions (CDFs) of the capacities of pilot adaptation and LTE spacing cases implies the achievability of throughput improvement using pilot adaptation under all operating conditions. The first three rows of Table 5.3 shows the average performance improvement of adaptive pilot configurations over the fixed pilot configurations.

5.3.0.2 Performance of Pilot Adaptation in MIMO-OFDM

Figure 5.6 shows the achievable ergodic capacity versus SNR for all the simulated pilot configurations for MIMO-OFDM. Similar to the case in SISO, we see that our pilot adaptation algorithm outperforms all fixed pilot configurations. Figure 5.7 shows the CDF of capacity for pilot pattern adaptation versus LTE spacing. We see that pilot pattern adaptation outperforms the LTE pilot pattern in all operating conditions. The capacity gains w.r.t. fixed pilot configurations is shown in Figure 5.8, where we see the capacity gains w.r.t. LTE spacing saturates at $\sim 20\%$. This behavior is likely because of the error floor introduced by the channel estimation algorithm in relatively fast fading and high τ_{rms} channel environments. Moreover, the matrix inversion operations in ZF receivers can result in relatively higher noise enhancement for fast fading scenarios even at high SNR values. This is seen as a clustering of the tail of the capacity CDF at $SNR = 13\,\mathrm{dB}$ and $SNR = 28\,\mathrm{dB}$. The last three rows of Table 5.3 summarize the capacity gains of pilot adaptation.

5.3.0.3 Variation of Capacity Gain with SNR

In Figures 5.5 and 5.8, we observe that the throughput gain of pilot adaptation w.r.t. that of LTE is not monotonically increasing as a function of the SNR. On the other hand, the throughput gain

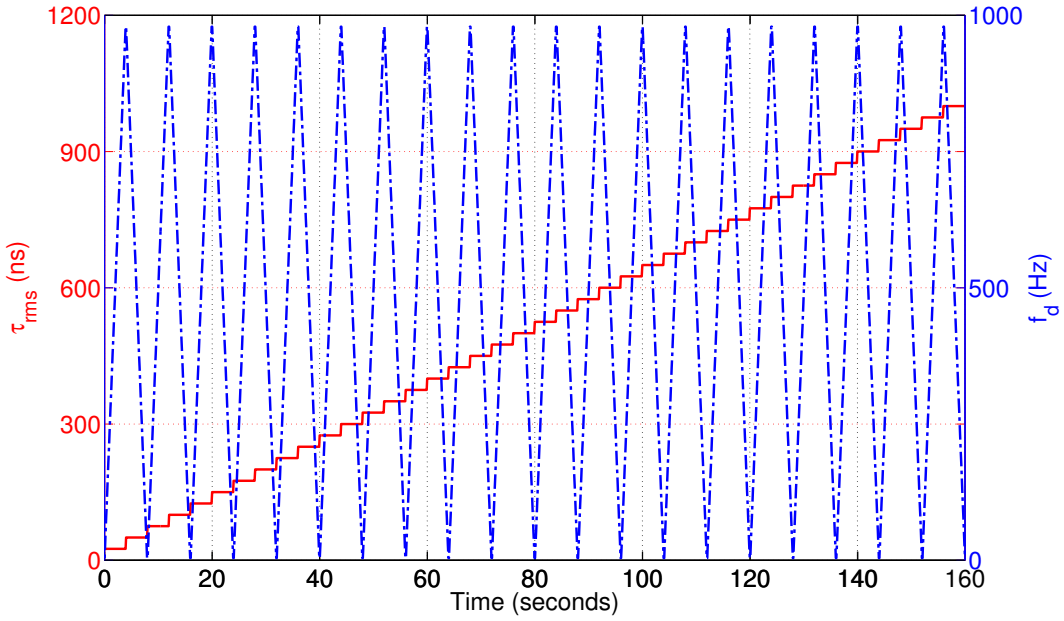

Figure 5.2: Scenario of channel statistics variation for all cases.

of pilot adaptation w.r.t. the other two fixed pilot spacing schemes increase monotonically. The capacity of each pilot configuration is dependent on the following factors:

(a) Average SNR (σ_n^2): It affects configurations with larger pilot spacing more.

(b) Channel estimation MSE (MSE_d): Increases with larger pilot spacing and vice versa. Also increases with increase in noise power σ_n^2.

(c) ICI power (σ_{ICI}^2): Affects all pilot configurations to the same extent.

(d) Spectral utilization function $(S(\Delta_p f, \Delta_p t))$: Increases with larger pilot spacing and vice versa.

By equation (5.3) the influence of ICI on all pilot schemes are almost the same. Hence changing the pilot spacing will not affect the ICI power significantly. By equations (5.2) and (2.16) - (2.26) it is clear that the channel estimation MSE MSE_d is dependent on the SNR. Also it is well known that the channel estimation MSE increases with increased pilot spacing. Using these ideas, the reasons for the observed trend in Figure 5.5 can be explained by the following arguments:

(a) At low SNR the channel statistics estimates in equation (5.9) is corrupted by high noise power. Hence pilot adaptation is not very effective in this SNR regime since the post-equalization SINR $\bar{\gamma}$ is dominated by the noise power σ_n^2. In this case, $\bar{\gamma}$ remains the same for almost all pilot patterns. Hence, capacity is determined almost exclusively by the spectral utilization function. Since LTE has a higher overhead due to a higher pilot density its capacity is lesser w.r.t. the other considered fixed pilot spacing schemes.

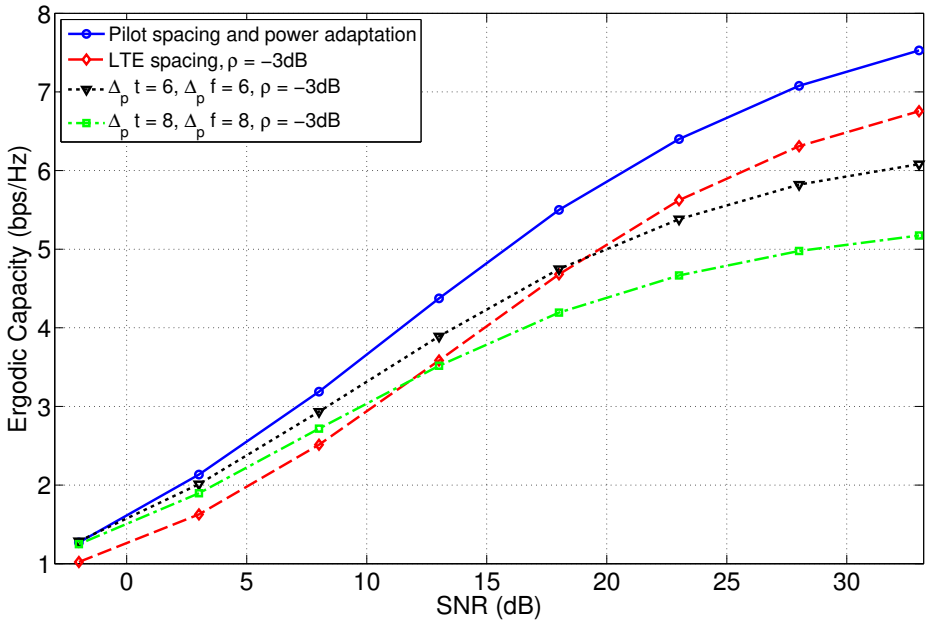

Figure 5.3: Ergodic Capacity Performance in SISO-OFDM for all considered pilot configurations.

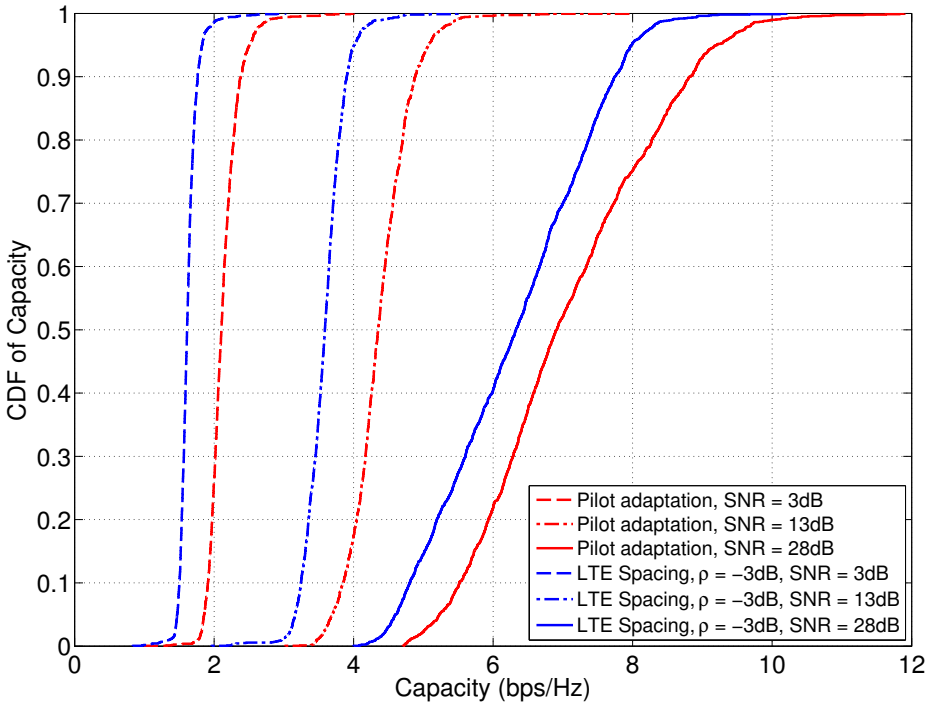

Figure 5.4: The CDF of Capacity for pilot adaptation versus LTE spacing, $\rho = -3\,\mathrm{dB}$ for SISO-OFDM.

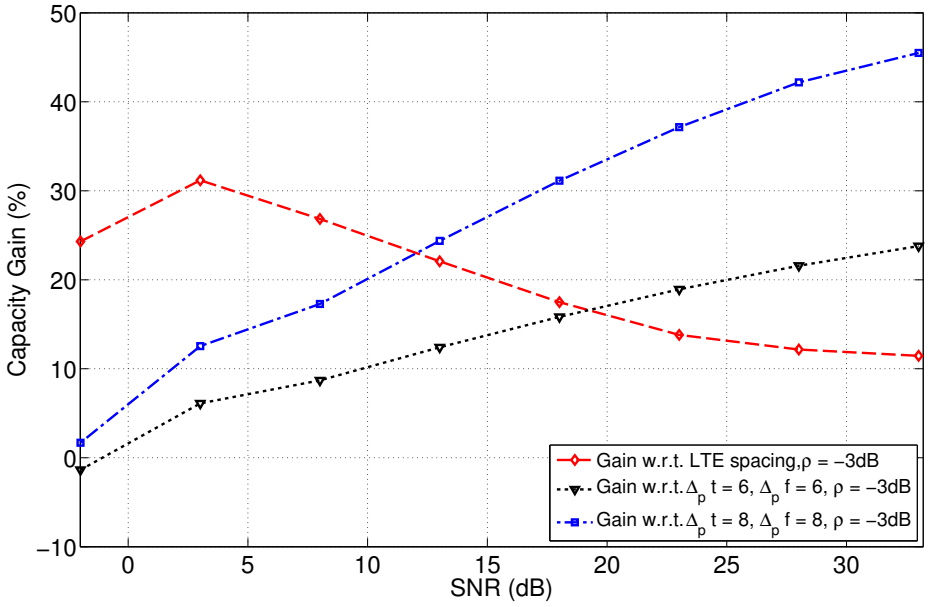

Figure 5.5: Capacity gain of pilot adaptation versus the other considered fixed pilot configurations for SISO-OFDM.

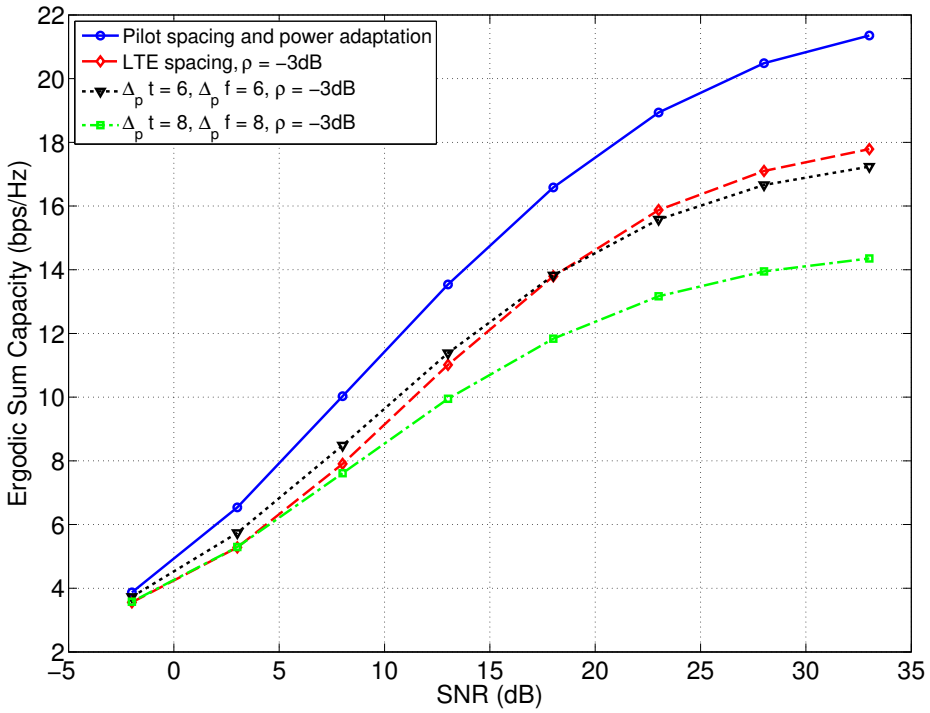

Figure 5.6: Ergodic Capacity Performance in MIMO-OFDM for all considered pilot configurations.

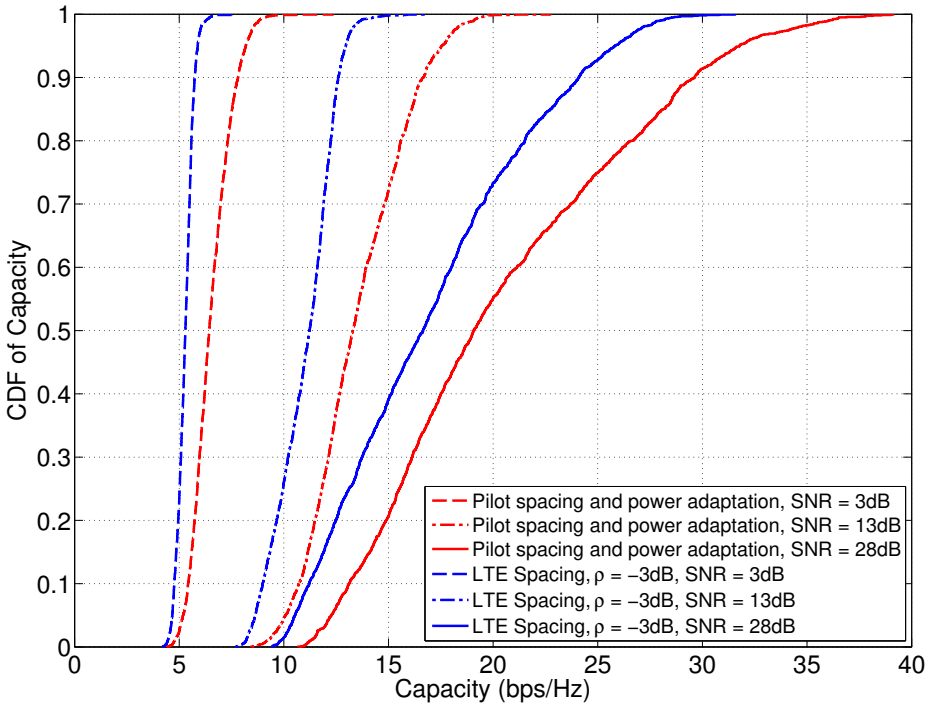

Figure 5.7: The CDF of capacity for pilot adaptation versus LTE spacing, $\rho = -3\,\mathrm{dB}$ for MIMO-OFDM.

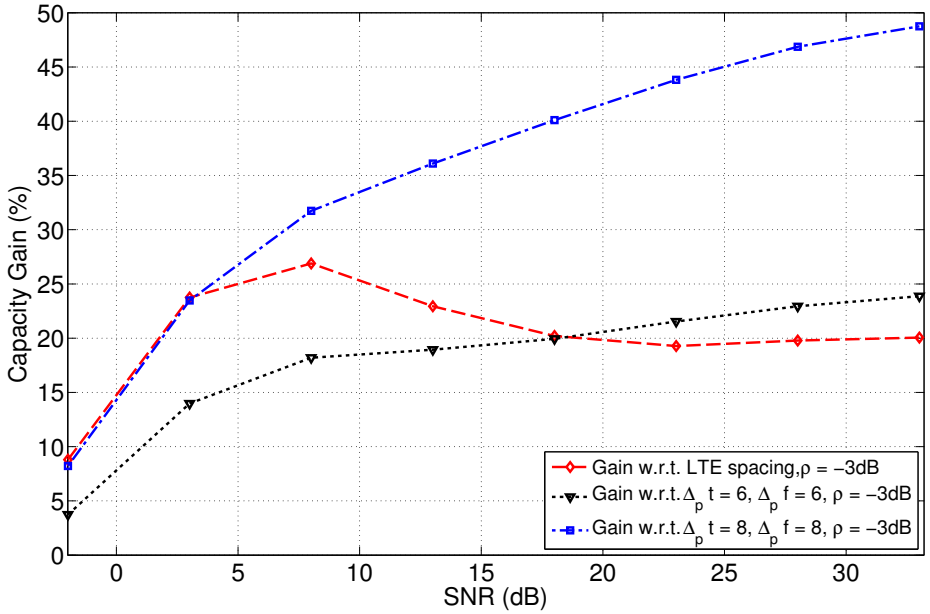

Figure 5.8: Capacity gain of pilot adaptation versus the other considered fixed pilot configurations for MIMO-OFDM.

(b) With increasing SNR the other factors begin to contribute to the capacity. On one hand the capacity improvements due to pilot adaptation begins to increase with increase in SNR. As the σ_n^2 value decreases the contribution of MSE_d term begins to dominate for all pilot spacing configurations. For LTE spacing its low spectral utilization decreases its capacity as compared to the other fixed pilot schemes. But as SNR increases, the other fixed pilot schemes begin to perform worse due to increasing MSE_d and their high spectral utilization becomes ineffective. Hence LTE eventually outperforms these schemes for $SNR \geq 20\,\mathrm{dB}$.

(c) For high values of SNR, MSE_d is dominated by the temporal and spectral channel correlation terms due to fading. At the same time the contribution of noise power σ_n^2 on MSE_d begins to decrease with increasing SNR. Therefore channel fading and ICI determines the capacity in this regime and pilot adaptation works accurately to track changes in the channel statistics. Since closer pilot spacing yields a lesser MSE_d value, LTE performs better while the other fixed pilot schemes lose capacity due to increased MSE_d.

(d) The capacity gain of pilot adaptation w.r.t. LTE spacing begins to saturate as SNR goes beyond $20\,\mathrm{dB}$. This is because the capacity begins to saturate in both LTE and pilot adaptation due to MSE_d, which does not depend on SNR in this regime. In other words, LTE spacing is close to the optimal pilot spacing for typical mobile wireless channels in high SNR conditions.

For the case of 4×4 MIMO-OFDM with full rank spatial multiplexing we see a similar trend in the capacity gains in Figure 5.8 as we do in the case of SISO-OFDM. Most of the arguments put forth above hold true here as well. However the performance of LTE spacing with that of the $\Delta_p t = \Delta_p f = 8, \rho = -3\,\mathrm{dB}$ case is similar at low SNR. This behavior is due to the fact that the channel estimation errors MSE_d accumulates on all 16 channel estimates (one channel estimate for each transmit-receive antenna pair) of the channel matrix $\mathbf{H}$ in equation (3.7). Hence the error due to MSE_d does not become negligible for very large pilot spacing.

However, it is clear that pilot adaptation outperforms all fixed pilot schemes as it balances channel estimation performance and pilot overhead for a wide range of channel fading statistics and noise conditions.

5.3.0.4 Comparison with the State of the Art

The authors in [56] have compared the performance of their pilot adaptation algorithm w.r.t. that of LTE. They have mapped each pilot pattern to a CQI value of LTE. Therefore, a flat fading channel in their case will result in (a) throughput gain due to overhead reduction of pilots, and (b) throughput scaling due to increased spectral efficiency as a result of higher modulation order (refer to Table 4.1). It is to be noted that:

1. They have considered data throughput as a metric for comparison, whereas we have considered ergodic capacity as a metric in order to compare our algorithm's performance versus

Table 5.3: Capacity gains of pilot adaptation w.r.t. fixed pilot configurations: comparison against state of the art

Baseline Pilot Configuration	Capacity Gain† (%)	Throughput Gain* (%) [56]
SISO, LTE Spacing	16.68‡	3-80
SISO, $\Delta_p t = 6, \Delta_p f = 6, \rho = -3\,\mathrm{dB}$	16.53	–
SISO, $\Delta_p t = 8, \Delta_p f = 8, \rho = -3\,\mathrm{dB}$	31.98	–
4×4 MIMO, LTE Spacing	20.6‡	40-850
4×4 MIMO, $\Delta_p t = 6, \Delta_p f = 6, \rho = -3\,\mathrm{dB}$	20.18	–
4×4 MIMO, $\Delta_p t = 8, \Delta_p f = 8, \rho = -3\,\mathrm{dB}$	39.62	–

† denotes gains averaged over all SNR values
$^{\ddagger}\rho = -3dB$
* In addition to pilot spacing and power, data modulation and coding scheme is adapted as well

several other fixed pilot configurations in addition to LTE.

2. The reported gains of pilot adaptation for SISO-OFDM in [56] are similar to what we have demonstrated. However, the maximum performance gain reported in [56] for MIMO-OFDM is an order of magnitude larger as compared to ours because of the adaptation of the modulation scheme as well, which tends to have a multiplicative effect.

Therefore, in this work, pilot adaptation is shown to outperform all fixed pilot configurations in both SISO- and MIMO-OFDM systems in terms of ergodic capacity. However, there still are a few practical considerations that need to be addressed before deployment in current LTE networks, which are discussed in the next section.

5.4 Some Practical Considerations for Pilot Adaptation in Current and Future Wireless Networks

The pilot adaptation scheme is dependent on the channel statistics estimated by the user that are fed back to the base station. Hence, the pilot patterns can vary among users in a cell with different channel statistics. This implies that pilot adaptation is not practical for pilots that are broadcasted in a cell as is the Cell-Specific Reference Signal (CRS) in LTE. Moreover, there are possibilities of pilot corruption due to pilot contamination between two cells if all types of pilots are adapted. We provide a few guidelines for pilot pattern adaptation:

1. Pilot adaptation cannot be directly implemented for broadcast pilots such as CRS.

2. It is well suited for user-specific pilots as, for e.g. UE specific Reference Signals of LTE [41].

3. It is also applicable for peer-to-peer links such as wireless backhaul, vehicular to vehicular, UAV to ground/UAV to UAV systems. In such systems, interference with other pilots typically does not arise.

4. Approaches like grouping of users having similar channel conditions during resource allocation [63] or active user-aware dynamic pilot distribution would be starting points for adaptation of broadcast pilots.

5.5 Conclusions

In this chapter, we developed a simple codebook-based algorithm to adapt the pilot spacing and power in SISO- and MIMO-OFDM systems. Using pilot adaptation, we demonstrated a channel capacity gain of about 10-30% for SISO, and 10-27% for 4×4 MIMO-OFDM w.r.t. the fixed LTE pilot configuration. Monte-Carlo simulations showed that pilot adaptation outperforms all fixed pilot configurations for almost all SNR values in a non-stationary wireless channel with smoothly varying channel statistics. We also discussed a scheme to reduce the channel statistics feedback requirements for inter-band carrier aggregation systems.

A ten-fold increase in spectral efficiency is expected to be necessary to meet the traffic demands of future 5G networks. Pilot pattern adaptation alone has the potential to enhance the spectral efficiency by $1.5 - 2\times$ (excluding the effects of adaptive modulation and coding), which is a necessary first step to reduce overhead in the transport blocks of current wireless networks.

Chapter 6

Conclusions and Future Work

6.1 Thesis Summary and Conclusions

This thesis investigated the role of pilot signals in the evolution of wireless networks. We focused on the resilience of pilots to targeted interference and on optimizing its density to maximize channel capacity as a function of the channel conditions in the absence of targeted interference. We also experimented with the LTE downlink to study its robustness to targeted interference on the CRS (downlink pilot signals) and, to the best of our knowledge, demonstrated the 'CQI spoofing attack' in LTE for the first time. The key conclusions of this thesis are outlined below.

In Chapter 2, we provided theoretical expressions for BER and channel estimation MSE, both in the presence as well as absence of a multi-tone pilot jammer. We estimated that multi-tone pilot jamming has the potential to disrupt communications by transmitting about $9\,\mathrm{dB}$ less power than the target signal if synchronized perfectly with its target (for pilot densities similar to the ones used in LTE). The theoretical and simulated performance was found to be very close to each other, validating the accuracy of our simulator.

In Chapter 3, we proposed and evaluated methods to counter a pilot jammer in both SISO- and MIMO-OFDM scenarios. For SISO-OFDM it was seen that for an asynchronous pilot jammer, there was an improvement in the channel estimation performance. To improve the BER performance, complementary methods such Adaptive Modulation and Coding, Hybrid ARQ are necessary. For MIMO-OFDM, we explored whether full rank spatial-multiplexing operation is possible in the presence of a synchronous power-constrained pilot jammer. We devised a simple cancellation scheme for such jammers by exploiting the channel flatness in either the time or frequency dimensions to cancel out the interference. We demonstrated that such cancellation can achieve $\sim 50 - 90\%$ of the interference-free ergodic sum capacity in 4×4 MIMO with full rank spatial multiplexing.

In Chapter 4, we demonstrated the problem of 'CRS Jamming' and 'CQI Spoofing' in the LTE

Downlink. Our RF measurements with 3GPP-compliant LTE test systems showed that CRS Jamming required $\sim 5\,\mathrm{dB}$ less power than Barrage Jamming to cause DoS at the UE. Pilot jammer evasion by cyclic shifting of pilot locations proved to be ineffective due to the inability of the UE to track the channel quality correctly. We have identified this to be a problem as severe as 'CRS Jamming' and conclude that further research on accurate CQI estimation/correction algorithms in the presence of targeted interference is necessary.

Finally in Chapter 5, we investigated the idea of pilot pattern adaptation in SISO- and MIMO-OFDM systems. We developed a simple codebook-based approach to adapt the pilot spacing and power in SISO- and MIMO-OFDM systems, which demonstrated a channel capacity gain of about 10-30 % for SISO, and 10-27% for 4×4 MIMO-OFDM w.r.t. the fixed LTE pilot configuration. Monte-Carlo simulations showed that pilot adaptation outperforms all fixed pilot configurations for almost all SNR values in nonstationary channels with smoothly varying channel statistics. We also discussed some practical constraints that need to be addressed before pilot adaptation can be implemented into current and future wireless standards.

6.2 Future Work

There can be several extensions to this work, some of which are categorized below.

6.2.1 Enhanced Mitigation Algorithms for Pilot Jamming

In this work, we have considered a power-constrained jammer that reduces its symbol rate w.r.t. the target signal to localize most of its power on pilot subcarriers. Mitigation strategies are necessary to deal with jammers which transmit at the same symbol rate as the target OFDM symbol. In this case, the jammer needs to be closely tracked in every symbol duration. This will prove useful to make the pilot signals more resilient against jamming.

In addition, jamming of uplink pilots in schemes like Single Carrier-Frequency Division Multiple Access (SC-FDMA) will also be a worthwhile effort, especially considering the fact that the received power of the uplink signal will always be order of magnitudes lower than that of the downlink signal.

6.2.2 Improving Resilience of LTE

This work specifically focused on the resilience of pilots to targeted interference in LTE. An immediate problem to be fixed in LTE is 'CQI Spoofing' and development of better CQI estimation algorithms is necessary to improve the throughput performance of LTE when the jammer explicitly avoids interfering with pilot locations of the LTE signal.

New threats will emerge with newer releases of LTE and it will be crucial to investigate the robustness of the LTE standard to these attacks.

6.2.3 Cross-layer Optimization in Interference Channels

Chapter 4 identified the problems caused by interference when assumptions go wrong during system design. Most CQI estimation algorithms are developed to optimize performance in frequency selective mobile fading channels. The same algorithm causes performance degradation when intentional or unintentional interference is present on data subcarriers. The ramifications of this interference on higher layers needs more research in order to design better protocols for 5G.

6.2.4 Trust-Aware Protocol Design

The performance of each layer depends on the layers below it in the protocol stack. In current protocols each layer trusts the input it gets from other layers. An interesting paradigm shift would be to investigate the effect of establishing different levels of trust between all layers of the protocol, on the system performance. Incorporating trust between layers into protocol design has the potential to mitigate undesired behavior in the presence of protocol-aware attackers.

6.2.5 Pilot Pattern Adaptation

Some constraints of pilot adaptation were highlighted in chapter 5 of this thesis. Considerable research effort is necessary to overcome the inherent constraints of adapting broadcast pilots. Since broadcast pilots comprise a major chunk of the essential overhead in the physical layer signal, it will be interesting to see if broadcast pilot patterns can be adapted at all, using techniques like the ones described in [63]. An interesting problem would be to solve the optimization problem posed in equation (5.1) in the presence of a multi-tone pilot jammer that constantly tracks changes in the pilot pattern of its target.

For 5G networks, alternate multicarrier waveforms such as Filter-bank Multicarrier (FBMC), Universal Filtered Multicarrier (UFMC) [5] are being actively researched. Like other multicarrier waveforms, pilot-aided channel estimation is the preferred method to equalize the FBMC signals [64]. Hence, algorithms to adapt pilot patterns to maximize throughput are necessary. Since they have different sources of interference than OFDM, it is necessary to be modeled accurately. The formulation of the cost function that maximizes the channel capacity (or its upper bound) for all potential waveforms would be a significant contribution to choose and optimize the PHY layer for 5G.

Appendix A

Additional Throughput Measurement Results

In chapter 4 the performance of LTE downlink in the presence of targeted interference was investigated. This appendix presents additional results to support our findings and conclusions in chapter 4. The throughput was measured for the LTE downlink in the following scenarios:

(a) CRS jamming,

(b) Data subcarrier jamming (one out of every three subcarriers),

(c) Barrage jamming.

The measurements were carried out for four trials for each of the above scenarios. The measurement results are shown in Table A.1. The following parameters are shown as a function of JSR for each case:

(a) Mean (μ) of measured throughput $\bar{R}_{meas}$,

(b) Standard deviation (σ) of measured throughput $\bar{R}_{meas}$,

(c) Median value of the reported Modulation and coding scheme (MCS).

An important takeaway from this table is the reported median MCS values for data subcarrier jamming. A high value of MCS in the presence of targeted interference results in a higher number of errors that reduces the throughput. Hence accurate CQI estimation algorithms are necessary to optimize the performance in the presence of targeted interference on data subcarriers.

Table A.1: Summary of statistics of measured throughput in the LTE jamming experiments.

JSR per	CRS			Data subcarriers (1 in 3)			Barrage		
RB (dB)	$\mu^{\ddagger}$	$\sigma^{\ddagger}$	MCS†	$\mu^{\ddagger}$	$\sigma^{\ddagger}$	MCS†	$\mu^{\ddagger}$	$\sigma^{\ddagger}$	MCS†
-15	14.99	0.057	18	14.13	0.0825	27	$\star$	$\star$	$\star$
-14	14.13	0.956	17	14.07	0.014	27	$\star$	$\star$	$\star$
-13	12.10	1.102	15	14.15	0.24	27	$\star$	$\star$	$\star$
-12	10.39	0.057	13	13.97	0.08	27	$\star$	$\star$	$\star$
-11	10.42	0.017	13	12.86	1.238	27	$\star$	$\star$	$\star$
-10	9.19	1.003	12	9.51	0.347	26	15.33	0.085	18
-9	8.01	0.028	11	9.1	0.202	26	14.86	0.172	18
-8	7.09	0.674	11	8.14	0.406	25	13.29	0.033	17
-7	5.81	0.76	8	7.57	0.524	24	11.61	0.107	15
-6	4.87	0.25	6	5.75	0.596	24	10.82	0.021	14
-5	4.68	0.035	6	3.39	1.822	22	10.29	0.261	13
-4	4.24	0.65	5	3.72	2.073	21	8.58	0.252	12
-3	3.66	0.57	5	4.47	0.056	20	8.29	0.068	12
-2	2.94	0.408	4	3.90	0.351	19	6.84	0.071	9
-1	2.16	0.140	3	3.29	0.389	18	6.46	0.055	8
0	1.70	0.126	3	1.44	1.043	18	5.18	0.02	7
1	0.938	0.503	3	1.01	1.348	15	4.86	0.077	7
2	0.898	0.042	2	0.39	0.547	13	4.01	0.214	6
3	0.581	0.076	0	0	0	$*$	3.1	0.107	5
4	0.084	0.103	0	0	0	$*$	2.41	0.190	5
5	0	0	$*$	0	0	$*$	1.82	0.133	5
6	0	0	$*$	0	0	$*$	1.31	0.319	3
7	0	0	$*$	0	0	$*$	0.452	0.289	2
8	0	0	$*$	0	0	$*$	0.153	0.108	1
9	0	0	$*$	0	0	$*$	0	0	$*$
Average	–	0.360	–	–	0.541	–	–	0.123	–

‡ measured in Mbps
† median value of measured MCS
$\star$ no measurements
– not applicable
$*$ UE disconnected

Bibliography

[1] S. Sesia, M. Baker, and I. Toufik, *LTE-The UMTS Long Term Evolution: From Theory to Practice*. John Wiley & Sons, 2011.

[2] ETSI, "LTE, Evolved Universal Terrestrial Radio Access (E-UTRA), Physical Layer Procedures (3GPP TS 36.213 v 12.4.0), Release 12," *3GPP*, 2015.

[3] 3GPP, "Releases," http://www.3gpp.org/specifications/67-releases, 2016, [Online; accessed 19-July-2016].

[4] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What Will 5G Be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[5] P. Banelli, S. Buzzi, G. Colavolpe, A. Modenini, F. Rusek, and A. Ugolini, "Modulation Formats and Waveforms for 5G Networks: Who Will Be the Heir of OFDM?: An overview of alternative modulation schemes for improved spectral efficiency," *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 80–93, Nov 2014.

[6] S. Schwarz and M. Rupp, "Society in motion: challenges for LTE and beyond mobile communications," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 76–83, May 2016.

[7] T. C. Clancy, "Efficient OFDM Denial: Pilot Jamming and Pilot Nulling," in *Communications (ICC), IEEE International Conference on*, June 2011, pp. 1–5.

[8] C. Shahriar, R. McGwier, and T. C. Clancy, "Performance impact of pilot tone randomization to mitigate OFDM jamming attacks," in *Consumer Communications and Networking Conference (CCNC), IEEE*, Jan 2013, pp. 813–816.

[9] C. S. Patel, G. L. Stuber, and T. G. Pratt, "Analysis of OFDM/MC-CDMA under channel estimation and jamming," in *Wireless Communications and Networking Conference (WCNC), IEEE*, vol. 2, March 2004, pp. 954–958 Vol.2.

[10] M. Han, T. Yu, J. Kim, K. Kwak, S. Lee, S. Han, and D. Hong, "OFDM Channel Estimation With Jammed Pilot Detector Under Narrow-Band Jamming," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 3, pp. 1934–1939, May 2008.

[11] J. A. Mahal and T. C. Clancy, "The closed-form BER expressions of PSK modulation for OFDM and SC-FDMA under jamming and imperfect channel estimation," in *Communications (ICC), IEEE International Conference on*, June 2014, pp. 2221–2226.

[12] C. Shahriar, T. C. Clancy, and R. W. McGwier, "Equalization attacks against OFDM: analysis and countermeasures," *Wireless Communications and Mobile Computing*, pp. n/a–n/a, 2015. [Online]. Available: http://dx.doi.org/10.1002/wcm.2648

[13] C. A. Cole, C. Shahriar, and T. C. Clancy, "An Anti-jam Communications Technique via Spatial Hiding Precoding," in *IEEE Military Communications Conference*, Oct 2014, pp. 490–494.

[14] G. D. Durgin, V. Kukshya, and T. S. Rappaport, "Wideband measurements of angle and delay dispersion for outdoor and indoor peer-to-peer radio channels at 1920 MHz," *IEEE Transactions on Antennas and Propagation*, vol. 51, no. 5, pp. 936–944, May 2003.

[15] J. Kakar, K. McDermott, V. Garg, M. Lichtman, V. Marojevic, and J. H. Reed, "Analysis and Mitigation of Interference to the LTE Physical Control Format Indicator Channel," in *IEEE Military Communications Conference*, Oct 2014, pp. 228–234.

[16] M. Lichtman, T. Czauski, S. Ha, P. David, and J. H. Reed, "Detection and Mitigation of Uplink Control Channel Jamming in LTE," in *IEEE Military Communications Conference*, Oct 2014, pp. 1187–1194.

[17] M. Labib, V. Marojevic, and J. H. Reed, "Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing," in *IEEE Conference on Standards for Communications and Networking (CSCN)*, Oct 2015, pp. 315–320.

[18] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic, and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 54–61, April 2016.

[19] R. P. Jover, J. Lackey, and A. Raghavan, "Enhancing the security of LTE networks against jamming attacks," *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1–14, 2014.

[20] O. Sallent and R. Ferrs, *Mobile Broadband Communications for Public Safety: The Road Ahead Through LTE Technology*. John Wiley & Sons, 2015.

[21] C. Shahriar, M. L. Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed, "PHY-Layer Resiliency in OFDM Communications: A Tutorial," *IEEE Communications Surveys Tutorials*, vol. 17, no. 1, pp. 292–314, First quarter 2015.

[22] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, Jan 1983.

[23] M. K. Ozdemir and H. Arslan, "Channel estimation for wireless OFDM systems," *IEEE Communications Surveys Tutorials*, vol. 9, no. 2, pp. 18–48, second quarter 2007.

[24] L. Jun, J. H. Andrian, and C. Zhou, "Bit Error Rate Analysis of jamming for OFDM systems," in *Wireless Telecommunications Symposium*, April 2007, pp. 1–8.

[25] I. Barhumi, G. Leus, and M. Moonen, "Optimal training design for MIMO-OFDM systems in mobile wireless channels," *IEEE Transactions on Signal Processing*, vol. 51, no. 6, pp. 1615–1624, June 2003.

[26] C. R. N. Athaudage and A. D. S. Jayalath, "Low-complexity channel estimation for wireless OFDM systems," in *Personal, Indoor and Mobile Radio Communications, 14th IEEE Proceedings on*, vol. 1, Sept 2003, pp. 521–525.

[27] Y. Li, "Pilot-symbol-aided channel estimation for OFDM in wireless systems," *IEEE Transactions on Vehicular Technology*, vol. 49, no. 4, pp. 1207–1215, Jul 2000.

[28] W. C. Jakes and D. C. Cox, *Microwave mobile communications*. Wiley-IEEE Press, 1994.

[29] R. Ratasuk, N. Mangalvedhe, A. Ghosh, and B. Vejlgaard, "Narrowband LTE-M System for M2M Communication," in *IEEE 80th Vehicular Technology Conference (VTC 2014-Fall)*, Sept 2014, pp. 1–5.

[30] J. Kim, J. Park, and D. Hong, "Performance analysis of channel estimation in OFDM systems," *Signal Processing Letters, IEEE*, vol. 12, no. 1, pp. 60–62, Jan 2005.

[31] Y. Li and L. J. Cimini, "Bounds on the interchannel interference of OFDM in time-varying impairments," *IEEE Transactions on Communications*, vol. 49, no. 3, pp. 401–404, 2001.

[32] M.-X. Chang and Y. T. Su, "Performance analysis of equalized OFDM systems in Rayleigh fading," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 721–732, Oct 2002.

[33] R. Nissel, M. Lerch, M. Simko, and M. Rupp, "Bit Error Probability for Pilot-Symbol-Aided OFDM Channel Estimation in Doubly-Selective Channels," in *Smart Antennas (WSA), 18th International ITG Workshop on*, March 2014, pp. 1–6.

[34] L. C. Godara, "Application of antenna arrays to mobile communications. II. Beam-forming and direction-of-arrival considerations," *Proceedings of the IEEE*, vol. 85, no. 8, pp. 1195–1245, Aug 1997.

[35] Q. H. Spencer, A. L. Swindlehurst, and M. Haardt, "Zero-forcing methods for downlink spatial multiplexing in multiuser MIMO channels," *IEEE Transactions on Signal Processing*, vol. 52, no. 2, pp. 461–471, Feb 2004.

[36] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. T. Hou, "Jamming Resilient Communication Using MIMO Interference Cancellation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1486–1499, July 2016.

[37] S. Sodagari and T. C. Clancy, "Efficient jamming attacks on MIMO channels," in *IEEE International Conference on Communications (ICC)*, June 2012, pp. 852–856.

[38] S. Amuru and R. M. Buehrer, "Optimal jamming against digital modulation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2212–2224, Oct 2015.

[39] J. G. Proakis and M. Salehi, *Digital Communications*. McGraw-Hill, 2007.

[40] T. Li, W. H. Mow, V. K. N. Lau, M. Siu, R. S. Cheng, and R. D. Murch, "Robust joint interference detection and decoding for OFDM-based cognitive radio systems with unknown interference," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 566–575, April 2007.

[41] ETSI, "LTE, Evolved Universal Terrestrial Radio Access (E-UTRA), Requirements for support of radio resource management (3GPP TS 36.133 v 10.1.0), Release 10," *3GPP*, 2011.

[42] ——, "LTE, Evolved Universal Terrestrial Radio Access (E-UTRA), Physical Channels and Modulation (3GPP TS 36.211 v 9.1.0), Release 9," *3GPP*, 2010.

[43] H. Yang, A. Huang, R. Gao, T. Chang, and L. Xie, "Interference Self-Coordination: A Proposal to Enhance Reliability of System-Level Information in OFDM-Based Mobile Networks via PCI Planning," *IEEE Transactions on Wireless Communications*, vol. 13, no. 4, pp. 1874–1887, April 2014.

[44] A. Paulraj, R. Nabar, and D. Gore, *Introduction to Space-time Wireless Communications*. Cambridge University Press, 2003.

[45] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 74–80, February 2014.

[46] S. Amuru, "Intelligent Approaches for Communication Denial," Ph.D. dissertation, Virginia Tech, September 2015.

[47] M. Simko, "Pilot Pattern Optimization for Doubly-Selective MIMO OFDM Transmissions," Ph.D. dissertation, Vienna University of Technology, May 2013.

[48] T. Doumi, M. F. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, D. Flore, "LTE for Public Safety Networks," *Communications Magazine, IEEE*, vol. 51, no. 2, pp. 106–112, 2013.

[49] "Amarisoft LTE100," http://amarisoft.com/document/Amarisoft_LTE100.pdf, 2016, [Online; last accessed 14-July-2016].

[50] "GNURadio," http://gnuradio.org/, 2016, [Online; last accessed 1-August-2016].

[51] "iPerf-The network bandwidth measurement tool," https://iperf.fr/, 2016, [Online; last accessed 1-August-2016].

[52] A. Barbieri, J. Tingfang, P. A. Agashe, Y. Wei, T. Yoo, T. Luo, M. S. Vajapeyam, H. Xu, and A. Damnjanovic, "CQI Estimation in a Wireless Communication Network," Oct. 13 2011, US Patent App. 13/084,154.

[53] A. M. Mansour, A. E. R. Nada, and A. H. Mehana, "Effect of noise variance estimation on channel quality indicator in lte systems," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, Dec 2015, pp. 156–160.

[54] W. Zhang, X.-G. Xia, and P.-C. Ching, "Optimal training and pilot pattern design for OFDM systems in Rayleigh fading," *Broadcasting, IEEE Transactions on*, vol. 52, no. 4, pp. 505–514, 2006.

[55] O. Simeone and U. Spagnolini, "Adaptive pilot pattern for OFDM systems," in *Communications, 2004 IEEE International Conference on*, vol. 2. IEEE, 2004, pp. 978–982.

[56] M. Simko, P. S. Diniz, Q. Wang, and M. Rupp, "Adaptive pilot-symbol patterns for MIMO OFDM systems," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 9, pp. 4705–4715, 2013.

[57] "WiMAX System Evaluation Methodology," http://www.cse.wustl.edu/~jain/wimax/ftp/wimax_system_evaluation_methodology_v2_1.pdf, July 7, 2008, accessed: 2nd-August-2016.

[58] L. Bernad, T. Zemen, F. Tufvesson, A. F. Molisch, and C. F. Mecklenbruker, "Delay and Doppler Spreads of Nonstationary Vehicular Channels for Safety-Relevant Scenarios," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 1, pp. 82–93, Jan 2014.

[59] D. Gore, R. W. Heath, and A. Paulraj, "On Performance of the Zero Forcing Receiver in Presence of Transmit Correlation," in *Proceedings of the IEEE International Symposium on Information Theory*, 2002, p. 159.

[60] F. A. Dietrich and W. Utschick, "Pilot-assisted channel estimation based on second-order statistics," *IEEE Transactions on Signal Processing*, vol. 53, no. 3, pp. 1178–1193, 2005.

[61] ITU, "ITURM Recommendation: 1225, Guidelines for evaluation of radio transmission technologies for IMT-2000," *International Telecommunication Union*, 1997.

[62] 3GPP, "User Equipment (UE) Radio Transmission and Reception," *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA)*, 2014.

[63] N. Ksairi, B. Tomasi, and S. Tomasin, "Pilot Pattern Adaptation for 5G MU-MIMO Wireless Communications," *arXiv preprint arXiv:1605.05061*, 2016.

[64] W. Cui, D. Qu, T. Jiang, and B. Farhang-Boroujeny, "Coded auxiliary pilots for channel estimation in fbmc-oqam systems," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 5, pp. 2936–2946, May 2016.