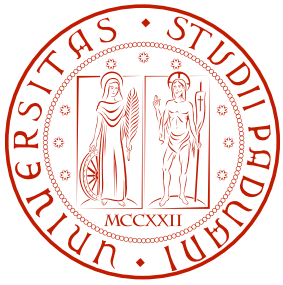

Università degli Studi di Padova

Dipartimento di Ingegneria dell'Informazione

Scuola di Dottorato in Ingegneria dell'Informazione

Indirizzo in Scienze e Tecnologie dell'Informazione

XXIII Ciclo

OFDM in Emerging Wireless Networks: Synchronization Algorithms and Physical Layer Security

Tesi di: *Francesco Renna*

Supervisore:
Prof. Nicola Laurenti

Direttore della Scuola:
Prof. Matteo Bertocco

Anno Accademico 2010/2011

Contents

Abstract

In the last decade, orthogonal frequency division multiplexing (OFDM) has been chosen as the physical layer solution for a large variety of wireless, high data rates communication standards. The reasons for this success are found in the possibility of coping with frequency selective channels with simple and efficiently implemented transceivers, and achieving high spectral efficiency. In order to push the performance of these systems close to their limit, emerging wireless networks need efficient methods for time and frequency synchronization, since an erroneous choice of the symbol timing and residual offsets in the clock and carrier frequencies at the transmitter and the receiver can highly impair transmissions due to the effects of intersymbol interference (ISI) and interchannel interference (ICI).

In the first part of this thesis we focus on time and frequency synchronization algorithms for ultrawide band (UWB) multiband (MB) OFDM systems. First, we consider the time synchronization problem and we analyze the case when the channel delay spread is larger than the cyclic prefix length determined by the standard, that is when ISI and ICI can not be completely avoided with a proper symbol timing. In this case, we identify as an appropriate target for synchronization the maximization of the ratio of the total useful received power over all subcarriers to the total power of ISI and ICI for a given channel realization. We also present a practical low-complexity synchronization scheme and show that its performance tops the results obtained by the best existing correlation-based timing estimators.

Moreover, the very high transmission rate of MB-OFDM architectures asks for carrier and clock frequency offset estimators with moderate complexity and fast acquisition times. Then, we formulate algorithms that are based upon the received frequency domain symbols, where the effects of both offsets can be observed, and jointly estimate them with either a linear least squares or a maximum likelihood approach. The performance of the algorithms is assessed through simulation in a realistic UWB channel scenario and compared with previous literature results.

In parallel with the request for large transmission rates, the use of sensitive data over wireless communications has raised an increasing demand for confidentiality (and security in general) of the transmitted information. Physical layer security is emerging as a valuable tool for future wireless networks to secure information directly at the physical layer by exploiting the channel diversity at the legitimate nodes and the attacker.

In the second part of this thesis, we consider how information-theoretic security results can be adapted and applied to systems that adopt OFDM as the modulation format. The multicarrier architecture is modeled as a particular instance of a multiple-input multiple-output (MIMO) channel. In this way, we are able to evaluate the capabilities of the OFDM system in transmitting confidential messages by leveraging the results presented in the literature for the MIMO Gaussian wiretap channel. We evaluate the information-theoretic secrecy rates that are achievable by an OFDM transmitter/receiver pair in the presence of an eavesdropper that might either use an OFDM structure or choose a more complex receiver architecture.

The physical layer features of the communication channels can be used not only to transmit secret messages but also to share secret keys. We consider the general case of secret-key agreement over MIMO channels (of which OFDM can be seen as a particular case) and we establish closed-form expressions for the secret-key capacity in the low-power and high-power regimes. In the low-power regime, we show that the optimal signaling strategy is independent of the eavesdropper's fading realization. By combining this signaling strategy with reconciliation and privacy amplification, one obtains a semi-blind key-distillation strategy in which the knowledge of the eavesdropper's fading is required for privacy amplification alone.

A similar approach is used to study the jamming game in an OFDM environment. In this scenario, the attacker is active and its objective is to disrupt the communication between the legitimate users by transmitting a jamming signal. The setup is modeled as a zero-sum game in which the payoff function is represented by the mutual information between the transmitter and the receiver. Optimal signaling strategies are determined for both the transmitter and the jammer, and the Nash equilibrium of the game is found for both discrete multitone (DMT) and filtered multitone (FMT) architectures.

Sommario

Nell'ultimo decennio, la tecnica nota come *orthogonal frequency division multiplexing* (OFDM) è stata scelta come soluzione di strato fisico per diversi sistemi di trasmissione *wireless* ad alto *bit rate*. Le ragioni di tale successo sono riscontrabili nella capacità di sfruttare canali selettivi in frequenza con dispositivi di semplice ed efficiente implementazione, nonché nella possibilità di ottenere un'elevata efficienza spettrale. Allo scopo di ottimizzare le prestazioni di questi sistemi, le reti *wireless* di nuova generazione necessitano di metodi efficaci per la sincronizzazione di tempo e di frequenza, dato che un'errata scelta del sincronismo di simbolo ed *offset* di frequenza residui di portante e campionamento possono disturbare fortemente le trasmissioni a causa dell'introduzione di interferenza di intersimbolo (ISI) ed interferenza di intercanale (ICI).

Nella prima parte della tesi il lavoro si è concentrato sulla formulazione e l'analisi di algoritmi di sincronizzazione di tempo e frequenza per sistemi *ultrawide band* (UWB) *multi-band* (MB) OFDM. Per prima cosa è stato considerato il problema della sincronizzazione di simbolo ed è stato analizzato il caso in cui la lunghezza del canale dispersivo è maggiore di quella del prefisso ciclico previsto dallo standard, ovvero quando sia ISI che ICI non possono essere completamente annullate scegliendo in maniera opportuna l'epoca di campionamento. In questo caso, un opportuno obiettivo per la sincronizzazione di simbolo è stato identificato nella massimizzazione del rapporto fra la potenza utile totale su tutte le sottoportanti e la potenza totale di ISI ed ICI, per una data realizzazione di canale. È stato anche derivato uno schema di sincronizzazione pratico a bassa complessità computazionale, che offre prestazioni migliori di quelle fornite dagli stimatori a correlazione esistenti in letteratura.

Inoltre, l'alto *rate* di trasmissione dei sistemi MB-OFDM richiede che la stima degli *offset* di campionamento e di portante venga effettuata con metodi a complessità moderata e con tempi di acquisizione ridotti. Pertanto, sono stati formulati algoritmi che operano sui sim-

boli ricevuti nel dominio della frequenza, dai quali è possibile rilevare gli effetti di entrambi gli *offset*, che vengono così stimati congiuntamente mediante approcci ai minimi quadrati o a massima verosimiglianza. Le prestazioni di questi algoritmi sono state valutate mediante simulazioni in uno scenario UWB realistico e sono state confrontate con i risultati ottenuti dagli stimatori presentati precedentemente in letteratura.

In parallelo con la richiesta di elevati *rate* di trasmissione, l'imponente traffico di dati sensibili attraverso comunicazioni *wireless* ha generato un bisogno crescente di segretezza (e sicurezza in generale) per l'informazione trasmessa su tali canali. La sicurezza a livello di strato fisico si sta rivelando un utile strumento per proteggere l'informazione trasmessa su reti *wireless* di nuova generazione, e sfrutta la diversità esistente fra le realizzazioni di canale dei terminali legittimi rispetto a quelle dell'attaccante.

Quindi, nella seconda parte della tesi, si è valutato come i risultati ottenuti nell'ambito dell'*information-theoretic security* possano essere adattati ad un sistema che adotta OFDM come tipo di modulazione. L'architettura multiportante è stata quindi rappresentata come un caso particolare di un canale *multiple-input multiple-output* (MMO). In questo modo è stato possibile valutare le potenzialità del sistema OFDM nel trasmettere messaggi riservati applicando ed adattando a questo caso i risultati presentati in letteratura riguardo canali *wiretap* MIMO gaussiani. Si sono così caratterizzati i *rate* di segretezza raggiungibili da una coppia trasmettitore/ricevitore OFDM in presenza di un ascoltatore indesiderato, sia nel caso in cui esso adotti un ricevitore di tipo OFDM, sia nel caso in cui esso possa implementare architetture di ricezione più complesse e sofisticate.

Le caratteristiche fisiche del canale di trsmissione possono essere sfruttate non solo per trasmettere messaggi in maniera che il loro contenuto sia segreto per eventuali attaccanti, ma anche per condividere in maniera sicura chiavi segrete, da utilizzare in sistemi di crittografia classica. In particolare, si è studiato il caso generale di condivisione di chiavi segrete mediante trasmissioni su canali MIMO (di cui OFDM può essere pensato come istanza particolare) e si sono ricavate in forma chiusa le espressioni per la capacità di chiavi segreta (ovvero il massimo *rate* con cui può essere scambiata una chiave segreta in presenza di un attaccante) nei regimi asintotici di basso ed alto SNR. Per bassi SNR, è stato dimostrato come la strategia ottima di trasmissione sia indipendente dalla realizzazione di canale dell'attaccante. Pertanto, combinando questa strategia di trasmissione con le fasi di *information reconciliation* e *privacy amplification*, è possibile ottenere uno schema di condivisione di chiavi di tipo *semi-blind*, per il quale la conoscenza del canale dell'attaccante è rischiesta solo nella fase finale

di *privacy amplification*.

Un approccio simile a quelli descritti finora è stato applicato per studiare il problema della robustezza dei sistemi OFDM ad attacchi di *jamming*. In questo scenario l'attaccante è attivo, ed il suo scopo è quello di disturbare la comunicazione fra i terminali legittimi mediante la trasmissione di un segnale di *jamming*, appunto. Tale *setup* è stato modellato mediante strumenti ricavati dalla Teoria dei Giochi, in particolare come gioco a somma zero in cui la funzione di *payoff* è rappresentata dall'informazione mutua scambiata fra trasmettitore e ricevitore. In quseto modo sono state determinate le strategie di trasmissione ottime sia per il trasmettitore legittimo che per l'attaccante, ed è stato trovato il punto di equilibrio di Nash del gioco sia per sistemi OFDM di tipo *discrete multitone* (DMT) che *filtered multitone* (FMT).

Chapter 1

Introduction

OFDM systems offer a simple and efficient solution in coping with frequency selective channels. Information is carried over parallel orthogonal subchannels, that can be easily equalized in the frequency domain [1]. The multiplexing of various subchannels over the transmission medium is obtained through the fast Fourier transform (FFT) algorithm [2]. This fact allows the use of efficient implementation architectures based on FFT chips for both modulator and demodulator [3, 4].

Due to these advantageous features, OFDM has been included in the physical layer specifications of a large variety of wireless standards. From the well established and widespread WLAN transmissions of the family IEEE 802.11 [5], to the more recent WiMax [6] and LTE [7, 8] protocols. Also the present and future standards for digital video broadcasting, DVB-T [9] and DVB-T2 [10], rely on OFDM-based transmissions. Multicarrier transmissions have also been introduced into UWB communications, with the implementation of MB-OFDM systems [11]. In all these cases, OFDM transmissions have been chosen as they represent an elegant and efficient way to employ the available band with high spectral efficiency. In order to optimize the performance provided by those systems, the careful design of algorithms for time and frequency synchronization plays a central role, due to the sensitivity of OFDM modulation to synchronization impairments. In particular, in this thesis we will consider time synchronization methods that are robust to an increased spectral efficiency of the system. Moreover, we will analyze frequency offset estimation algorithms that take advantage of the augmented spectral diversity introduced in modern broadband wireless communications.

Traditionally, the main objective driving the analysis and the design of the physical layer

features of communication systems has been to guarantee reliability of data transmissions against different channel conditions and device impairments. Nevertheless, recent results from Information Theory have demonstrated that the intrinsic randomness inherent in wireless communication channels can be harnessed to enhance network security. In particular, the seminal works of Wyner [12] and Csiszár and Körner [13] have proved the possibility of hiding confidential messages from unauthorized eavesdroppers by leveraging the channel diversity between the legitimate receiver and the attacker, without using classic cryptographic schemes. Similarly, the works of Ahslwede and Csiszár [14] and Maurer [15] have shown that secret keys for use in classical cryptography can be distilled from common randomness transmitted over wireless channels. Besides, physical layer security issues have considerd not only the presence of passive eavesdroppers in the network, but also the problem of active jamming on the transmitted signals has been extensively studied [16–18]. Starting from these considerations, our analysis of multicarrier transmissions in wireless networks will focus also on the problem of providing secure communication by physical layer strategies that are specifically designed for the OFDM modulation, thus aiming to contribute to the bridging of the gap between information theoretic results and practical implementation of these paradigms.

In this chapter we will present the general scheme of an OFDM transmission system in the presence of either passive or active attackers that intend to overhear or disturb the communication. We will briefly describe the features of two common types of OFDM modulation, i.e., the DMT, implementing cyclic prefix (CP) or zero pad suffix (ZS) transmissions [19], and the FMT, both the critically sampled (CS) and non-critically sampled (NS) types [20]. We will also report the orthogonality conditions that must be satisfied in order to avoid destructive interference among subchannels and different OFDM symbols. Finally, we will show efficient implementation architectures for DMT and FMT systems and present a MIMO representation of the discrete-time equivalent of an OFDM system.

Throughout this thesis, vectors are indicated with lower-case boldface symbols, whereas upper-case boldface letters are used for matrices. The symbol * indicates the conjugate transpose of a matrix and † denotes its Moore-Penrose pseudo-inverse. $\boldsymbol{I}_n$ and $\mathbf{0}_{n\times m}$ are respectively the $n \times n$ identity matrix and an $n \times m$ matrix of zeros. For compactness, subscripts will be dropped whenever the matrix dimensions are clear from the context. The i-th eigenvalue of the square matrix $\boldsymbol{A}$ is indicated by $\lambda_i(\boldsymbol{A})$, whereas the i-th singular value of the matrix $\boldsymbol{A}$ is denoted by $\sigma_i(\boldsymbol{A})$. We use $\|\cdot\|^2$ to denote the squared Euclidean norm of a

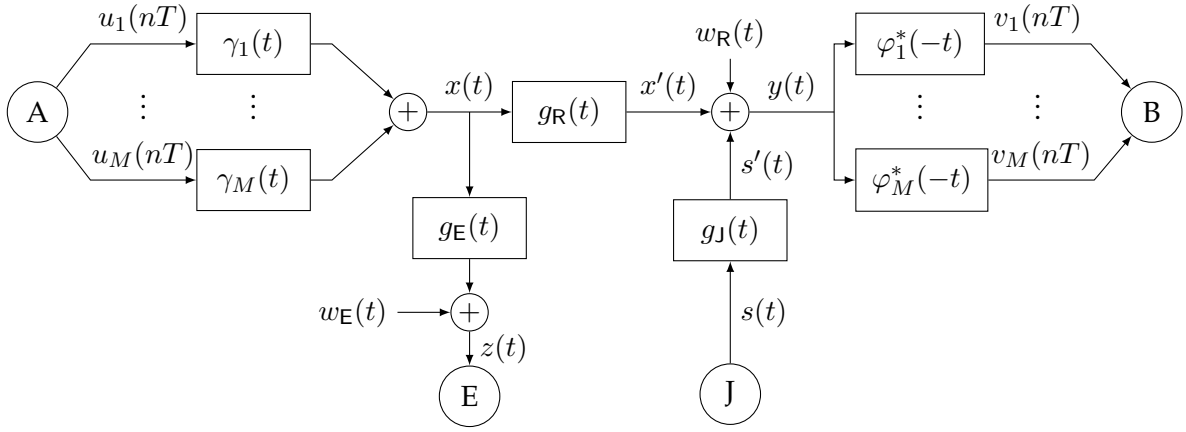

Figure 1.1. *Block diagram of the filter bank description of an OFDM system over dispersive channel in the presence of an either passive (eavesdropper) or active (jammer) attacker. The OFDM symbol duration is denoted by T.*

vector, i.e. $\|\boldsymbol{a}\|^2 = \sum_i |a_i|^2$; and $\|\cdot\|_{\mathsf{F}}^2$ to denote the squared Frobenius norm of a matrix, i.e. $\|\boldsymbol{A}\|_{\mathsf{F}}^2 = \sum_i \sum_\ell |a_{i\ell}|^2$. The trace of a matrix is denoted with $\mathrm{tr}(\cdot)$. The notation $\boldsymbol{A} \succeq \boldsymbol{B}$ means that the matrix $\boldsymbol{A} - \boldsymbol{B}$ is positive semidefinite. The symbols $\sqrt{\boldsymbol{A}} = \boldsymbol{A}^{1/2}$ denotes the positive semidefinite square root matrix of the (positive semidefinite) matrix $\boldsymbol{A}$. We indicate the positive part of a quantity x as $[x]^+ = \max\{x, 0\}$, the time reversal operation as $g_-(n) = g(-n)$, and the signal convolution between g and h as $g * h$. The symbol $\mathbb{U}_{(a,b)}(t)$ denotes the indicator function of the interval (a, b). We also use the notation $f(x) \asymp g(x)$ to indicate that $\lim_{x\to\infty} f(x)/g(x) = 1$. The expectation operator is denoted by $\mathbb{E}\{\cdot\}$ and use the symbol $\mathbb{I}(\cdot;\cdot)$ to denote the mutual information between two random variables. We indicate the entropy and differential entropy of a random quantity with $\mathbb{H}(\cdot)$ and $h(\cdot)$, respectively. If not specified otherwise, logarithms are in base 2.

1.1 OFDM as a filter bank

1.1.1 General scheme

A very general model for OFDM modulation is depicted in Figure 1.1 and consists of describing the baseband equivalent of both the transmitter and the receiver as filter banks. Each filter bank is made of M frequency-shifted versions of the same filter, $\gamma_i(t)$, $i = 1, \ldots, M$, for the transmitter and $\varphi_i(t)$, $i = 1, \ldots, M$, for the receiver, that are centered around the M subcarrier frequencies f_i, multiples of the subcarrier spacing F_{u} (usually

$f_i = m_i F_{\mathsf{u}}$, with $m_i = -M/2, \ldots, M/2-1$). Then, the baseband equivalent of the modulated signal can be written as

$$x(t) = \sum_{n=-\infty}^{\infty} \sum_{i=1}^{M} u_i(nT)\gamma_0(t-nT)e^{j2\pi m_i F_{\mathsf{u}}(t-nT)}, \tag{1.1}$$

in which n denotes the OFDM symbol index and T is its duration. The symbols $u_i(nT)$, $i = 1, \ldots, M$ loaded on the M subcarriers are usually called *frequency domain* symbols, whereas $x(t)$ comprises the corresponding *time domain* values of the signal.

The filter shapes $\gamma_0(t)$ and $\varphi_0(t)$ determine the different OFDM architectures. DMT systems employ filters with finite impulse response duration within the OFDM symbol period T. The inverse of the subcarrier spacing $T_{\mathsf{u}} = 1/F_{\mathsf{u}}$ is called *useful symbol duration*. T_{u} is a fraction of T and the value $T_{\mathsf{g}} = T - T_{\mathsf{u}}$ is denoted as the *guard interval* of the system. The ratio $\rho = T_{\mathsf{g}}/T_{\mathsf{u}}$ represents the redundancy introduced in the transmission in order to cope with dispersive channels. The DMT systems with CP use filters with impulse responses

$$\gamma_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(-T_{\mathsf{g}},T_{\mathsf{u}})}(t) \quad , \quad \varphi_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(0,T_{\mathsf{u}})}(t), \tag{1.2}$$

The corresponding frequency responses are

$$\Gamma_0(f) = (1+\rho)\sqrt{T_{\mathsf{u}}}\,\mathrm{sinc}(Tf)e^{-j\pi f(T_{\mathsf{u}}-T_{\mathsf{g}})} \quad , \quad \Phi_0(f) = \sqrt{T_{\mathsf{u}}}\,\mathrm{sinc}(T_{\mathsf{u}}f)e^{-j\pi f T_{\mathsf{u}}}. \tag{1.3}$$

The transmitter and receiver filters impulse responses for ZS are instead

$$\gamma_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(0,T_{\mathsf{u}})}(t) \quad , \quad \varphi_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(0,T)}(t), \tag{1.4}$$

and their Fourier transforms are given by

$$\Gamma_0(f) = \sqrt{T_{\mathsf{u}}}\,\mathrm{sinc}(T_{\mathsf{u}}f)e^{-j\pi f T_{\mathsf{u}}} \quad , \quad \Phi_0(f) = (1+\rho)\sqrt{T_{\mathsf{u}}}\,\mathrm{sinc}(Tf)e^{-j\pi f T}. \tag{1.5}$$

CP and ZS are very similar and provide very efficient and simple device implementation at the expense of signal power loss due to the asymmetry between the transmitter and receiver filter spaces. In particular, the ZS transmitter provides a modulated signal with smaller ripple in the useful band spectrum, but higher side lobes, compared to CP. Moreover, it is possible to obtain sharp notches in the ZS transmitted spectrum by switching off the corresponding subcarriers. On the other hand, the noise samples obtained after CP demodulation, in the frequency domain, are uncorrelated, since the receiver filter impulse response $\varphi_i(t)$ are orthogonal.

On the other hand, the FMT systems implement subchannels that are separated in frequency and have bandwidth equal to the subcarrier spacing. For this reason, such systems are easier to describe in the frequency domain. In particular, the subcarrier spacing for CS systems is equal to the inverse of the OFDM symbol period, $F_{\mathsf{u}} = 1/T$, and the frequency responses of the filters at the transmitter and the receiver have root raised-cosine shape, with roll-off factor ρ

$$\Gamma_0(f) = \Phi_0(f) = \sqrt{T(1+\rho)\mathrm{rcos}(\rho, T(1+\rho)f)}. \tag{1.6}$$

The NS solution, instead, adopts a subcarrier spacing larger than the OFDM symbol rate. Namely, $F_{\mathsf{u}} = (1+\rho)/T$, and $\rho \in \mathbb{Q}$ is chosen as a simple fraction (typically $\rho = 1/4$) in order to guarantee a simple numerical implementation. Then, the frequency responses of the filters have again root rasied-cosine shape with roll-off factor ρ

$$\Gamma_0(f) = \Phi_0(f) = \sqrt{T\mathrm{rcos}(\rho, Tf)}. \tag{1.7}$$

However, the clear separation in frequency among the different subchannels of FMT systems is paid with higher implementation complexity for transmitters and receivers, due to the need of specifically shaped filters. Moreover, CS provides the advantage of higher efficiency at the expense of the introduction of intersymbol interference. The parameters and filter expressions of the DMT and FMT systems described in this chapter are summarized in Table 1.1.

In our scenario, OFDM transmissions are performed in the presence of an attacker. We consider two types of attack: passive eavesdropping and active jamming. In the first case, the transmitted signal $x(t)$ is overheard by the eavesdropper after being distorted by the channel $g_{\mathsf{E}}(t)$. The objective of the attacker in this scenario is to disclose the content of the communication between the legitimate terminals and retrieve the values of the message symbols $u_i(nT)$ from observations of the signal $z(t)$. The aim of an active attack, instead, is to disrupt the communication between the transmitter and the legitimate receiver, in order to cause a *denial of service* event. Then, the attacker broadcasts a jamming signal $s(t)$ that, after being distorted by the channel $g_{\mathsf{J}}(t)$, interferes with the legitimate receiver input. We also note that, the eavesdropper and the jammer could be the same entity implementing both attack strategies.

Throughout this work, when it is not otherwise stated, we consider transmissions over slowly fading dispersive channels; that is, the impulse responses of the channels are assumed to be constant over the duration of a packet. We also denote with $w_{\mathsf{R}}(t), w_{\mathsf{E}}(t)$ the

Table 1.1. *Parameters and filters for the transmission of L OFDM symbols over common DMT and FMT systems. The notation $\mathbb{U}_{(a,b)}(t)$ represents the unit amplitude rectangular signal extending from a to b, while $\mathrm{rcos}(\rho, x)$ represents the raised cosine with roll-off ρ.*

system	efficiency	transmit and receive filters	bandwidth	pck duration
CP	$F_{\mathsf{u}}T = 1+\rho$	$\gamma_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(-T_{\mathsf{g}},T_{\mathsf{u}})}(t)$, $\varphi_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(0,T_{\mathsf{u}})}(t)$	$B_x > MF_{\mathsf{u}}$	$T_{\mathsf{p}} = LT$
ZS	$F_{\mathsf{u}}T = 1+\rho$	$\gamma_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(0,T_{\mathsf{u}})}(t)$, $\varphi_0(t) = \sqrt{F_{\mathsf{u}}}\,\mathbb{U}_{(0,T)}(t)$	$B_x > MF_{\mathsf{u}}$	$T_{\mathsf{p}} = LT$
CS	$F_{\mathsf{u}}T = 1$	$\Gamma_0(f) = \sqrt{\frac{T}{1+\rho}\,\mathrm{rcos}\left(\rho, \frac{T}{1+\rho}f\right)}$, $\Phi_0(f) = \Gamma_0(f)$	$B_x = MF_{\mathsf{u}}$	$T_{\mathsf{p}} > LT$
NS	$F_{\mathsf{u}}T = 1+\rho$	$\Gamma_0(f) = \sqrt{T\,\mathrm{rcos}(\rho, Tf)}$, $\Phi_0(f) = \Gamma_0(f)$	$B_x = MF_{\mathsf{u}}$	$T_{\mathsf{p}} > LT$

zero mean, additive white Gaussian noise (AWGN) processes originated by thermal noise in the devices at the legitimate receiver and the eavesdropper, respectively.

1.1.2 Orthogonality conditions

We focus now on the features of multicarrier transmissions over frequency selective channels, and the conditions that must be satisfied by the dispersive channels in order to preserve orthogonality among the M subcarriers. For the sake of compactness we drop the explicit expression of the OFDM symbol period T. Then, if we gather the M symbols transmitted within the n-th OFDM symbol into the column vector $\boldsymbol{u}(n) = [u_1(n), \ldots, u_M(n)]^T$, and the corresponding received ones in the vector $\boldsymbol{v}(n) = [v_1(n), \ldots, v_M(n)]^T$, the input/output relationship for the whole OFDM system is given by the $M \times M$ matrix filter relation

$$\boldsymbol{v}(n) = \sum_{k=-\infty}^{+\infty} \boldsymbol{H}(n-k)\boldsymbol{u}(k) + \bar{\boldsymbol{w}}(n), \tag{1.8}$$

in which the components of the frequency domain noise vector $\bar{\boldsymbol{w}}(n)$ are given by the projection of the AWGN $w_{\mathsf{R}}(t)$ onto the receiver signal space, that is

$$\bar{w}_i(n) = \int_{-\infty}^{+\infty} w_{\mathsf{R}}(t)\varphi_i^*(t-nT)dt. \tag{1.9}$$

The general term in the matrix $\boldsymbol{H}$ is the sampled version (with sampling period T) of the convolution between the ℓ-th transmit filter, the main channel and the i-th receive filter

$$H_{i\ell}(n) = \varphi_{i-}^{*} * g_{\mathsf{R}} * \gamma_{\ell}(nT). \tag{1.10}$$

According to the i-th row of the matrices $\boldsymbol{H}(n)$, the demodulated symbol on the i-th subcarrier may therefore be affected by amplitude and phase distortion, by ICI due to the loss of orthogonality between subcarriers, as well as by ISI from other OFDM symbols.

If we decompose the filter into the components that give the useful part, the ICI, and the ISI, as follows

$$\boldsymbol{H}_{\mathsf{u}} = \operatorname{diag}\left(H_{11}(0), \ldots, H_{MM}(0)\right) \tag{1.11a}$$

$$\boldsymbol{H}_{\mathsf{ICI}} = \boldsymbol{H}(0) - \boldsymbol{H}_{\mathsf{u}} \tag{1.11b}$$

$$\boldsymbol{H}_{\mathsf{ISI}}(n) = \begin{cases} \boldsymbol{0} & , \ n = 0 \\ \boldsymbol{H}(n) & , \ n \neq 0 \end{cases} \tag{1.11c}$$

then the output vector $\boldsymbol{v}(n)$ can be decomposed into

$$\boldsymbol{v}(n) = \boldsymbol{v}_{\mathsf{u}}(n) + \boldsymbol{v}_{\mathsf{ICI}}(n) + \boldsymbol{v}_{\mathsf{ISI}}(n) + \bar{\boldsymbol{w}}(n) \tag{1.12}$$

where

$$\boldsymbol{v}_{\mathsf{u}}(n) = \boldsymbol{H}_{\mathsf{u}}\boldsymbol{u}(n) \tag{1.13a}$$

$$\boldsymbol{v}_{\mathsf{ICI}}(n) = \boldsymbol{H}_{\mathsf{ICI}}\boldsymbol{u}(n) \tag{1.13b}$$

$$\boldsymbol{v}_{\mathsf{ISI}}(n) = \sum_{k=-\infty}^{+\infty} \boldsymbol{H}_{\mathsf{ISI}}(n-k)\boldsymbol{u}(k) \tag{1.13c}$$

Then, based on (1.10) and the filter expressions for the various systems, we can identify the conditions the transmission channel must satisfy in order to avoid ISI and ICI.

We start considering first the DMT systems. In this case, it is straightforward to show that, if the channel delay spread is shorter then the guard interval T_{g}, then the transmission is free from ISI and ICI. In fact, we can notice immediately that, given the above constraint on the channel delay spread, the cascade of transmit filter, channel and receive filter impulse response $\varphi_{i-}^{*} * g_{\mathsf{R}} * \gamma_{\ell}(t)$ has a support contained in the time interval $(-T, T)$, hence, interference from other OFDM symbols is avoided. In order to show that also ICI is reduced to zero once the channel impulse response has support contained in the interval $[0, T_{\mathsf{g}})$, we

explicitly compute the values of the channel matrix $\boldsymbol{H}(0)$,

$$H_{i\ell}(0) = \int_{-\infty}^{+\infty} \gamma_\ell(u) g_{\mathsf{R}}(t-u) \varphi_i^*(t) du\, dt \tag{1.14}$$

$$= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \gamma_0(u) g_{\mathsf{R}}(t-u) \varphi_0(t) e^{j2\pi(f_\ell u - f_i t)} du\, dt. \tag{1.15}$$

On considering the two different DMT architectures separately, for the CP case it holds

$$H_{i\ell}(0) = F_{\mathsf{u}} \int_0^{T_{\mathsf{u}}} \int_{-T_{\mathsf{g}}}^{T_{\mathsf{u}}} g_{\mathsf{R}}(t-u) e^{j2\pi(f_\ell u - f_i t)} du\, dt \tag{1.16}$$

$$= F_{\mathsf{u}} \int_0^{T_{\mathsf{u}}} e^{-j2\pi f_i t} \int_{-T_{\mathsf{g}}}^{T_{\mathsf{u}}} g_{\mathsf{R}}(t-u) e^{j2\pi f_\ell u} du\, dt. \tag{1.17}$$

Then, since the support of $g_{\mathsf{R}}(t-u)$ is contained in the interval $(t-T_{\mathsf{g}}, t)$, the second integral can be expressed as a function of the channel frequency response

$$\int_{-T_{\mathsf{g}}}^{T_{\mathsf{u}}} g_{\mathsf{R}}(t-u) e^{j2\pi f_\ell u} du = G_{\mathsf{R}}(f_\ell) e^{j2\pi f_\ell t}. \tag{1.18}$$

Hence, we can write

$$H_{i\ell}(0) = G_{\mathsf{R}}(f_\ell) F_{\mathsf{u}} \int_0^{T_{\mathsf{u}}} e^{j2\pi(f_\ell - f_i)t} dt \tag{1.19}$$

$$= G_{\mathsf{R}}(f_\ell) F_{\mathsf{u}} \int_0^{T_{\mathsf{u}}} e^{j2\pi(m_\ell - m_i)F_{\mathsf{u}} t} dt \tag{1.20}$$

$$= \begin{cases} G_{\mathsf{R}}(f_i) & , \ i = \ell \\ 0 & , \ i \neq \ell \end{cases} \tag{1.21}$$

from which we observe that the M subchannels are not interfering among each others and the useful coefficients are given by the channel frequency response at the subcarrier frequency.

Similarly, for the ZS case it holds

$$H_{i\ell}(0) = F_{\mathsf{u}} \int_0^{T} \int_0^{T_{\mathsf{u}}} g_{\mathsf{R}}(t-u) e^{j2\pi(f_\ell u - f_i t)} du\, dt \tag{1.22}$$

$$= F_{\mathsf{u}} \int_0^{T_{\mathsf{u}}} e^{j2\pi f_\ell u} \int_0^{T} g_{\mathsf{R}}(t-u) e^{j2\pi f_i t} dt\, ut. \tag{1.23}$$

Here, the support of $g_{\mathsf{R}}(t-u)$ is contained in the interval $(u, u+T_{\mathsf{g}})$, hence, the internal integral can be computed again in terms of the Fourier transform of $g_{\mathsf{R}}(t)$, and we obtain

$$\int_0^{T} g_{\mathsf{R}}(t-u) e^{j2\pi f_i t} dt = G_{\mathsf{R}}(f_i) e^{-j2\pi f_i u}, \tag{1.24}$$

from which we have the same result that holds when the system adopts cyclic prefix transmission

$$H_{i\ell}(0) = G_{\mathsf{R}}(f_i)F_{\mathsf{u}} \int_0^{T_{\mathsf{u}}} e^{j2\pi(m_\ell - m_i)F_{\mathsf{u}}t}dt \tag{1.25}$$

$$= \begin{cases} G_{\mathsf{R}}(f_i) & , \ i = \ell \\ 0 & , \ i \neq \ell \end{cases} . \tag{1.26}$$

On the other hand, ICI does not affect FMT transmissions, regardless to the channel impulse response duration, as different subchannels occupy disjoint bands. Moreover, if the channel frequency response is constant over each subchannel, that is

$$G_{\mathsf{R}}(f) = G_{\mathsf{R}}(f_i) \quad , \quad f \in [f_i - F_{\mathsf{u}}/2, f_i + F_{\mathsf{u}}/2], \tag{1.27}$$

the cascade of the transmit filter, channel and receive filter for NS systems is shown to verify the Nyquist criterion [21], hence, ISI does not arise.

On the contrary, CS suffers from ISI even when transmission takes palce over AWGN channels, as its filters do not comply with the Nyquist criterion . Nevertheless, in this case ISI is due to only symbols transmitted on the same subcarrier, hence it can be removed using equalization methods that operate separately on each single subchannel. Moreover, if (1.27) is satisfied, ISI can be arbitrarily reduced by decreasing the filters roll-off factor ρ (a typical value in practical implementations is $\rho = 1/20$ [22]).

1.1.3 Efficient implementation

The actual implementation of OFDM in modern communication systems has become a reality thanks to the possibility of performing the multiplexing of the M parallel subchannels with methods based on the FFT algorithm [2–4]. We consider DMT systems first, since they can guarantee very simple implementations for modulator and demodulator, without requiring a polyphase filter network. The description of the efficient implementation architectures is based on the discrete-time equivalent system, sampled at frequency $F_0 = MF_{\mathsf{u}}$, in order to verify the hypothesis of the sampling theorem. Then, on denoting with $T_0 = 1/F_0$ the sampling period, the useful symbol period is given by M samples, that is $T_{\mathsf{u}} = MT_0$, and, without loss of generality, we assume the guard interval is chosen as a multiple of T_0, say $T_{\mathsf{g}} = \mu T_0$. Then, an OFDM symbol of duration T consists of $N = M + \mu$ samples that are obtained from the frequency domain symbols in $\boldsymbol{u}(n)$ according to the scheme depicted in Figures **??** and 1.3. The CP transmitter computes the inverse fast Fourier transform (IFFT)

of the vector $\boldsymbol{u}(n)$ and then appends the last μ samples of the IFFT output at the beginning of the OFDM symbol. For this reason, this technique is called cyclic prefix transmission. On the other hand, the ZS architecture is equivalent to computing the IFFT of the input $\boldsymbol{u}(n)$ and padding it with a suffix of μ zeros. Then, the so obtained N samples pass through a parallel-to-serial converter and are fed to the digital-to-analog converter (DAC). The resulting signal is upconverted to the transmission carrier frequency and transmitted over the dispersive channel.

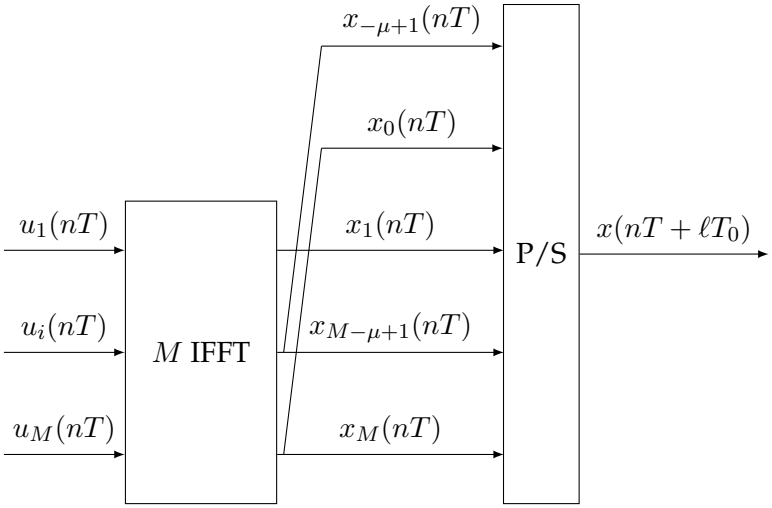

Figure 1.2. *Efficient implementation of the DMT modulator for cyclic prefix transmissions.*

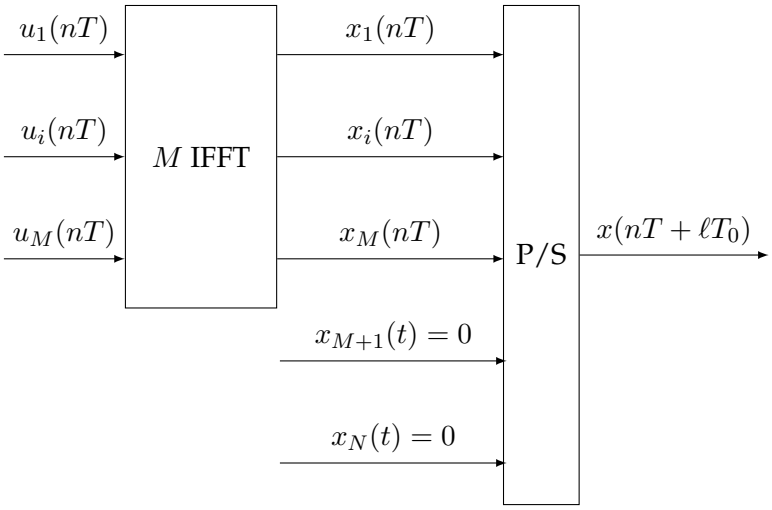

Figure 1.3. *Efficient implementation of the DMT modulator for zero-padding suffix transmissions.*

At the receiver side, after downconversion and the analog-to-digital converter (ADC),

the CP receiver discards the first μ received samples of each OFDM symbol and computes the FFT of the remaining M values. Conversely, in the ZS receiver, the last μ samples of the received symbol are added to the first μ before computing the M-size FFT of the results. This last architecture is called *overlap-and-add* receiver.

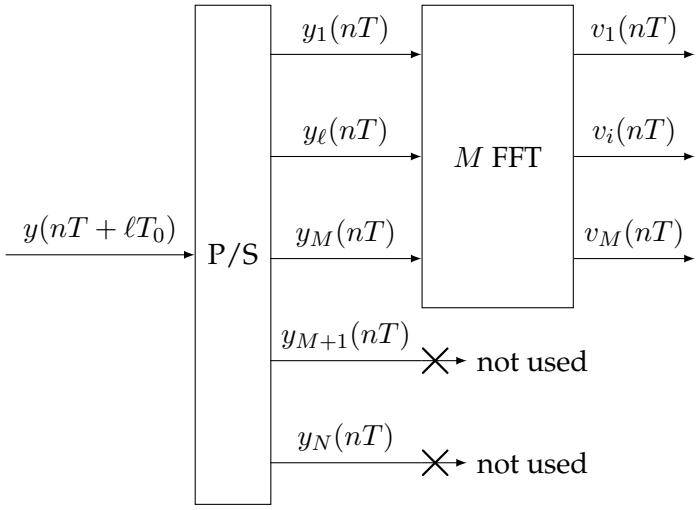

Figure 1.4. *Efficient implementation of the CP demodulator. The last fraction of each received symbol is discarded.*

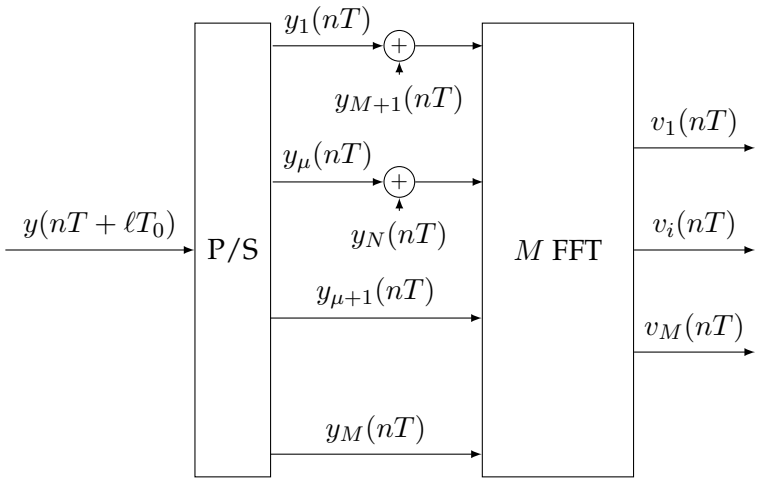

Figure 1.5. *Efficient implementation of the ZS demodulator. The* overlap-and-add *operation is performed before computing the FFT of the received symbol.*

Similarly to what happens for DMT systems, also FMT transmissions can be implemented with efficient schemes based on the FFT computation. Nevertheless, both transmit-

ters and receivers need the realization of a polyphase filter network operating at the OFDM symbol frequency $1/T$, hence, they are less common in applications than DMT transceivers.

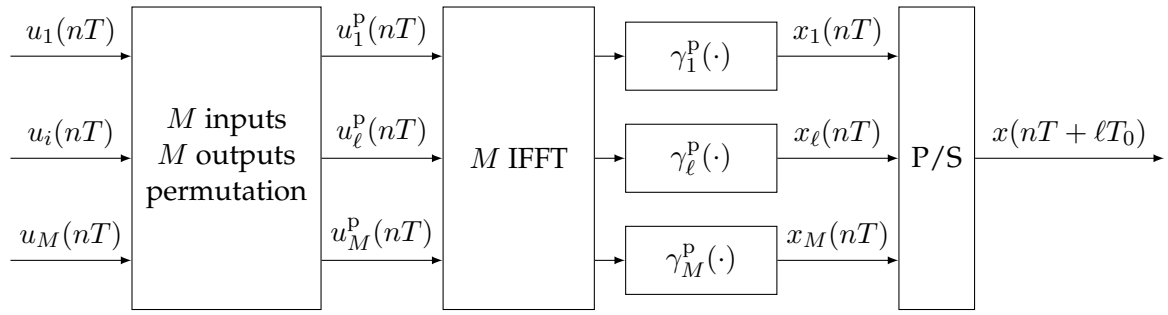

Figure 1.6. *Efficient implementation of the FMT modulator. The filters $\gamma_i^{\mathrm{p}}(t)$ are the polyphase components of $\gamma_0(t)$.*

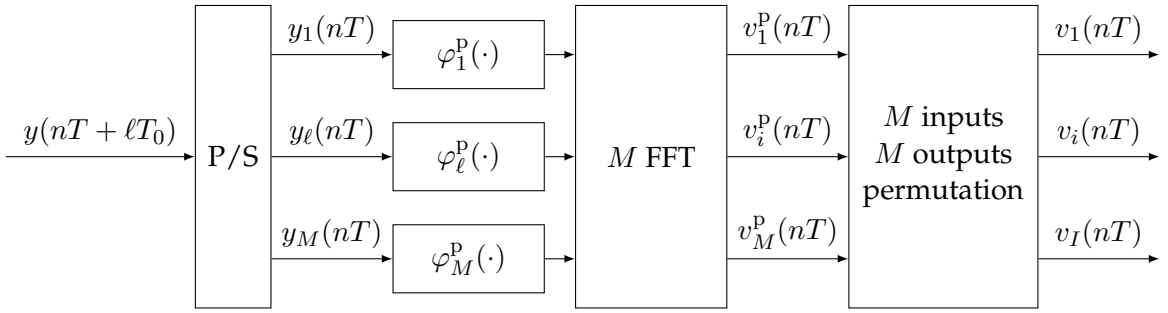

Figure 1.7. *Efficient implementation of the FMT demodulator. The filters $\varphi i^{\mathrm{p}}(t)$ are the polyphase components of $\varphi_0(t)$.*

1.2 OFDM as a MIMO Gaussian channel

The efficient implementation of OFDM suggests an equivalent matrix representation of the system, that turns out to be useful in assessing its performance as a particular instance of a MIMO Gaussian channel. In particular, we focus on the description of DMT systems, for which it is advantageous to perform the analysis in the time domain. We gather the samples (with sampling period $T_0 = 1/F_0$) of the main channel impulse response in the vector $\boldsymbol{g}_{\mathsf{R}} = [g_{\mathsf{R}}(0), g_{\mathsf{R}}(1), \ldots, g_{\mathsf{R}}(L_{\mathsf{R}}-1)]$. Then, on collecting all the NL samples corresponding to the transmission of L OFDM symbols over the dispersive channel in the vector $\boldsymbol{x} \in \mathbb{C}^{NL}$, and denoting with $\boldsymbol{y} \in \mathbb{C}^{NL+L_{\mathsf{R}}-1}$ the corresponding signal at the receiver input (obtained as the

discrete convolution between $\boldsymbol{x}$ and $\boldsymbol{g}_{\mathsf{R}}$), the following relation holds,

$$\boldsymbol{y} = \boldsymbol{G}_{\mathsf{R}}\boldsymbol{x} + \boldsymbol{w}_{\mathsf{R}}, \tag{1.28}$$

in which the noise vector $\boldsymbol{w}_{\mathsf{R}} \sim \mathcal{CN}(0, \boldsymbol{I}_{NL+L_{\mathsf{R}}-1})$ comprises independent, zero-mean, unit-variance, circularly symmetric complex Gaussian variables and the multiplication of $\boldsymbol{x}$ by the channel matrix $\boldsymbol{G}_{\mathsf{R}}$ represents the convolution with $\boldsymbol{g}_{\mathsf{R}}$. Namely, $\boldsymbol{G}_{\mathsf{R}} \in \mathbb{C}^{(NL+L_{\mathsf{R}}-1)\times NL}$ is the lower-triangular, Toeplitz matrix

$$\boldsymbol{G}_{\mathsf{R}} = \begin{bmatrix} g_{\mathsf{R}}(0) & 0 & \cdots & 0 \\ g_{\mathsf{R}}(1) & g_{\mathsf{R}}(0) & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ g_{\mathsf{R}}(L_{\mathsf{R}}-1) & \ddots & \ddots & g_{\mathsf{R}}(0) \\ 0 & g_{\mathsf{R}}(L_{\mathsf{R}}-1) & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{\mathsf{R}}(L_{\mathsf{R}}-1) \end{bmatrix}. \tag{1.29}$$

The same model can be used to describe the eavesdropper channel, and, on denoting with $\boldsymbol{G}_{\mathsf{E}} \in \mathbb{C}^{NL+L_{\mathsf{E}}-1\times NL}, \boldsymbol{w}_{\mathsf{E}} \in \mathbb{C}^{NL+L_{\mathsf{E}}-1}$ the eavesdropper channel matrix and noise vector, respectively, we can write

$$\boldsymbol{z} = \boldsymbol{G}_{\mathsf{E}}\boldsymbol{x} + \boldsymbol{w}_{\mathsf{E}}. \tag{1.30}$$

The same matrix representation of convolution is also used to described the dispersion induced by the frequency selective channel onto the jamming signal $\boldsymbol{s}' = \boldsymbol{G}_{\mathsf{J}}\boldsymbol{s}$.

In order to impose the OFDM structure on the legitimate transmitter signal, we write

$$\boldsymbol{x} = \boldsymbol{T}\boldsymbol{u}, \tag{1.31}$$

with the vector $\boldsymbol{u} \in \mathbb{C}^{ML}$ containing the frequency domain symbols loaded on the M subcarriers of the L symbols. The OFDM modulation matrix $\boldsymbol{T}$ is an $NL \times ML$ matrix that can be described in terms of the Kronecker product as

$$\boldsymbol{T} = \boldsymbol{I}_L \otimes \boldsymbol{T}_M \tag{1.32}$$

where $\boldsymbol{I}_L$ represents the $L \times L$ identity matrix and $\boldsymbol{T}_M = \boldsymbol{A}\boldsymbol{F}_M^*$ is the $N \times M$ matrix obtained by the product of the cyclic prefix (zero-padding suffix) matrix $\boldsymbol{A}$ responsible for inserting the redundancy that is needed to overcome the delay spread of the dispersive channel, and

the $M \times M$ IFFT matrix $\boldsymbol{F}_M^*$. Namely, for a CP system

$$\boldsymbol{A} = \left[\begin{array}{c} \mathbf{0} \quad \boldsymbol{I}_\mu \\ \hline \boldsymbol{I}_M \end{array} \right], \tag{1.33}$$

where we recall $\mu = N - M$ is the length of the CP, whereas for the ZS system with a suffix of length μ, we have

$$\boldsymbol{A} = \left[\begin{array}{c} \boldsymbol{I}_M \\ \\ \mathbf{0}_{\mu \times M} \end{array} \right]. \tag{1.34}$$

Similarly, demodulation at the OFDM receiver can be represented by the multiplication

$$\boldsymbol{v} = \boldsymbol{R}\boldsymbol{y}, \tag{1.35}$$

in which the channel output is multiplied by the $ML \times (NL + L_{\mathsf{R}} - 1)$ matrix

$$\boldsymbol{R} = \boldsymbol{I}_L \otimes \boldsymbol{R}_M. \tag{1.36}$$

Here, $\boldsymbol{R}_M \in \mathbb{C}^{M \times N}$ is defined as the product $\boldsymbol{R_M} = \boldsymbol{F}_M \boldsymbol{B}$, with $\boldsymbol{F}_M$ the $M \times M$ FFT matrix and $\boldsymbol{B}$ is such that, for either system, owing to the orthogonality condition $L_{\mathsf{R}} \leq \mu$,

$$\boldsymbol{R}\boldsymbol{G}_{\mathsf{R}}\boldsymbol{T} = \boldsymbol{I}_L \otimes \mathrm{diag}(G_{\mathsf{R}}(f_i)), \tag{1.37}$$

in which $G_{\mathsf{R}}(f_i)$, $i = 1, \ldots, M$ is the length M FFT of the legitimate channel impulse response. So for the CP system we have

$$\boldsymbol{B} = \left[\begin{array}{ccc} \mathbf{0}_{M \times \mu} & \boldsymbol{I}_M & \mathbf{0}_{M \times (L_{\mathsf{R}}-1)} \end{array} \right], \tag{1.38}$$

whereas for the ZS system we have

$$\boldsymbol{B} = \left[\begin{array}{c|c|c} \boldsymbol{I}_M & \begin{array}{c} \boldsymbol{I}_\mu \\ \mathbf{0} \end{array} & \mathbf{0}_{M \times (L_{\mathsf{R}}-1)} \end{array} \right]. \tag{1.39}$$

In Figure 1.8 we report the matrix representation of the general OFDM system with passive or active attacker.

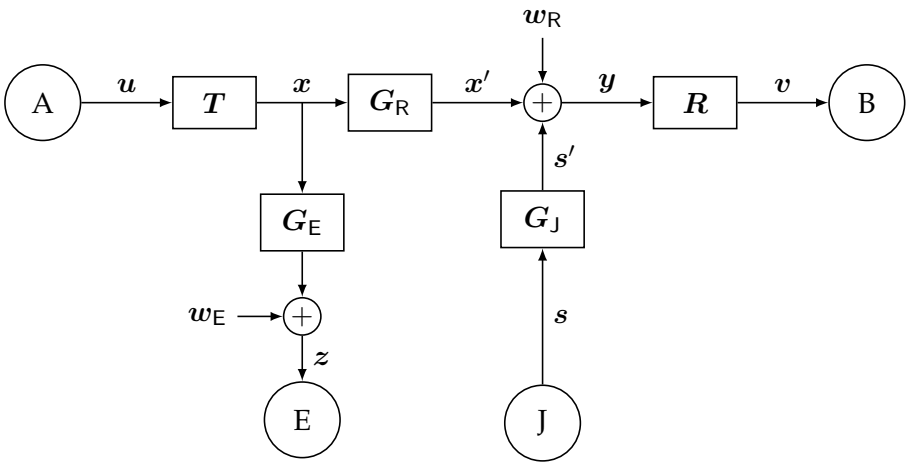

Figure 1.8. *Block diagram of the discrete-time vector/matrix equivalent of the OFDM system with passive and active attacker in Figure 1.1.*

Part I

Synchronization algorthms

Chapter 2

Time synchronization for very dispersive channels

The problem of symbol(or frame) synchronization for OFDM systems has been widely explored. From the initial works [23–25] to more recent developments and applications to specific systems and standards [26, 27] many techniques have been devised to estimate the symbol timing and their performance has been evaluated either via the estimator mean squared error (MSE) with respect to the correct timing, or via the resulting uncoded bit error rate (BER) of the system.

By far, the most common case for OFDM systems with CP (and analogously for those with ZS and overlap-and-add demodulation) is when the channel is dispersive but its delay spread is limited by the duration of the cyclic prefix (or the zero-padded suffix). In this case, since one-tap per subchannel equalization is needed anyway, the purpose of symbol synchronization is that of positioning the receiver reference instant so that the channel impulse response lies within the cyclic prefix and hence no ISI and no ICI arise, as it was shown in Section 1.1.2. Therefore there is no single correct timing point, but rather an interval of correct instants, corresponding to the difference between the length of the cyclic prefix and that of the channel. The performance of a synchronizer in this case could be evaluated by the lock-on probability, that is the probability of not having ISI and ICI, or by the statistical powers of the two interferences.

In the literature, the cyclic prefix is often assumed to be chosen *a priori* longer than the channel [28], since otherwise ICI and ISI would severely limit the system performance. The opposite scenario has therefore seldom been addressed. However, a system designed for

a shorter channel may occasionally operate on a longer one, or the cyclic prefix could be designed on purpose to be shorter than the channel either in order to reduce its redundancy, and so enhance the spectral efficiency, or to increase robustness with respect to time-varying channels [29]. Such a case happens also in the ECMA-368 Multiband OFDM standard [11] where the zero-padded suffix is about 70 ns long, whereas many of the channels on which it is intended to operate, such as those described in [30], are longer than 100 ns. It is also expected to happen in fourth generation cellular systems where cyclic prefixes of 4-5 μs must cope with channels that are twice as long [31]. For longer channels, as ICI and ISI are unavoidable, the aim of timing synchronization should be to minimize the impact of ISI and ICI on the system performance [29, 32, 33].

Then, we consider the less common scenario of very dispersive channels for both CP and ZS systems. We seek to accurately determine a target performance for synchronization systems, to evaluate the results of applying existing techniques to the longer channel case, and to propose an original technique that is best suited for such cases.

In this chapter and Chapter 3, we will denote the channel from the transmitter towards the legitimate receiver simply with $g(t)$, as the synchronization algorithms under analysis are designed ignoring the presence of an attacker.

2.1 OFDM over very dispersive channels

The frame synchronization phase at the OFDM receiver is performed after downconversion and sampling of the received signal. Hence, we detail in this section the discrete-time equivalent of the baseband OFDM model described in Section 1.1, in which we explicitly show the dependence from the receiver reference instant. The channel and filters are represented by their sampled versions with $T_0 = 1/(MF_{\mathsf{u}})$ the sampling period and for the sake of a compact notation we write in this chapter $g(t)$ for the value of g at time tT_0, $t \in \mathbb{Z}$. Moreover we let $W_M = e^{j2\pi/M}$.

As regards the input symbols we assume that $u_i(n)$ are uncorrelated with zero-mean and power $\mathbb{E}\left\{|u_i(n)|^2\right\} = P_i$[1].

When considering the discrete-time equivalent system, the general term in the matrix $\boldsymbol{H}$

[1] In a realistic scenario, a few subcarriers are commonly turned off (which is equivalent to setting $P_i = 0$) while others may use different powers, for the purpose of spectral shaping of the continuous-time transmitted signal.

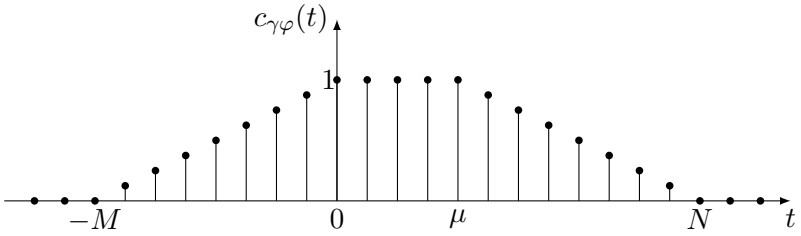

Figure 2.1. *Plot of the cross-correlation $c_{\gamma\varphi}(t)$ for both the CP and ZS systems.*

in (1.10) specifies as the N times decimated version of the discrete convolution between the ℓ-th transmit filter, the channel and the i-th receive filter

$$H_{i\ell}(n) = \varphi_{i-}^{*} * g * \gamma_{\ell}\,(nN) \tag{2.1a}$$

$$= W_M^{m(nN+t_0)} \sum_t T_0\,\varphi_0(t - t_0 - nN) \sum_u T_0\,g(t-u)\gamma_0(u) W_M^{\ell u - it} \tag{2.1b}$$

where t_0 is the starting instant of the demodulation FFT window. As it has been recalled in Section 1.1.2, if the channel impulse response lies within the interval $[0, \mu]$, the useful coefficients are given by the M-size discrete Fourier transform (DFT) of the channel impulse response

$$H_{ii}(0) = \sum_{t=0}^{\mu} T_0\,g(t) W_M^{-it} = T_0\,\mathrm{DFT}_M\,[g(t)|i] \tag{2.2}$$

whereas the interference components vanish, i.e. $\boldsymbol{H}_{\mathsf{ICI}} = \mathbf{0}$ and $\boldsymbol{H}_{\mathsf{ISI}}(n) = \mathbf{0}\ ,\ \forall\, n$, so that the system is free of both ISI and ICI.

On the contrary, we devote our attention to the case when the delay spread of the channel impulse response $g(t)$ exceeds the length μ of the cyclic prefix (or the zero-padding guard interval) between OFDM symbols. Thus, both ISI and ICI components do arise, while the useful coefficients are given by

$$H_{ii}(0) = \sum_{t=-\infty}^{+\infty} T_0\,g(t) c_{\gamma\varphi}(t - t_0) W_M^{-i(t-t_0)} \tag{2.3}$$

where $c_{\gamma\varphi}(t) = \sum_u T_0\,\varphi_0(u+t)\gamma_0(u)$, derived in [29] for the CP system, also holds for the ZS one and has the trapezoidal form plotted in Figure 2.1.

2.2 Ideal symbol synchronization

2.2.1 Problem statement

In the case in exam, the ideal timing should choose for any given realization the starting instant for the FFT demodulation window with the aim to maximize the signal to interfer-

ence plus noise ratio (SINR) on each subcarrier $i = 1, \ldots, M$

$$\Lambda_i = \frac{\mathbb{E}\left\{|v_{\mathrm{u},i}(n)|^2\right\}}{\mathbb{E}\left\{|v_{\mathrm{ICI},i}(n)|^2\right\} + \mathbb{E}\left\{|v_{\mathrm{ISI},i}(n)|^2\right\} + \mathbb{E}\left\{|\bar{w}_i(n)|^2\right\}} \tag{2.4}$$

where the expectations are only taken with respect to the symbol and noise distributions, given the channel realization and the FFT timing. However, for a given channel impulse response, the maximum of (2.4) is attained at different starting instants for different subcarriers. This problem is overcome in [29] by replacing the statistical powers in (2.4) with their average over the statistical description of a random channel assumed to be wide sense stationary with uncorrelated scattering (WSSUS), and by seeking the timing instant that maximizes the ratio between average powers. In this work we aim at maximizing for any given realization the *global SINR* over all subchannels

$$\Lambda = \frac{\mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{u}}(n)\|^2\right\}}{\mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{ICI}}(n)\|^2\right\} + \mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{ISI}}(n)\|^2\right\} + \mathbb{E}\left\{\|\bar{\boldsymbol{w}}(n)\|^2\right\}} \,. \tag{2.5}$$

With effective channel coding, data on corrupted subchannels are corrected based on the data demodulated from stronger ones. Hence, maximizing (2.5) yields minimization of the coded BER, as shown in Figure 2.2. This approach is better suited for time-invariant or slow fading channels, where we can fit the synchronization to the actual realization. On the other hand the method in [29] is better suited to fast fading channels where the channel can span different realizations within a single packet and coding is used across symbols. In [32] the minimization of the global interference power is sought, but the useful and interference components are incorrectly defined based on the expression in (2.2) rather than the correct one in (2.3).

2.2.2 Ideal synchronization in the full band system

In this section, for the sake of a compact formulation for the maximization of (2.5) over t_0, we will make use of a simplified and more tractable version of the OFDM system in which all the M subcarriers are loaded with the same power

$$P_i = P_u \quad , \quad i = 1, \ldots, M \,. \tag{2.6}$$

We call such a system "*full band* OFDM" and observe that, despite its ingenuousness, it represents a good approximation of actual OFDM systems, even those with spectrum shaping, where power is reduced or turned off in a few outer subcarriers.[2]

[2]On the other hand, the approximation would be rather loose if *power loading* were used with widely varying powers across different subcarriers.

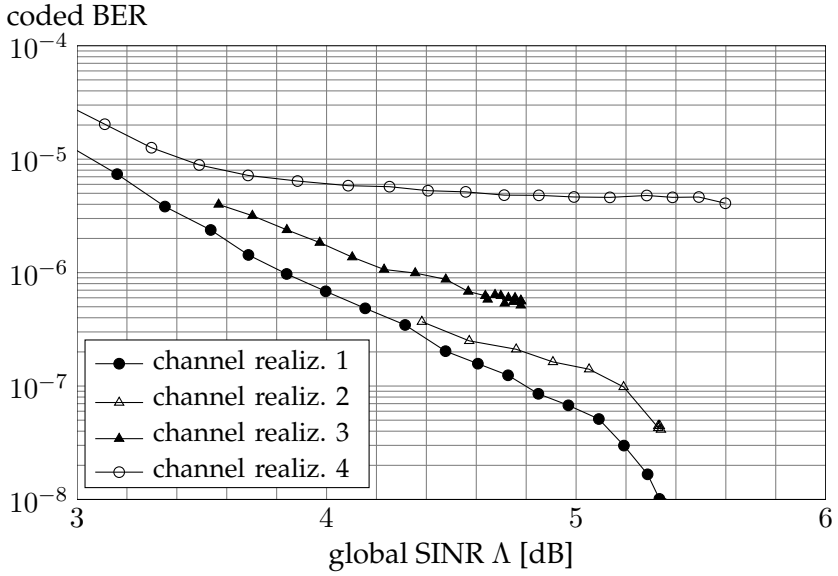

Figure 2.2. *Coded BER versus global SINR for some realizations of the UWB residential non line of sight (NLOS) channel model [30], with different symbol timing instants. Simulations use parameters for ECMA-368 [11] at the* $160\,Mb/s$ *transmission rate, with a rate* $1/2$ *convolutional code and QPSK modulation. Each line corresponds to a different realization of the channel, each data point to a different position of the starting instant for the FFT demodulation window.*

In the full band system, the output components satisfy

$$\mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{u}}(n)\|^2\right\} = P_u\|\boldsymbol{H}_{\mathsf{u}}\|_{\mathsf{F}}^2 \tag{2.7a}$$

$$\mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{ICI}}(n)\|^2\right\} = P_u\|\boldsymbol{H}_{\mathsf{ICI}}\|_{\mathsf{F}}^2 \tag{2.7b}$$

$$\mathbb{E}\left\{\|\boldsymbol{u}_{\mathsf{ISI}}(n)\|^2\right\} = P_u\sum_k \|\boldsymbol{H}_{\mathsf{ISI}}(k)\|_{\mathsf{F}}^2 \tag{2.7c}$$

and we can use the following result.

Theorem 1. *Let the matrices* $\boldsymbol{H}(n)$, $n \in \mathbb{Z}$ *depend on the timing epoch* t_0 *as described in (2.1b). The sum*

$$\sum_{n=-\infty}^{+\infty} \|\boldsymbol{H}(n)\|_{\mathsf{F}}^2 = \sum_{n=-\infty}^{+\infty}\sum_{i=1}^{M}\sum_{\ell=1}^{M} |H_{i\ell}(n)|^2 \tag{2.8}$$

is independent of t_0.

Proof. The proof is based on the fact that $\boldsymbol{H}(n)$ is the 2-dimensional DFT of $\varphi_0(t - t_0 - nN)g(t-u)\gamma_0(u)$ and by Parseval theorem, its Frobenius norm coincides with the energy of that function. By summing over all n we eliminate the dependance on t_0. □

We can thus state that, in the full band system, the sum of the three terms (2.7a)-(2.7c) depends on the channel impulse response $g(t)$ but is independent of the timing epoch t_0.

Hence, in order to maximize the ratio (2.5), it is sufficient to maximize the power of the useful component (2.7a) in the numerator, as the interference powers in the denominator are minimized accordingly.

A result analogous to Theorem 1 was proved in [29] for the expectation $\mathbb{E}\left\{\sum_{n,\ell}|H_{i\ell}(n)|^2\right\}$ over the distribution of a WSSUS random channel, leading to a maximization of the average SINR for each subcarrier i. Here we prove that when considering the aggregated powers over all subcarriers, it holds for *every realization* of any time-invariant channel. Even in [32], where aggregated powers and time-invariant channels are considered, this result is not stated, thus leading the author to only seek the minimization of the interference power.

It is also possible to express the maximization of (2.7a) in the time domain, thanks to the following result.

Theorem 2. *In the full band system, the total power of the useful components is given by*

$$\mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{u}}(n)\|^2\right\} = P_u M \sum_{t=0}^{M-1} T_0\ |\tilde{g}(t)|^2 \tag{2.9}$$

where

$$\tilde{g}(t) = \sum_k T_0\, g(t-kM) c_{\gamma\varphi}(t-kM-t_0) \tag{2.10}$$

Proof. From (2.3) we see that the diagonal of $\boldsymbol{H}_{\mathsf{u}}$ is given by the DFT of $\tilde{g}(t)$, which is the M-point overlap-and-add periodic version of $g(t)c_{\gamma\varphi}(t-t_0)$. By Parseval theorem the squared Frobenius norm of $\boldsymbol{H}_{\mathsf{u}}$ is therefore given by the energy of $\tilde{g}(t)$ in one period. □

We can therefore express the ideal synchronization point for the full band system as

$$t_0^{\mathrm{id}} = \arg\max_{t_0} \sum_t |\tilde{g}(t)|^2 \tag{2.11}$$

and we should note that the sum in (2.10) has at most $N/M+1$ terms. Moreover, in the most frequent case that $g(t)$ is shorter than M samples, the same sum in (2.10) has a single nonzero term for each t and (2.11) becomes

$$t_0^{\mathrm{id}} = \arg\max_{t_0} \sum_t |g(t)|^2\, c_{\gamma\varphi}^2(t-t_0)\ . \tag{2.12}$$

Observe that (2.12) resembles the results in [29,31] where $|g(t)|^2$ is replaced by its statistical expectation, and those in [32, 33], where the incorrect definition of the useful component based on (2.2) instead of (2.3) leads the authors to use $c_{\gamma\varphi}(t)$ instead of $c_{\gamma\varphi}^2(t)$.

2.3 Practical synchronization

2.3.1 Synchronization with a training sequence

In a practical synchronization scenario, the channel g is not known, but it must be estimated to a certain error from the received signal. We therefore assume that, for the purpose of synchronization, the receiver makes use of a known training sequence $x_{\mathsf{tr}}(t)$ of length L_{tr}, with impulsive autocorrelation and unit energy, that is transmitted in the preamble of each packet (for a packet-based transmission), or periodically inserted in a continuous transmission. Then, by taking the cross-correlation $y'(t)$ between the received and transmitted sequences

$$y'(t) = \sum_{u=0}^{L_{\mathsf{tr}}-1} T_0 \, x^*_{\mathsf{tr}}(u) y(u+t) = g(t) + w'(t) \tag{2.13a}$$

we obtain an estimate of the channel impulse response, corrupted by the noise $w'(t) = \sum_u T_0 \, x^*_{\mathsf{tr}}(u-t) w(u)$ that is again complex-valued and Gaussian, with independent components having zero mean and variance σ_w^2.

2.3.2 Existing methods

Several timing algorithms have been proposed in the OFDM literature, that exploit a training sequence with impulsive autocorrelation. They follow either of two approaches:

- *amplitude-based*: searching for either the first instant in which $y'(t)$ exceeds a certain amplitude threshold [26], or for the point of maximum amplitude [34, §4.6] [35]. The latter method is well suited for line of sight (LOS) or non dispersive channels, while the former is appropriate when the first few channel paths are the strongest.
- *energy-based*: searching for a window of μ consecutive samples with maximal energy of $y'(t)$ [34, §4.7] [36]. This method provides nearly optimal synchronization for arbitrary channels with a delay spread less than μ.

A more popular approach is to transmit a *periodic* training sequence and to make use of the cross energy between two sliding rectangular windows of the received signal separated by one sequence period. The timing estimate is then located as the window position that maximizes either the cross energy [23], or its value normalized versus the auto energy [25], or the difference between the two [37], possibly with a weighting coefficient depending on the signal to noise ratio (SNR) [24] (see [37] for an overview of these methods). However, the

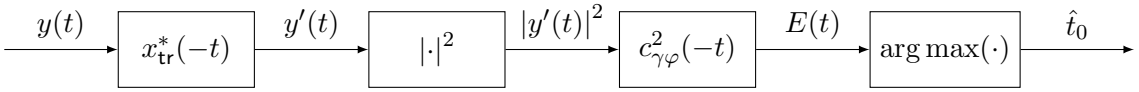

Figure 2.3. *Block diagram of the proposed method for symbol synchronization, showing the two filters needed to calculate correlations with $x_{\mathsf{tr}}(t)$ and $c^2_{\gamma\varphi}(t)$.*

widespread use of this class of methods is not justified on the ground of a better performance in timing estimation, but rather by their robustness with respect to carrier frequency offsets, as well as by a lower computational complexity. As a matter of fact, it was shown in [26] and [27] (among others) that correlation methods can exhibit better performance, especially at low SNR, since they make use of the clean transmitted template instead of the noisy received one.

As regards works that consider the channel to be longer than the cyclic prefix [29, 31], they do not yield a practical synchronization algorithm making use of the training sequence, as they are based on either the knowledge of channel statistics, which is unrealistic, or their accurate estimation, which requires long observations. A practical synchronizer can instead be derived from [32], while [33] proposes a blind (non data aided) version of the same method.

2.3.3 Formulation of the proposed estimator

We now propose a timing method based on (2.12). The formulation is similar to that in [36] or in [32] but instead of maximizing the energy of $y'(t)$ in a rectangular or trapezoidal window we seek

$$\hat{t}_0 = \arg\max_{t_0} E(t_0)\ , \quad E(t_0) = \sum_t T_0\ \left|y'(t)\right|^2 c^2_{\gamma\varphi}(t - t_0)\ . \tag{2.14}$$

Under the hypothesis that $g(t)$ is not longer than M samples, and except for very low SNR, this maximizes the useful component (2.9) in the full band system. Moreover, even in a system with unused or tapered subcarriers, we expect a nearly optimal performance since the energy fraction that is lost in the unused carriers is always kept low for the sake of spectral efficiency. Observe that, as shown in Figure 2.3, the function $E(\cdot)$ can be efficiently evaluated as the cascade of a first correlation, a magnitude squaring and another correlation.

2.3.4 Upper bounds for synchronization performance

In order to evaluate the effectiveness of the proposed synchronization method we now establish some upper bounds on the performance that can be achieved in a realistic environment (hence not full band, in general).

A first upper bound is of course represented by the SINR that can be achieved with ideal synchronization, that is by maximizing (2.5) under perfect knowledge of the channel realization $g(t)$

$$t_0^{\mathrm{id}} = \arg\max_{t_0} \Lambda \tag{2.15}$$

or in a nearly equivalent way by maximizing the useful power[3]

$$t_0^{\mathrm{id}} = \arg\max_{t_0} \mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{u}}(n)\|^2\right\} = \arg\max_{t_0} \{\boldsymbol{g}^* \boldsymbol{D}(t_0)\boldsymbol{g}\} \tag{2.16}$$

where the vector $\boldsymbol{g}$ collects the channel impulse response and the general entry in the matrix $\boldsymbol{D}(t_0)$ is given by

$$D_{tu}(t_0) = \sum_i T_0\, P_i W_M^{i(t-u)} c_{\gamma\varphi}(t - t_0) c_{\gamma\varphi}(u - t_0)\ . \tag{2.17}$$

On a less ideal yet still optimistic assumption, the receiver will not have perfect knowledge of the actual realization of the channel impulse response, but of its statistics. We seek the optimal timing estimator that maximizes the power of the useful component $\mathbb{E}\left\{\|\boldsymbol{v}_{\mathsf{u}}(n)\|^2\right\}$ based on the observation of the received signal $y(t)$ and the knowledge of the channel statistical description. By collecting the received samples into the vector $\boldsymbol{y}$ and making $\boldsymbol{g}$ a random vector with known probability density function (PDF), we can write the optimal timing estimator as the function

$$\hat{t}_0^{\mathrm{opt}} = \nu^{\mathrm{opt}}(\boldsymbol{y}) \tag{2.18}$$

that maximizes

$$\mathbb{E}\left\{\boldsymbol{g}^* \boldsymbol{D}(\nu(\boldsymbol{y}))\boldsymbol{g}\right\} \tag{2.19}$$

over all possible $\nu(\cdot)$. Such function is given by

$$\nu^{\mathrm{opt}}(\boldsymbol{\psi}) = \arg\max_{t_0} \left\{\mathbb{E}\left\{\boldsymbol{g}^* \boldsymbol{D}(t_0)\boldsymbol{g} | \boldsymbol{y} = \boldsymbol{\psi}\right\}\right\} \tag{2.20}$$

where the conditional expectation is not easily evaluated, unless the channel coefficients exhibit independent fading. The corresponding expected useful power is given by the value of (2.19) with $\nu^{\mathrm{opt}}(\boldsymbol{y})$ replacing $\nu(\boldsymbol{y})$. While the ideal synchronization (2.15)-(2.16) yields the

[3] Equivalence holds to a very good approximation as long as the fraction of unused carriers is small.

best performance among all schemes, including those that make use of channel side information, the estimator (2.18)-(2.20) yields the highest SINR among all the schemes that derive their estimate from $y(t)$. It is therefore more meaningful as an upper bound benchmark for the performance of practical estimators.

2.4 Simulations and results

2.4.1 The ECMA-368 UWB Multiband OFDM system

In order to assess the performance of the proposed method, and compare it with existing methods and with the upper bounds derived in Section 2.3.4, we have considered a system complying with the ECMA-368 standard [11]. UWB MB-OFDM systems guarantee high transmission bit rate, for wireless, low-range transmissions. To achieve these performances, those systems implement frequency hopping (FH) across large portions of the available spectrum, thus allowing successive OFDM symbols to be transmitted over different bands. In particular, the ECMA-368 transmitted signal occupies the unlicensed frequencies from $3.1\,$GHz to $10.6\,$GHz. The total spectrum is subdivided in 14 bands, each

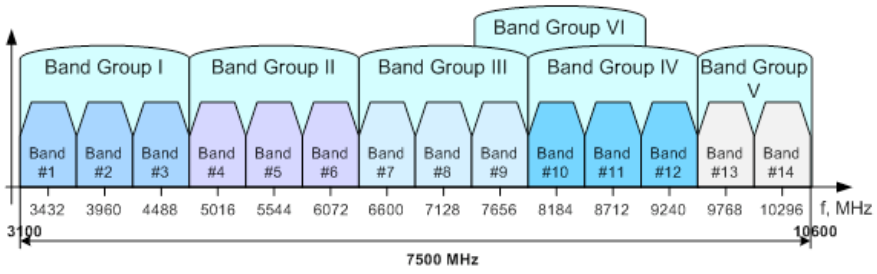

Figure 2.4. *Spectrum allocation of the UWB MB-OFDM system described in the standard [11]. Frequency hopping is implemented within each band group.*

having width $F_0 = 528\,$MHz, as shown in Figure 2.4. The first 12 bands are collected in 4 groups, each consisting of 3 bands, whereas the last 2 bands form a separated group. Then, FH is implemented among the 3 bands that form a single group, according to a periodical scheme repeated every 6 OFDM symbols. The central frequencies of the the 14 bands are

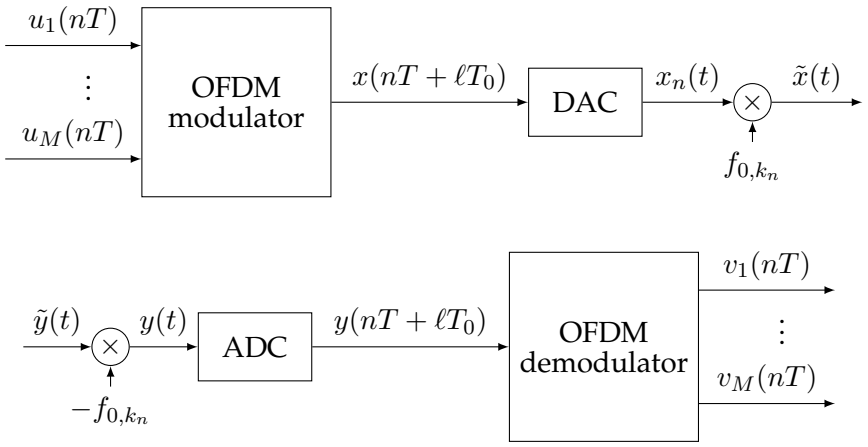

Figure 2.5. *Multiband OFDM modulator and demodulator. Different OFDM symbols are transmitted over different bands according to the FH scheme.*

given by

$$f_{0,k} = (k + 5.5)F_0 = 3432, \ldots, 10296\,\text{MHz}. \tag{2.21}$$

On recalling the system model described in Section 1.1, at the n-th OFDM symbol period, the transmitted signal is obtained by modulating the complex valued symbols in the vector vector $\boldsymbol{u}(nT) = [u_1(nT), u_2(nT), \ldots, u_M(nT)]^T$ with the transmit filters $\gamma_i(t)$, $i = 1, \ldots, M$. Then, the so obtained time domain values are fed to the DAC. The baseband analog signal

$$x_n(t) = \sum_{i=1}^{M} u_i(nT)\gamma_0(t - nT)e^{j2\pi m_i F_{\mathsf{u}}(t-nT)}, \tag{2.22}$$

is then upconverted with frequency f_{0,k_n}, determined by the FH sequence k_n giving for the analytic representation of the modulated signal

$$\tilde{x}(t) = \sum_{n=-\infty}^{+\infty} x_n(t)e^{j2\pi f_{0,k_n}t} \tag{2.23}$$

$$= \sum_{i=1}^{M}\sum_{n=-\infty}^{+\infty} u_i(nT)\gamma_0(t - nT)e^{j2\pi(f_{i,k_n}t - m_i F_{\mathsf{u}} nT)}, \tag{2.24}$$

where the subcarrier frequencies are $f_{i,k} = f_{0,k} + m_i F_{\mathsf{u}}$.

The channel impulse response and the additive noise can be replaced by their analytic representations $\tilde{g}(t)$ and $\tilde{w}(t)$ respectively, and we obtain the analytic representation of the signal at the receiver input

$$\tilde{y}(t) = \tilde{x} * \tilde{g}(t) + \tilde{w}(t). \tag{2.25}$$

At the receiver, downconversion is performed following the same FH sequence. Then, after

anti-aliasing filtering, the signal is sampled with frequency F_0 and fed to the corresponding OFDM demodulator, that filters the baseband received signal with the filters $\varphi_i(t)$.

The OFDM modulation scheme consists of a DMT modulation with ZS over a single band. Among the $M = 128$ available subcarriers, only $I = 122$ are active and carry data or pilot symbols for channel estimation and synchronization, whereas the others are guard subcarriers that are switched off to avoid interband interference. Data symbols $u_i(nT)$ belong to a QPSK or 16-QAM constellation. The zero-padding guard interval consists of $\mu = 32$ samples. Moreover, 5 further zero samples are appended to each OFDM symbol in order to allow oscillators to switch from one band to another in the FH sequence.

To allow for time and frequency synchronization, the standard [11] defines a preamble that is added at the beginning of every data packet: it is made up from the repetition (12 or 24 times) of a single OFDM symbol transmitted over the 3 different bands according to the periodical FH scheme, with period $6T$. Each time domain signal corresponding to a single OFDM symbol has approximately impulsive autocorrelation. In Table 2.1 we summarize the parameters that characterize the OFDM modulation adopted by the ECMA-368 standard.

parameter	**(nominal) value**
sampling frequency	$F_0 = 528\,\text{MHz}$
sampling period	$T_0 = 1/F_0 = 1.894\,\text{ns}$
FFT size	$M = 128$
intercarrier spacing	$F_u = F_0/M = 4.125\,\text{MHz}$
nr. of active subcarriers	$I = 122$
nr. of samples in a OFDM symbol	$N = 165$
OFDM symbol period	$T = NT_0 = 312.5\,\text{ns}$
central frequency for k-th band	$f_{0,k} = (k + 5.5)F_0$ $= 3432, \ldots, 10296\,\text{MHz}$

Table 2.1. *OFDM parameters for the ECMA-368 system*

2.4.2 Results

Different channel models and SNR values ranging from $0\,\text{dB}$ to $35\,\text{dB}$ have been considered in simulations. For each realization of the channel and noise, we have performed timing synchronization based on the training sequence with the methods described in Section 2.3,

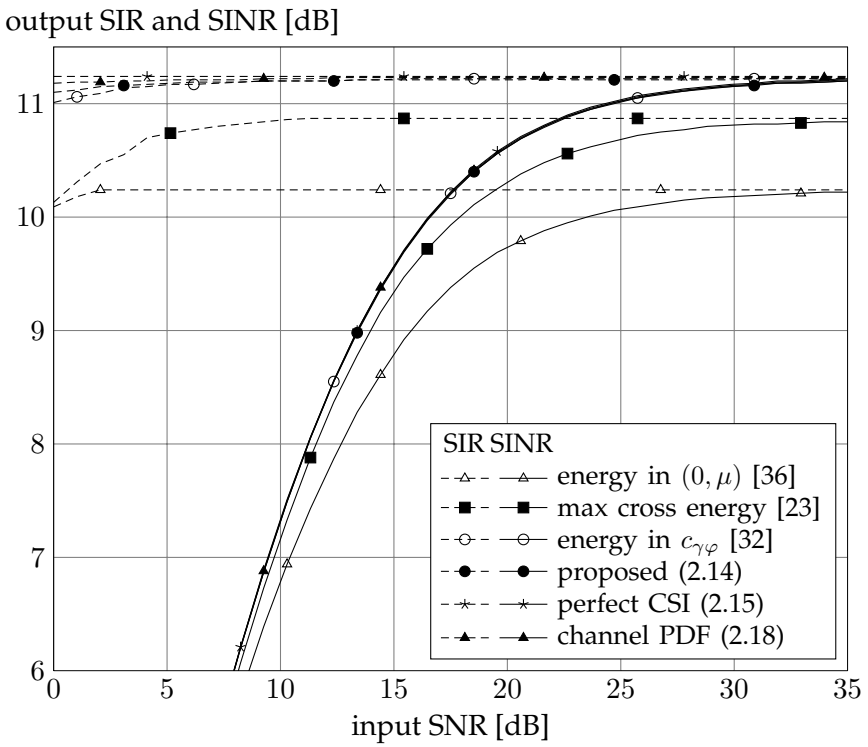

Figure 2.6. *SIR and SINR after demodulation, versus input SNR, with different synchronization algorithms. The channel coefficients have independent Rayleigh fading with a constant power delay profile. The upper bound curves and the performance curve of the proposed method consistently overlap over the whole SNR range.*

then have evaluated the signal to interference ratio (SIR) and the SINR (2.5) obtained by each method. Eventually, we have averaged the results over the channel and noise realizations.

The results shown in Figure 2.6 have been obtained for a 70-tap channel with independent Rayleigh fading and flat power delay profile, where the upper bound estimator (2.20) can be easily formulated. We can observe that the proposed method performance nearly coincides with both upper bounds, and shows a performance gain with respect to other methods (about 0.35 dB for cross energy methods and at least 1 dB for cross correlation methods), except for the one in [32] yielding very close performance.

We have also considered a more complicated and realistic channel model, i.e. the one presented in [30] for Ultra Wideband propagation in a non line of sight (NLOS) residential environment, which has given the results shown in Figure 2.7. Here it is not possible to derive (2.20) in a compact form, so we only show the performance obtained with (2.15) as an upper bound. Anyway, we see that the proposed solution shows only a 0.03 dB loss to

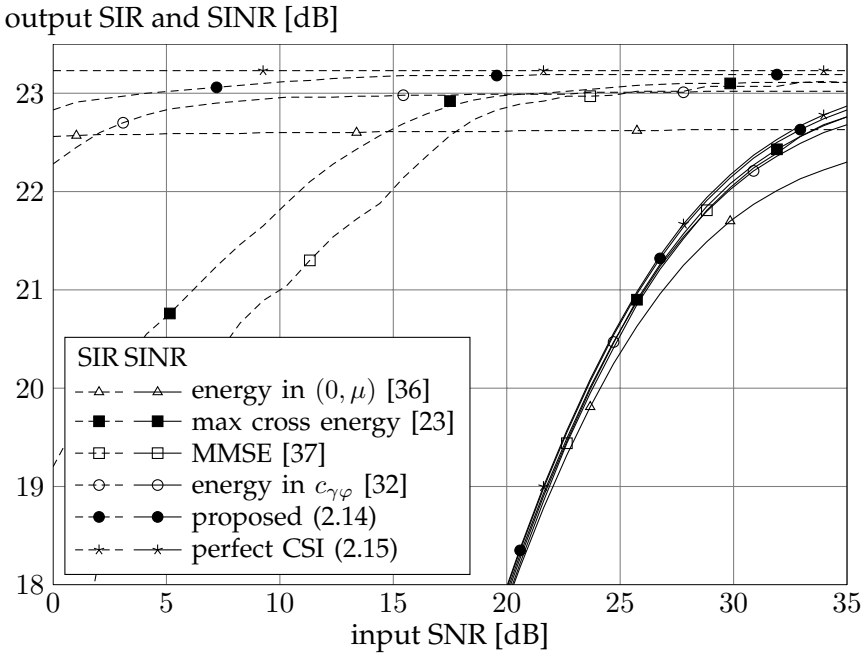

Figure 2.7. *SIR and SINR after demodulation, versus input SNR, for the UWB residential NLOS channel model [30]. Both the proposed method and the methods based on periodic sequenes approach the upper bound as regards the SINR, although they exhibit strong differences as regards SIR.*

the upper bound, while exhibiting a gain of 0.2 dB with respect to the method in [32] and of 0.6 dB to the method in [36]. As regards the cross energy methods [23, 37] we observe that despite their poor performance in terms of SIR in the low-medium SNR regime, when a global measure such as SINR is considered they approach the upper bounds (and the proposed estimator) closely, with a 0.1 dB loss.

Chapter 3

Carrier and clock frequency synchronization for MB-OFDM systems

The Multiband-OFDM modulation presented in Section 2.4 represents a modification of traditional OFDM that guarantees high transmission rates and robustness against dispersive channels by exploiting a large unlicensed spectrum. As a drawback, these systems, as all the OFDM-based transmissions, are particularly sensitive to the instability of oscillators. In fact, the carrier and sampling frequency offsets between the transmitter and the receiver destroy the orthogonality properties of the transmitted signal, thus provoking destructive interference among the signal components transmitted on the subchannels. As a result, the performance of the whole system suffers severe degradation. These considerations lead to the necessity of implementing precise carrier and sampling frequency offsets estimation and compensation at the receiver side.

In literature we can find different approaches to solve the frequency offset estimation problem that are specifically designed for OFDM modulation, as in [25, 38–41]. Here we focus on the UWB Multiband-OFDM system specified by the ECMA-368 standard [11], and propose two different algorithms for the joint estimation of both carrier and sampling frequency offset, beside discussing the adaptation of existing algorithms. The estimators, originally designed for OFDM transmission, are modified to suit the Multiband-OFDM signal structure. Only moderate complexity algorithms are considered, since the system has a high symbol rate, hence the estimation process must be performed quickly and can rely on a

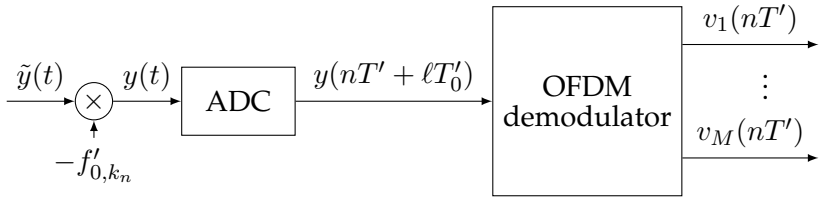

Figure 3.1. *Multiband OFDM demodulator. Non-idealities in the devices can introduce carrier frequency offsets* $\Delta f_{0,k} = f'_{0,k} - f_{0,k}$ *and clock frequency offset* $\Delta F_0 = F'_0 - F_0$.

fairly large amount of data.

Eventually the performance of the proposed algorithms is evaluated by simulation on a UWB channel scenario, and compared with current literature results, in terms of the estimates mean square error (MSE).

3.1 Multband OFDM with frequency offsets

The system model we adopt to consider the frequency synchronization problem has been described in Section 2.4.1. We assume that time synchronization is performed according with the method proposed in Chapter 2 and we consider the effects of carrier and clock frequency offsets. Namely, downconversion at the receiver is performed with carrier frequencies $f'_{0,k}$ that may differ from those at the transmitter by an offset $\Delta f_{0,k} = f'_{0,k} - f_{0,k}$. Hence, under the assumption that the channel delay spread does not exceed the duration T_{g} of the zero padded interval between symbols, we obtain the baseband signal[1]

$$y(t) = x * g(t) e^{-j2\pi \Delta f_{0,k_n} t} + w(t) \tag{3.1}$$

where $x(t)$ is the baseband version of $\tilde{x}(t)$, and $w(t)$ the downconverted noise. After antialiasing filtering, the signal is sampled with frequency $F'_0 = 1/T'_0$ that may itself differ from the transmitter value by an offset $\Delta F_0 = F'_0 - F_0$ so that the received complex-valued samples in the n-th OFDM symbol can be written as

$$y(nT' + \ell T'_0) = x * g(nT' + \ell T'_0) e^{-j2\pi \Delta f_{0,k_n} (nT' + \ell T'_0)} + w(nT' + \ell T'_0), \tag{3.2}$$

where $\ell = 0, \ldots, N-1$ and $T' = NT'_0$ is the receiver OFDM symbol period. When considering the outputs of the FFT block for the I subchannels, called the frequency domain values

[1]The standard [11] provides that the transmit carrier frequencies are phase coherent within a single band over the duration of a single packet. In deriving equations (3.1)–(3.4) we implicitly assume that the same holds for downconversion at the receiver side.

of the received signal, the two offsets combine into an equivalent subcarrier offset [41]

$$\Delta f_{i,k} = \Delta f_{0,k} + m_i \Delta F_0/M, \quad i = 1, \ldots, I \tag{3.3}$$

that causes the constellation to shrink and rotate, besides introducing ICI. Thus the frequency-domain received value for the n-th symbol period in the i-th subchannel is given by

$$v_i(nT') = AG(f_{i,k_n})u_i(nT)e^{-j2\pi\Delta f_{i,k_n}nT'} + \xi(nT'), \tag{3.4}$$

with $G(f_{i,k})$ the channel response at the frequency $f_{i,k}$, $A = \mathrm{sinc}_N(\Delta f_{i,k_n}T')$ the attenuation factor and $\xi(nT')$ representing the sum of ICI and noise terms.

Targets for the estimator accuracy can be set starting from two requirements:

1. the amplitude attenuation and additional ICI power should not degrade the SNR on the i-th subchannel significantly;
2. the constellation rotation between two successive phase corrections should not bring the frequency domain value out of its correct decision region.

We start by focusing on requirement 1 and, using the expression for the average ICI power in [41] (see also [42], where only the carrier frequency offset is considered), the average SNR becomes

$$\Lambda_i' = \frac{\mathrm{sinc}_N^2(\Delta f_{i,k_n}T')\Lambda_i}{1 + [1 - \mathrm{sinc}_N^2(\Delta f_{i,k_n}T')]\Lambda_i} \tag{3.5}$$

where Λ_i is the SNR in the absence of a carrier frequency offset. Thus if we require $\Lambda_i' > (1-\varepsilon)\Lambda_i$ we get an upper bound on $|\Delta f_{i,k_n}|$ that can be very well approximated for $\varepsilon \ll 1$ as

$$|\Delta f_{i,k_n}| < \frac{1}{\pi T}\sqrt{\frac{3\varepsilon}{1 + \Lambda_i(1-\varepsilon)}} \tag{3.6}$$

For example, allowing a $0.1\,\mathrm{dB}$ loss ($\varepsilon = 0.023$) at an SNR $\Lambda_i = 20\,\mathrm{dB}$ we get $|\Delta f_{i,k_n}| < 6.5 \cdot 10^{-3} F_{\mathsf{u}} \simeq 27\,\mathrm{kHz}$, a bound that, as we will see, can easily be met by practical estimators.

As regards requirement 2, if L_φ is the number of OFDM symbols separating two consecutive instances of phase estimation and correction we need

$$|\Delta f_{i,k_n}| < \frac{1}{2\pi L_\varphi T'}\varphi_{\mathsf{max}} \tag{3.7}$$

with

$$\varphi_{\mathsf{max}} = \begin{cases} \pi/4 & , \text{ for QPSK} \\ \pi/4 - \arcsin\left(\sqrt{2}/3\right) & , \text{ for 16-QAM} \end{cases} \tag{3.8}$$

Therefore, the less precise the frequency estimator is, the more often phase correction must be accomplished. Alternatively, if channel estimation is only performed at the start of each

packet, a more precise frequency offset estimator will allow to use longer packets. For example, in order not to need any phase correction within a 100-symbol packet with a 16-QAM constellation it should be $|\Delta f_{i,k_n}| < 1.5\,\text{kHz}$ which represents rather a strong requirement.

3.2 Algorithms and analysis

3.2.1 Previous work

The literature on OFDM time and frequency synchronization is well developed, especially regarding estimation of carrier frequency offsets, whereas the problem of estimating sampling frequency offsets has received less attention. However, not all the proposed approaches for estimation of the offsets Δf_0 and ΔF_0 can be considered for the ECMA system, and even the appropriate algorithms must be modified in order to suit the FH structure of OFDM modulation in ECMA.

Most algorithms for carrier frequency estimation in OFDM systems follow the Schmidl-Cox approach [25,39], which requires a repeated pattern in the transmitted signal and makes use of the time-domain received samples. It can be adapted to the FH pattern by using equation (3.2) considering that due to the FH periodicity, the n-th and $(n+6)$-th OFDM symbols within the preamble are identical and transmitted on the same band, thus yielding the estimates

$$\widehat{\Delta f_{0,k}} = \frac{1}{2\pi 6T} \arg \left\{ \sum_{n:k_n=k} \sum_{\ell=0}^{N-1} y(nT' + \ell T'_0) y^*((n+6)T' + \ell T'_0) \right\} \tag{3.9}$$

A similar technique is employed in [43] in a rather naive fashion, and in a more refined version in [44] where the correlation between symbols at many different distances is used, thus achieving higher accuracy. However, as was pointed out by the authors themselves, this also has the drawback of reducing acquisition range of the estimator in [44] to $\Delta f_{0,k} \geq 1/[2d_{\mathsf{max}}T]$ where $d_{\mathsf{max}}T$ is the maximum lag value considered in the correlation. For the 12-symbol preamble, where $d_{\mathsf{max}} = 9$ this corresponds to about $40\,\text{ppm}$ for band #3 in the first band group, and about $20\,\text{ppm}$ for band #11. The solution proposed there is to reduce d_{max} when the initial offset is known a priori to be high, thereby trading acquisition range for variance.

As regards clock frequency estimation, Schmidl and Cox in [45] used frequency domain values such as those in (3.4), with the assumption that the carrier frequency offset had been

previously corrected, and their technique can be adapted to the ECMA-368 modulation as

$$\widehat{\Delta F_0} = \frac{M}{2\pi 6T} \frac{\sum_{i=1}^{I} \arg\left\{\sum_n v_i(nT')\, v_i^*((n+6)T')\right\}\, \rho_i\, m_i}{\sum_{i=1}^{I} \rho_i\, m_i^2} \tag{3.10}$$

where $\rho_i = \sum_n |v_i(nT')\, v_i^*((n+6)T')|$. A related approach is used in [46] where again it is assumed that the carrier frequency is ideally correct and the clock frequency is not estimated and corrected from the preamble at the beginning of each packet, but rather controlled in a closed tracking loop, during data transmission, with values derived from the pilot subchannels.

3.2.2 Weighted Least Squares Estimator (WLSE)

A possible scheme is to first obtain estimates $\widehat{\Delta f_{i,k}}$ of the equivalent offsets on all subcarriers, based on the frequency domain received values $v_i(nT')$, in a similar fashion to [38]. Then, an estimate of both the carrier and clock frequency offset can be derived from the $\widehat{\Delta f_{i,k}}$.

By recalling (3.4), estimates of the subcarrier offset can be expressed as [2]

$$\widehat{\Delta f_{i,k}} = \frac{1}{2\pi 6T} \arg\left\{ \sum_{n:k_n=k} v_i(nT')\, v_i^*((n+6)T') \right\} \tag{3.11}$$

where the sum is performed over all n such that both the n-th and $(n+6)$-th OFDM symbols are transmitted on the k-th band and are within the preamble. Then, the equivalent offset estimates for the I subcarriers in the three bands are grouped into the column vector $\hat{\boldsymbol{f}} = \left[\widehat{\Delta f_{1,k}}, \ldots, \widehat{\Delta f_{I,k+2}}\right]^T$. Then, we consider $\hat{\boldsymbol{f}}$ to be the observation vector of a further estimation process whose aim is to estimate the parameters $\Delta f_{0,k}, \Delta F_0$. The estimation is based on the fact that $\hat{\boldsymbol{f}}$ can be expressed as a linear function of the parameters, as

$$\widehat{\Delta f_{i,k}} = \Delta f_{i,k} + e_{i,k} = \Delta f_{0,k} + m_i \Delta F_0 / M + e_{i,k}\ , \tag{3.12}$$

with $e_{i,k}$ representing the error in the (i,k) estimate.

In the case when the three carrier frequencies of the same band group $\{f_{0,k}, f_{0,k+1}, f_{0,k+2}\}$ used for FH are given by three independent oscillators the vector parameter to be estimated

[2] These estimators can work properly as it is safe to assume that the maximum subcarrier offset is less than $\frac{1}{12T}$.

is $\boldsymbol{\vartheta} = [\Delta f_{0,k}, \Delta f_{0,k+1}, \Delta f_{0,k+2}, \Delta F_0]$ so we can write in matrix notation

$$\hat{\boldsymbol{f}} = \begin{bmatrix} \Delta f_{0,k}\mathbf{1} + \Delta F_0 \boldsymbol{m} \\ \Delta f_{0,k+1}\mathbf{1} + \Delta F_0 \boldsymbol{m} \\ \Delta f_{0,k+2}\mathbf{1} + \Delta F_0 \boldsymbol{m} \end{bmatrix} + \boldsymbol{e} = \boldsymbol{M}\boldsymbol{\vartheta} + \boldsymbol{e}, \tag{3.13}$$

where $\mathbf{1}$ is a column of 1's of length I, $\boldsymbol{m} = \frac{1}{M}\left[m_1 \ \dots \ m_I\right]^T$, $\boldsymbol{e} = \left[e_{1,k} \ \dots \ e_{I,k+2}\right]^T$ and

$$\boldsymbol{M} = \begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \boldsymbol{m} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \boldsymbol{m} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \boldsymbol{m} \end{bmatrix}$$

with $\mathbf{0}$ a column of I zeros.

On the other hand if the three carrier frequencies are derived from the same oscillator, then we have $\frac{f'_{0,k}}{k+11/2} = \frac{f'_{0,k+1}}{k+13/2} = \frac{f'_{0,k+2}}{k+15/2}$, so we can restrict the vector parameter to be $\boldsymbol{\vartheta} = [\Delta f_{0,k}, \Delta F_0]$ and equation (3.13) can still be written with

$$\boldsymbol{M} = \begin{bmatrix} \mathbf{1} & \boldsymbol{m} \\ \frac{k+13/2}{k+11/2}\mathbf{1} & \boldsymbol{m} \\ \frac{k+15/2}{k+11/2}\mathbf{1} & \boldsymbol{m} \end{bmatrix}$$

Eventually, when the same oscillator drives all the carriers and the sampling clock, we only need to estimate one parameter, say $\boldsymbol{\vartheta} = \Delta F_0$ and the matrix $\boldsymbol{M}$ in (3.13) becomes

$$\boldsymbol{M} = \begin{bmatrix} (k+11/2)\mathbf{1} + \boldsymbol{m} \\ (k+13/2)\mathbf{1} + \boldsymbol{m} \\ (k+15/2)\mathbf{1} + \boldsymbol{m} \end{bmatrix}$$

In the hypothesis that the estimators $\widehat{\Delta f_{i,k}}$ are unbiased, orthogonal and with the same variance, the *best linear unbiased estimator* (BLUE) would be the linear least squares estimator [47]. On the contrary when the transmission takes place on a frequency selective channel, as in UWB, the estimators $\widehat{\Delta f_{i,k}}$ are characterized by widely different variances, according to the SNR value of each subcarrier. In this case, the BLUE is given by the *weighted* least squares estimator (WLSE) [47]

$$\widehat{\boldsymbol{\vartheta}} = \boldsymbol{\Theta}_{\mathsf{WLSE}}^T \hat{\boldsymbol{f}}, \ \ \boldsymbol{\Theta}_{\mathsf{WLSE}}^T = \left(\boldsymbol{M}^T \boldsymbol{W} \boldsymbol{M}\right)^{-1} \boldsymbol{M}^T \boldsymbol{W} \tag{3.14}$$

with weight matrix $\boldsymbol{W} = \boldsymbol{K}_{\hat{\boldsymbol{f}}}^{-1}$, where $\boldsymbol{K}_{\hat{\boldsymbol{f}}} = \operatorname{diag}\left(\{\sigma^2_{\widehat{\Delta f_{i,k}}}\}\right)$ is the covariance matrix of the vector $\hat{\boldsymbol{f}}$. In particular, it is shown in [48] that, when the SNR at the (i,k) subcarrier is $\Lambda_{i,k} > 10\,\text{dB}$,

$$\sigma^2_{\widehat{\Delta f_{i,k}}} \simeq \frac{1}{(2\pi 6T)^2 \Lambda_{i,k}}. \tag{3.15}$$

As the SNR values $\Lambda_{i,k}$ are not available in general, prior to channel estimation, we replace the weight matrix $\boldsymbol{W}$ in equation (3.14) with $\mathrm{diag}\left(\{\rho_{i,k}\}\right)$ where

$$\rho_{i,k} = \sum_{n:k_n=k} \left| v_i(nT') v_i^*((n+6)T') \right|$$

are roughly proportional to $\Lambda_{i,k}$.

3.2.3 Joint Maximum Likelihood Estimator (JMLE)

With a low SNR on some subcarriers the corresponding $\Delta f_{i,k}$ may extend beyond the unbias interval of its estimator, hence the WLSE performance will suffer in harsh dispersive channels. For this reason, it is more convenient to have the estimation rely directly on the demodulated FFT output rather than going through the equivalent subcarrier offset estimates.

In [41] a *joint approximate maximum likelihood estimator* (JMLE) for both Δf_0 and ΔF_0 is derived that uses the information carried by the frequency domain values of two repeated OFDM symbols: hence, the log-likelihood function is

$$\begin{aligned} &\ln p(\boldsymbol{v}((n+6)T'), \boldsymbol{v}(nT')|\boldsymbol{\vartheta}) = \\ &\ln p(\boldsymbol{v}((n+6)T')|\boldsymbol{v}(nT'), \boldsymbol{\vartheta}) + \ln p(\boldsymbol{v}(nT')|\boldsymbol{\vartheta}), \end{aligned} \tag{3.16}$$

where $p(\cdot|\cdot)$ indicates the conditional probability density function. By making the assumption that the ICI term and the attenuation on the useful part of the received signal are independent from the frequency offset[3], in [41] it is shown that the maximum likelihood estimator of $\boldsymbol{\vartheta}$ is the value $\widehat{\boldsymbol{\vartheta}}$ that maximizes the expression

$$\Lambda_{\mathsf{JMLE}}(\boldsymbol{\vartheta}) = \mathrm{Re}\left[\boldsymbol{\delta}^* \tilde{\boldsymbol{v}}\right], \tag{3.17}$$

where

$$\boldsymbol{\delta}^* = \left[e^{j2\pi\Delta f_{1,k} 6T} \ \cdots \ e^{j2\pi\Delta f_{I,k+2} 6T} \right] \tag{3.18}$$

$$\tilde{\boldsymbol{v}} = \left[\tilde{v}_{1,k} \ \cdots \ \tilde{v}_{I,k+2} \right]^T \tag{3.19}$$

with

$$\tilde{v}_{i,k} = \sum_{n:k_n=k} v_i((n+6)T') v_i^*(nT') \tag{3.20}$$

[3]This hypothesis is not consistent, but the performances obtained making this approximation are still very competitive, as we will see in the simulation section.

Now we can express the log-likelihood function with the substitutions $\alpha_k = 2\pi\Delta f_{0,k}6T$ and $\beta = 2\pi\Delta F_0 6T/M$ and obtain

$$\Lambda_{\mathsf{JMLE}}(\boldsymbol{\vartheta}) = \mathrm{Re}\left(\sum_k \sum_{i=1}^{I} e^{j(\alpha_k + m_i\beta)}\tilde{v}_{i,k}\right) = \mathrm{Re}\left[\sum_k e^{j\alpha_k}\tilde{V}_k(\beta)\right], \tag{3.21}$$

where

$$\tilde{V}_k(\beta) = \sum_{i=1}^{I} \tilde{v}_{i,k} e^{jm_i\beta} \tag{3.22}$$

are Fourier sums with coefficients $\{\tilde{v}_{i,k}\}$. Hence, the estimation process consists in a maximization problem over the vector $\boldsymbol{\vartheta}$, depending on whether four distinct oscillator are used at receiver, or just two oscillator (one for all carriers, one for the sampling clock), or a single one (driving all carriers and the clock). In the first case the maximization is easily solved as

$$\hat{\beta} = \arg\max_{\beta} \sum_k \left|\tilde{V}_k(\beta)\right| \ , \ \ \hat{\alpha}_k = -\arg\tilde{V}_k(\hat{\beta}) \tag{3.23}$$

whereas in the second case, the solution is the pair

$$\begin{aligned}(\hat{\alpha}_k, \hat{\beta}) = \arg\max_{\alpha_k,\beta} \\ \mathrm{Re}\left[e^{j\alpha_k}\tilde{V}_k(\beta) + e^{j\frac{k+13/2}{k+11/2}\alpha_k}\tilde{V}_{k+1}(\beta) + e^{j\frac{k+15/2}{k+11/2}\alpha_k}\tilde{V}_{k+2}(\beta)\right]\end{aligned} \tag{3.24}$$

and in the third case we have

$$\hat{\beta} = \arg\max_{\beta} \sum_k \mathrm{Re}\left[e^{jM(k+11/2)\beta}\tilde{V}_k(\beta)\right] \quad , \quad \hat{\alpha}_k = (k+11/2)M\hat{\beta} \tag{3.25}$$

In all cases we finally get the offset estimators as

$$\widehat{\Delta F_0} = \frac{M}{2\pi 6T}\hat{\beta} \ , \ \ \widehat{\Delta f_{0,k}} = \frac{1}{2\pi 6T}\hat{\alpha}_k \tag{3.26}$$

Notice that, as $\tilde{V}_k(\beta)$ is periodic by 2π, the acquisition range for ΔF_0 extends up to $M/(12T)$, corresponding to about 6.5% of the sampling frequency nominal value, far beyond the instability of any practical oscillator. However it seems reasonable to keep the interval of evaluation for $\tilde{V}(\beta)$ within the limits for practical oscillators (up to a few hundreds ppm). Similarly, from the periodicity with respect to α_k, we easily derive that the acquisition range for $\Delta f_{0,k}$ is $1/(12T)$ in the case of four oscillators, corresponding to 77 ppm for band #1, then as the band number increases, down to 25 ppm for band #14. On the other hand it increases to $(2k+11)/(12T)$, corresponding to about $1/1000$ of its nominal value, in the case of two oscillators, and to the 6.5% of its nominal value when it is derived from the same oscillator as F_0.

The computational burden of evaluating the series $\tilde{V}_k(\beta)$ over a sufficiently fine grid can either be reduced through the efficient computation of the DFT of sparse sequences [49], or circumvented through a second order MacLaurin series approximation that for instance, in the case of four distinct oscillators leads to the closed form estimator

$$\hat{\beta} = -\frac{\sum_k \mathrm{Re}[\tilde{V}_k'(0)\tilde{V}_k^*(0)]}{\sum_k \mathrm{Re}[\tilde{V}_k''(0)\tilde{V}_k^*(0)] + \sum_k |\tilde{V}_k'(0)|^2} \tag{3.27}$$

$$\hat{\alpha}_k = -\arg\left(\tilde{V}_k(0) + \hat{\beta}\tilde{V}_k'(0) + \frac{1}{2}\hat{\beta}^2\tilde{V}_k''(0)\right) \tag{3.28}$$

with

$$\tilde{V}_k(0) = \sum_{i=1}^{I} \tilde{v}_{i,k},\ \tilde{V}_k'(0) = j\sum_{i=1}^{I} m_i\tilde{v}_{i,k},\ \tilde{V}_k''(0) = -\sum_{i=1}^{I} m_i^2\tilde{v}_{i,k}\ . \tag{3.29}$$

As can be expected the above approximation leads to some loss in performance especially for low SNR, when the maximum of the likelihood function is not sharp enough.

3.3 Simulations and results

The performance of the algorithms presented in the previous section has been evaluated through simulations and compared to other solutions proposed in the literature for OFDM and MB-OFDM systems. We have simulated transmission over the first band group with the UWB propagation channel modeled according to the characteristics of the LOS indoor office scenario given in [30] and estimation is based on the standard 12-symbol preamble preceding each packet. Moreover, quantization effects introduced by the receiver ADC were modeled as well, setting an 8 bit representation for both the in-phase and quadrature component of the received signal.

Three different scenarios have been simulated, according to different implementation of the radio frequency MB-OFDM receiver front-end. In the first case, a different oscillators generates the demodulating carriers for each band, and another one drives the sampling clock, so that all four frequency offsets can have different values. We have implemented the joint ML estimator via the algorithm in [49] to compute $\tilde{V}_k(\beta)$ with a resolution of about $170\,\mathrm{Hz}$ in the grid of possible values for ΔF_0, as well as through the second-order approximation formula. The algorithm by Schimdl and Cox has been implemented considering repeated OFDM symbols at distance $6T$ within the synchronization preamble, and we have also implemented the scheme described in [44] with a similar approach, based on the correlation of the whole preamble at different lag values. The performance of all algorithms

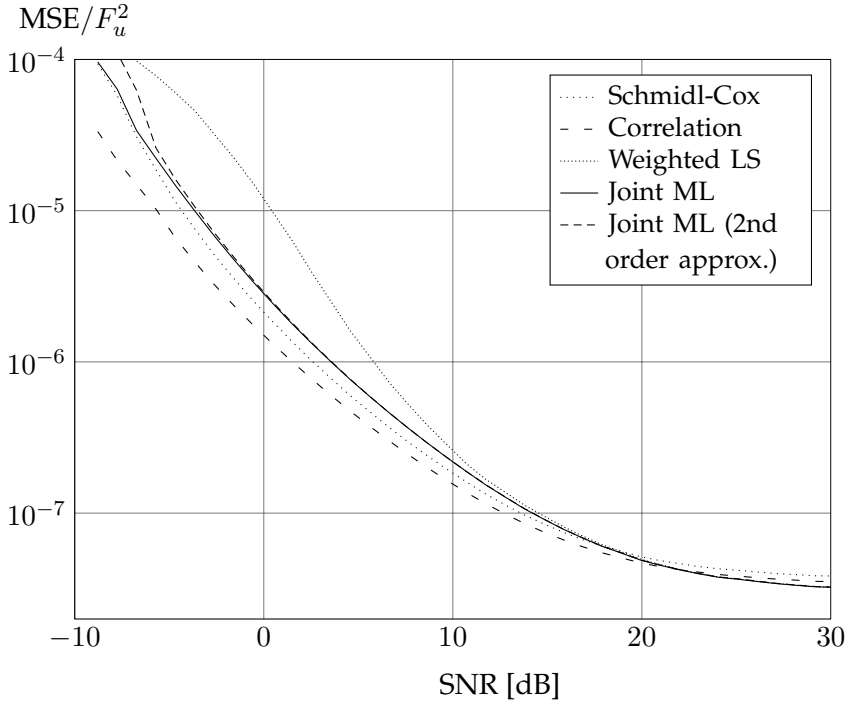

Figure 3.2. *MSE of the carrier frequency offset estimates in the case when each demodulating carrier and the sampling clock is driven by an independent oscillators.*

has been assessed in terms of the MSE of the clock offset estimate, and the average of the MSE for the estimates of the three carrier frequencies. Figs. 3.2 and 3.3 show results with the true offset values set to $\Delta F_0/F_0 = 20\,\text{ppm}$, $\Delta f_{0,1}/f_{0,1} = 15\,\text{ppm}$, $\Delta f_{0,2}/f_{0,2} = 10\,\text{ppm}$ and $\Delta f_{0,3}/f_{0,3} = -20\,\text{ppm}$ and we can observe that the different methods offer similar performance for high SNR ($> 15\,\text{dB}$) but the carrier estimates obtained with the correlation approach are more precise than the others for lower SNR values. On the other hand, the latter algorithm does not estimate the clock frequency offset, and in Figure 3.3 we can see that JMLE shows the best performance in the clock frequency offset estimation, especially in the low-SNR region. Observe also that the weighted LS algorithm shows poor performances in the low-medium SNR region, and that the second-order approximation of the ML scheme well approaches the performance of the more complex grid evaluation for SNR over $0\,\text{dB}$.

In the second scenario, all three carriers are derived from a unique oscillator, hence the corresponding frequency offsets are linked to each other by a multiplicative constant, but are independent of the clock frequency, which is given by a second oscillator. Here, the proposed weighted LS and joint ML algorithms are compared with the Schmidl-Cox algorithm and both the methods presented in [44]. In the implementation of the Schmidl-Cox algo-

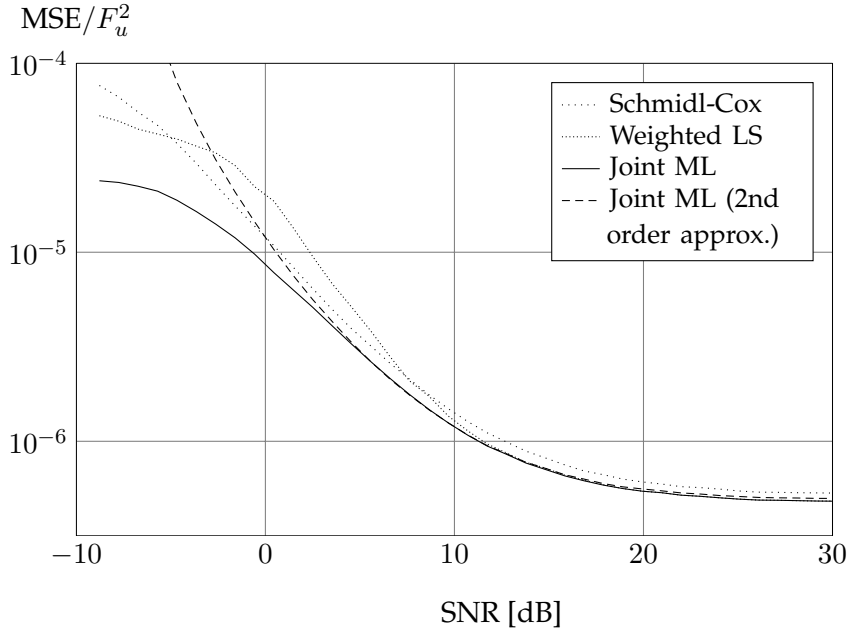

Figure 3.3. *MSE of the clock frequency offset estimates in the case when each demodulating carrier and the sampling clock is driven by an independent oscillators.*

rithm, the 3 carrier offsets are estimated separately, then a linear regression is applied to the three values to determine the single final estimate. The same is done for the estimator based on correlation and averaging cited in [44] while the second more sophisticated algorithm in [44], based on the BLUE principle, takes also into account the different channel responses and the different channel energies in the the three bands. However, as in the adopted channel model the three bands have very similar energies, the performance of the two algorithms aree indistinguishable. In Figures 3.4 and 3.5 we see the results obtained with offset values $\Delta F_0 = 10\,\text{ppm}$, $\Delta f_{0,1}/f_{0,1} = \Delta f_{0,2}/f_{0,2} = \Delta f_{0,3}/f_{0,3} = 20\,\text{ppm}$. The Li-Jacobs-Minn method exhibits the lowest MSE for carrier frequency estimation in this case, as shown by the curves in Figure 3.4, due to its averaging of the estimates over the three bands and to the small sampling frequency offset. As regards clock frequency estimation, Figure 3.5 shows again that the joint ML algorithm offers better performance compared to the weighted LS and the Schmidl-Cox technique.

Finally, following the standard [11] directive to derive sampling frequency and carrier frequencies from the same oscillator at the transmitter, in the third scenario we assume that the same is done at the receiver, so that the four frequencies are linked by multiplicative constants. Since in this case $\widehat{\Delta F_0}$ can be retrieved from the carrier offset estimation, we

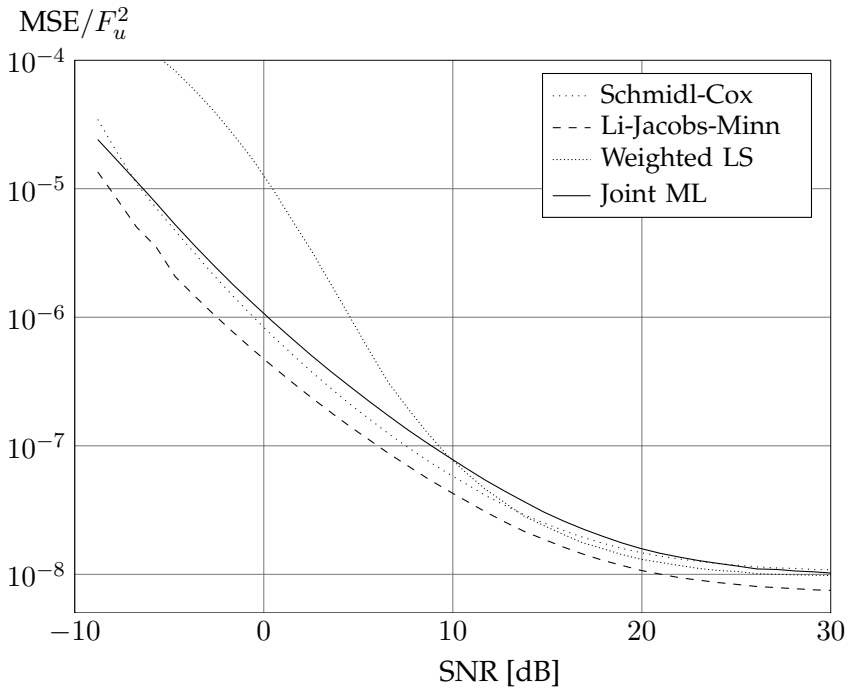

Figure 3.4. *MSE of the carrier frequency offset estimates in the case when a single oscillator drives all demodulating carriers.*

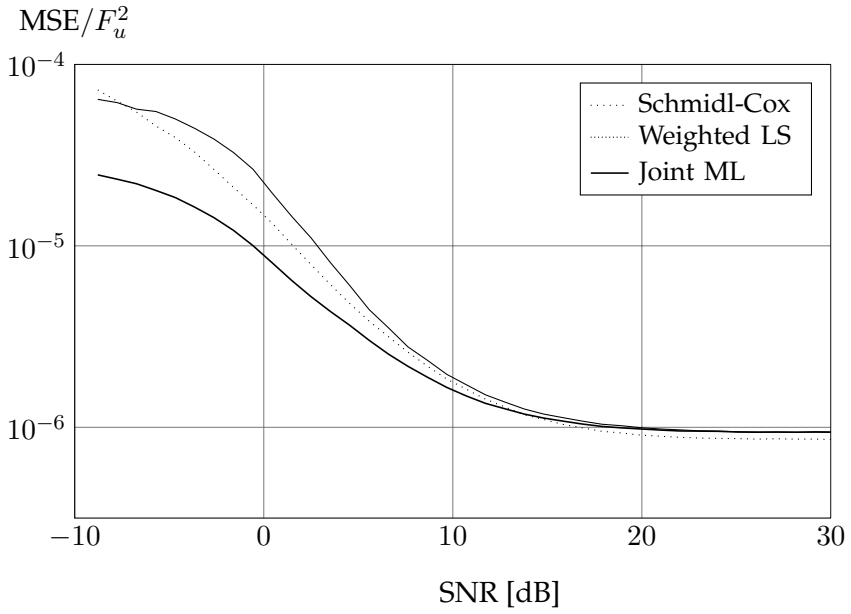

Figure 3.5. *MSE of the clock frequency offset estimates in the case when a single oscillator drives all demodulating carriers.*

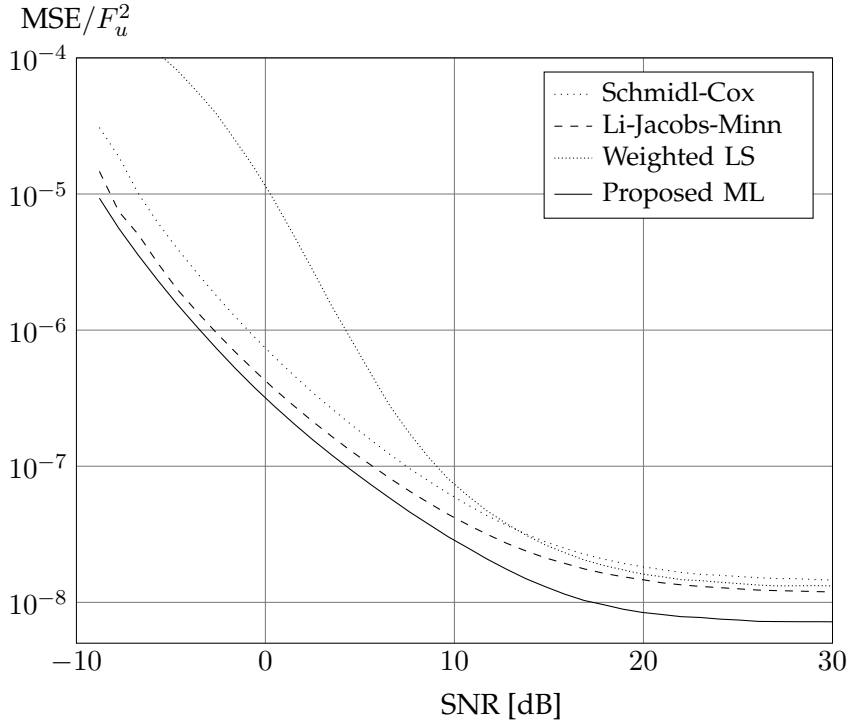

Figure 3.6. *MSE of the carrier frequency offset estimates in the case when a single oscillator drives both sampling clock and demodulating carriers.*

evaluate the algorithm performance only in terms of the MSE for carrier offset. The results shown in Figure 3.6, for a true offset value of 20 ppm in the unique oscillator, prove that for this application scenario the ML algorithm outperforms the other approaches for both low and high SNR values. For instance, at 20 dB our estimator has an MSE of about $1.43 \cdot 10^5$ Hz^2, which guarantees the residual error after correction to be bounded within 1.1 kHz with high probability and from (3.7) allows to perform phase correction every 130 symbols with a 16-QAM constellation. Corrsepondingly, the Li-Jacobs-Minn estimator has a MSE of about $2.5 \cdot 10^5$ and requires phase compensation to be performed every 100 symbols.

Part II

Physical layer security

Chapter 4

Physical layer secrecy for OFDM systems

The exponentially increasing demand for wireless, ubiquitous communications and the need of a way to securely transmit data are becoming challenging constraints for system designers. Information secrecy has been assumed traditionally to be guaranteed by algorithms operating at the higher levels of communication protocols. More specifically, the problem of hiding information from malicious eavesdroppers has been tackled starting from the assumption of an underlying reliable end-to-end communication channel. However, recent results from Information Theory, as those cited in Chapter 1, have demonstrated that inherent randomness of wireless channels can be leveraged in order to provide secure communications. In particular, the physical layer of communications has been addressed as a valuable tool in order to guarantee confidentiality of the messages transmitted over the wireless medium.

Methods that ensure confidentiality of the message content by taking advantage of the OFDM system structure have recently appeared in the literature. The authors in [50] consider the possibility of applying elliptic curve cryptography to the OFDM modulated signal. However, the detrimental effects of the dispersive channel on the encrypted signal are not taken into account in the analysis. In [51], a technique previously implemented to secure optical transmissions is modified to suit the wireless OFDM scenario. Subcarrier symbols are mapped into a denser constellation according to a secret key and artificial noise is injected into the modulated signal in order to prevent reliable symbol detection by the eavesdropper. On the other hand, the legitimate receiver, being aware of the secret key, can demap

the received symbols back to the sparse constellation. In [52], chaos-based cryptography is applied in combination with channel coding in order to ensure secrecy and error detection at the same time. The OFDM setting is considered only when evaluating the system performance.

All the above methods are based on classical cryptographic approaches, which make use of some secret information (the key) previously exchanged between the legitimate parties. Knowledge of the key allows the legitimate receiver to efficiently decrypt the message, while, for an eavesdropper that does not share the secret key, decryption is impractically complex. In this work, instead, we aim to investigate the performance of an information-theoretic security approach, which is explicitly founded on the channel characteristics at the physical layer. In this case, secrecy of the transmitted message is offered by the randomness in the transmission channel and it is defined within a statistical framework. In this setting, the concept of perfect secrecy [53] is introduced as the statistical independence between the information bearing message and the eavesdropper's observations. The seminal works [12, 13] characterized secrecy capacity for a wiretap channel as the maximal rate at which information can be transmitted, while guaranteeing a vanishing mutual information rate between the message and the eavesdropper observations. In particular, the results on the secrecy capacity are based on the wiretap channel model introduced by Wyner [12]. In such model, a transmitter sends information to the legitimate receiver, but this is also received by the eavesdropper. The transmitter can adopt any encoding and modulation scheme and both the authorized and unauthorized receiver are aware of the transmission technique that has been used. Hence, they both are potentially able to recover the confidential message from the received signal when there is no difference between their channels. However, since the main channel and the eavesdropper channel are different (they are described in [12] through a discrete memoryless channel (DMC) model, with given transition probabilities), the received signals are also different. Based on these assumptions, physical layer security on the wiretap channel is achieved when the legitimate receiver is able to exactly reconstruct the secret message, whereas the asymptotic mutual information rate between the signal available to the eavesdropper and the confidential message is kept arbitrarily low. Then, Wyner's model was generalized by Csiszár and Körner for the broadcast channel with public and confidential messages [13]. A different channel model was adopted in [54], in which it was shown that over a wiretap channel with additive white Gaussian noise, it is impossible to guarantee secure communication when the eavesdrop-

per experiences channel conditions that are equal to (or better than) those of the legitimate receiver. However, apart from coding, diversity in the fading conditions can be exploited opportunistically to increase security. In particular, works [55] and [56] have shown that different fading states (or, equivalently, parallel Gaussian channels with different gains) offer the opportunity of secret communications even when the average SNR of the main channel is lower than the one of the eavesdropper. However, coding and power allocation need knowledge of the eavesdropper channel realization. On the other hand, in the work [57] a blind scheme has been proposed, that is only based on the statistical description of the eavesdropper channel and that achieves secrecy capacity. Multiple antennas represent another important asset to exploit to secure communications, since the degrees of freedom available at the transmitter side can be used to either encode information in the null space of the eavesdropper channel or to inject artificial noise to confuse the eavesdropper [58]. Also the secrecy capacity of the MIMO Gaussian wiretap channel has recently been characterized. In [59, 60] the authors give a complete characterization of the secrecy capacity under a matrix covariance constraint on the input covariance matrix. On the other hand, when a total power constraint is considered, the secrecy capacity can be computed only in the high-power [61] and low-power [62] regimes.

In order to provide practical implementations of information-theoretic security schemes over actual systems, it seems appropriate to further investigate the effects of the modulation format over the secrecy performance of the system. In the information-theoretic security literature, OFDM has usually been modeled as a set of parallel Gaussian channels [56,63,64], with the implicit assumption that also the eavesdropper adopts an OFDM demodulator with cyclic prefix removal and FFT. The secrecy capacity for this scenario and the corresponding power allocation have been derived [56]. Similarly, optimal power allocation strategies for the multiuser broadcast case are derived in [63] and [64]. In [65], the same parallel channels model is used, but secrecy is defined and achieved in terms of minimum mean squared error at the eavesdropper. In [66] the parallel channels framework is used to provide security by overloading subcarriers with multiple transmitters. The time varying channel is seen as a periodically renewed secret key, shared between the legitimate parties and kept hidden from the eavesdropper.

The assumption of an OFDM receiver at the eavesdropper is relaxed in [67], although the eavesdropper is still supposed to drop the initial part of each received symbol. Consequently, the scenario is modeled as a more general MIMO Gaussian wiretap channel (such as

those in [60] and [59]). In [67], the authors propose a Vandermonde precoding scheme that hides information in the null space of the equivalent eavesdropper MIMO channel matrix. However, the eavesdropper is still assumed to adhere to the decoding rules of the proposed protocol.

Our aim in this thesis is to consider the more conservative case in which the transmitter and the legitimate receiver adopt OFDM transmission, in particular DMT modulation, whereas the eavesdropper is free to implement a more sophisticated and possibly more effective receiver. The performance for this scenario is compared with that of the parallel channels model, i.e. when also the eavesdropper implements OFDM, and with the achievable secrecy rates of the frequency selective channel itself, regardless of the transceiver implementations of all the parties. In this way, we can quantify the cost due to implementation of OFDM to transmit data under perfect secrecy constraints.

4.1 Secrecy capacity of OFDM systems with a generic eavesdropper

Our objective is to assess the secrecy rates that are attainable when an OFDM system is deployed between the transmitter and the legitimate receiver, whereas the eavesdropper is allowed to use a more sophisticated demodulator. We consider only DMT modulation and we use the MIMO system model of Section 1.2 to describe the discrete time equivalent of OFDM transmissions. Both the main and the eavesdropper channels are fixed during transmissions, and they are known by all users. Without loss of generality, we consider normalized versions of the additive Gaussian noise, in order to write the corresponding covariance matrices as $\boldsymbol{K}_{\boldsymbol{w}_\mathsf{R}} = \boldsymbol{K}_{\boldsymbol{w}_\mathsf{E}} = \boldsymbol{I}$. We assume that the CP (or ZS) is longer than the delay spread of the main channel g_R in order to avoid ISI and ICI at the legitimate receiver. For the sake of compactness, we focus on the transmission of a single OFDM symbol. The scenario under analysis is first compared with the case in which the adversary also implements an OFDM receiver, which can be described by a parallel channel model as in [56] and [55]. Then, the same results are compared with those provided by the fading channels $(\boldsymbol{G}_\mathsf{R}, \boldsymbol{G}_\mathsf{E})$, without imposing any constraint on the modulation format. In this way, we are able to clearly quantify the burden of the OFDM scheme with respect to the potential performance provided by the fading channel itself.

When all the nodes in the network implement OFDM transmission, the system can be

regarded as the parallel of M Gaussian wiretap channels. The secrecy capacity for this scenario was characterized in [56] as

$$C_{\mathsf{s}} = \max_{\sum P_i \leq P} \sum_{i=1}^{M} \left[\log \frac{1 + |G_{\mathsf{R}}(f_i)|^2 P_i}{1 + |G_{\mathsf{E}}(f_i)|^2 P_i} \right]^+, \tag{4.1}$$

and the optimal input power allocation was derived by solving the Karush-Kuhn-Tucker (KKT) conditions of the convex maximization problem obtained by setting $P_i = 0$ whenever $|G_{\mathsf{R}}(f_i)| < |G_{\mathsf{E}}(f_i)|$.

On the other hand, once we refrain from imposing the OFDM structure to the eavesdropper demodulator, the orthogonality conditions at the eavesdropper side might not be satisfied and a parallel channel model does not capture the complexity of the signal received by the attacker. In this case, we can leverage the description in Section 1.2 of OFDM transmission as a particular instance of a MIMO channel. By combining the expressions of the channel outputs (1.28) and (1.30) with OFDM modulation (1.31) and demodulation (1.35), we can model the system as a whole, comprising the OFDM transmitter, the legitimate channel, the OFDM receiver and the eavesdropper channel, as a MIMO Gaussian wiretap channel [59, 60]:

$$\begin{aligned} \boldsymbol{v} &= \boldsymbol{H}_{\mathsf{R}} \boldsymbol{u} + \bar{\boldsymbol{w}}_{\mathsf{R}} \\ \text{and} \quad \boldsymbol{z} &= \boldsymbol{H}_{\mathsf{E}} \boldsymbol{u} + \boldsymbol{w}_{\mathsf{E}} \end{aligned} \tag{4.2}$$

with $\boldsymbol{H}_{\mathsf{R}} = \operatorname{diag}(G_{\mathsf{R}}(f_i))$, $\boldsymbol{H}_{\mathsf{E}} = \boldsymbol{G}_{\mathsf{E}} \boldsymbol{T}$ and $\bar{\boldsymbol{w}}_{\mathsf{R}} = \boldsymbol{R} \boldsymbol{w}_{\mathsf{R}}$. Consequently, the covariance matrix of the demodulated noise at the legitimate receiver is $\boldsymbol{K}_{\bar{\boldsymbol{w}}_{\mathsf{R}}} = \boldsymbol{R}\boldsymbol{R}^*$. Similarly, the covariance matrix of the channel input $\boldsymbol{x} = \boldsymbol{T}\boldsymbol{u}$ is given by $\boldsymbol{K}_{\boldsymbol{x}} = \boldsymbol{T}\boldsymbol{K}_{\boldsymbol{u}}\boldsymbol{T}^*$. Hence, we aim to determine the secrecy capacity for the MIMO Gaussian wiretap channel (4.2) under total power constraint on the transmitted signal:

$$\operatorname{tr}(\boldsymbol{K}_{\boldsymbol{x}}) = \operatorname{tr}(\boldsymbol{T}\boldsymbol{K}_{\boldsymbol{u}}\boldsymbol{T}^*) \leq P. \tag{4.3}$$

By using the general result of Csiszár and Körner [13], in particular its version extended to continuous alphabet problems with average cost constraints, one obtains the single letter expression of the secrecy capacity

$$C_{\mathsf{s}} = \max_{p(q, \boldsymbol{u})} [\mathbb{I}(q; \boldsymbol{v}) - \mathbb{I}(q; \boldsymbol{z})] \tag{4.4}$$

where q is an auxiliary random variable satisfying the Markov relation

$$q \to \boldsymbol{u} \to (\boldsymbol{v}, \boldsymbol{z}). \tag{4.5}$$

The optimal choice for the random variable q is determined by the following lemma, which leverages the results in [68] about the secrecy capacity of the MIMO Gaussian wiretap channel with matrix covariance constraint. In this scenario, the input covariance matrix $\boldsymbol{K_u}$ must satisfy the inequality $\boldsymbol{K_u} \preceq \boldsymbol{S}$.

Lemma 1. *The secrecy capacity of the MIMO Gaussian wiretap channel (4.2) under the trace constraint (4.3) is achieved without channel prefixing (that is with $q = \boldsymbol{u}$), and the corresponding input $\boldsymbol{u}$ is Gaussian distributed.*

Proof. By using the result in [68, Theorem 3], we can state that the secrecy capacity of the MIMO Gaussian wiretap channel (4.2) under the generic matrix covariance constraint

$$\mathbf{0} \preceq \boldsymbol{K_u} \preceq \boldsymbol{S} \tag{4.6}$$

is obtained without channel prefixing and with Gaussian input $\boldsymbol{u}$, that is

$$\max_{p(q,\boldsymbol{u}):\boldsymbol{K_u}\preceq\boldsymbol{S}} [\mathbb{I}(q;\boldsymbol{v}) - \mathbb{I}(q;\boldsymbol{z})] = \max_{\substack{\boldsymbol{u}\sim\mathcal{CN}(\mathbf{0},\boldsymbol{K_u}) \\ \boldsymbol{K_u}\preceq\boldsymbol{S}}} [\mathbb{I}(\boldsymbol{u};\boldsymbol{v}) - \mathbb{I}(\boldsymbol{u};\boldsymbol{z})] \tag{4.7}$$

Then, we define the set

$$\mathcal{K}_P = \{\boldsymbol{K} : \mathrm{tr}(\boldsymbol{T}\boldsymbol{K}\boldsymbol{T}^*) \leq P\}\,. \tag{4.8}$$

and state the equality

$$\bigcup_{\boldsymbol{S}\in\mathcal{K}_P} \{\boldsymbol{K} : \mathbf{0} \preceq \boldsymbol{K} \preceq \boldsymbol{S}\} = \mathcal{K}_P. \tag{4.9}$$

To prove it, note that the inclusion $\bigcup_{\boldsymbol{S}\in\mathcal{K}_P} \{\boldsymbol{K} \preceq \boldsymbol{S}\} \supseteq \mathcal{K}_P$ is trivial. As regards the reverse, for any $\boldsymbol{K} \preceq \boldsymbol{S}$, with $\boldsymbol{S} \in \mathcal{K}_P$ we have

$$\mathrm{tr}(\boldsymbol{T}\boldsymbol{K_u}\boldsymbol{T}^*) \leq \mathrm{tr}(\boldsymbol{T}\boldsymbol{S}\boldsymbol{T}^*) \leq P\,, \tag{4.10}$$

that is $\boldsymbol{K} \in \mathcal{K}_P$.

Having proved (4.9) we can write

$$\begin{aligned}
C_{\mathsf{s}} &= \max_{p(q,\boldsymbol{u}):\boldsymbol{K_u}\in\mathcal{K}_P} [\mathbb{I}(q;\boldsymbol{v}) - \mathbb{I}(q;\boldsymbol{z})] && (4.11)\\
&= \max_{\boldsymbol{S}\in\mathcal{K}_P} \max_{p(q,\boldsymbol{u}):\boldsymbol{K_u}\preceq\boldsymbol{S}} [\mathbb{I}(q;\boldsymbol{v}) - \mathbb{I}(q;\boldsymbol{z})] && (4.12)\\
&= \max_{\boldsymbol{S}\in\mathcal{K}_P} \max_{\substack{\boldsymbol{u}\sim\mathcal{CN}(\mathbf{0},\boldsymbol{K_u}) \\ \boldsymbol{K_u}\preceq\boldsymbol{S}}} [\mathbb{I}(\boldsymbol{u};\boldsymbol{v}) - \mathbb{I}(\boldsymbol{u};\boldsymbol{z})] && (4.13)\\
&= \max_{\boldsymbol{K_u}\in\mathcal{K}_P} [\mathbb{I}(\boldsymbol{u};\boldsymbol{v}) - \mathbb{I}(\boldsymbol{u};\boldsymbol{z})]. && (4.14)
\end{aligned}$$

where we have used the set equality (4.9) in the first step, and (4.7) in the second step. This concludes the proof. □

From Lemma 1, we can write the secrecy capacity for the OFDM system with generic eavesdropper as

$$C_{\mathsf{s}} = \max_{\mathrm{tr}(\boldsymbol{K_x})\leq P} \left[\mathbb{I}(\boldsymbol{u};\boldsymbol{v}) - \mathbb{I}(\boldsymbol{u};\boldsymbol{z})\right] \tag{4.15}$$

$$= \max_{\mathrm{tr}(\boldsymbol{T}\boldsymbol{K_u}\boldsymbol{T}^*)\leq P} \left[\log \frac{|\boldsymbol{R}\boldsymbol{R}^* + \boldsymbol{H}_{\mathsf{R}}\boldsymbol{K_u}\boldsymbol{H}_{\mathsf{R}}^*|}{|\boldsymbol{R}\boldsymbol{R}^*|} - \log|\boldsymbol{I} + \boldsymbol{H}_{\mathsf{E}}\boldsymbol{K_u}\boldsymbol{H}_{\mathsf{E}}^*|\right]. \tag{4.16}$$

At this point, we still need to reformulate the maximization problem in a suitable way to apply the asymptotic result in the literature concerning the evaluation of the secrecy capacity under total power constraint. For the CP system (4.16) simplifies as $\boldsymbol{R}\boldsymbol{R}^* = \boldsymbol{I}_M$, while the input power constraint must be reformulated. From the observation of the transmission matrix (1.33) we notice that the trace constraint can be rewritten as

$$\mathrm{tr}(\boldsymbol{T}\boldsymbol{K_u}\boldsymbol{T}^*) = \mathrm{tr}(\boldsymbol{A}^*\boldsymbol{A}\boldsymbol{F}^*\boldsymbol{K_u}\boldsymbol{F}) = \mathrm{tr}(\boldsymbol{D}_{\mathsf{CP}}\boldsymbol{F}^*\boldsymbol{K_u}\boldsymbol{F}) \tag{4.17}$$

where

$$\boldsymbol{D}_{\mathsf{CP}} = \boldsymbol{A}^*\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{I}_{M-\mu} & \boldsymbol{0} \\ \hline \boldsymbol{0} & 2\boldsymbol{I}_{\mu} \end{array}\right]. \tag{4.18}$$

Then, given the invertible matrix $\boldsymbol{F}_{\mathsf{CP}} = \sqrt{\boldsymbol{D}_{\mathsf{CP}}}\boldsymbol{F}^*$, we have

$$\mathrm{tr}(\boldsymbol{T}\boldsymbol{K_u}\boldsymbol{T}^*) = \mathrm{tr}(\boldsymbol{F}_{\mathsf{CP}}\boldsymbol{K_u}\boldsymbol{F}_{\mathsf{CP}}^*). \tag{4.19}$$

On the other hand, for the ZS case it is easy to verify that $\mathrm{tr}(\boldsymbol{T}\boldsymbol{K_u}\boldsymbol{T}^*) = \mathrm{tr}(\boldsymbol{K_u})$, but the *overlap-and-add* structure of the receiver colors the noise such that its covariance matrix at the legitimate receiver is given by

$$\boldsymbol{K}_{\bar{\boldsymbol{w}}_{\mathsf{R}}} = \boldsymbol{R}\boldsymbol{R}^* = \boldsymbol{F}\boldsymbol{B}\boldsymbol{B}^*\boldsymbol{F}^* = \boldsymbol{F}\boldsymbol{D}_{\mathsf{ZS}}\boldsymbol{F}^* \tag{4.20}$$

where, similarly to the CP case, we have defined

$$\boldsymbol{D}_{\mathsf{ZS}} = \boldsymbol{B}\boldsymbol{B}^* = \left[\begin{array}{c|c} 2\boldsymbol{I}_{\mu} & \boldsymbol{0} \\ \hline \boldsymbol{0} & \boldsymbol{I}_{M-\mu} \end{array}\right]. \tag{4.21}$$

.

Hence, we can write the secrecy capacity of a DMT system with generic eavesdropper as

$$C_{\mathsf{s}} = \max_{\mathrm{tr}(\tilde{\boldsymbol{K}}_{\boldsymbol{u}})\leq P} \left[\log|\boldsymbol{I} + \tilde{\boldsymbol{H}}_{\mathsf{R}}\tilde{\boldsymbol{K}}_{\boldsymbol{u}}\tilde{\boldsymbol{H}}_{\mathsf{R}}^*| - \log|\boldsymbol{I} + \tilde{\boldsymbol{H}}_{\mathsf{E}}\tilde{\boldsymbol{K}}_{\boldsymbol{u}}\tilde{\boldsymbol{H}}_{\mathsf{E}}^*|\right] \tag{4.22}$$

where, for the CP system

$$\tilde{\boldsymbol{K}}_{\boldsymbol{u}} = \boldsymbol{F}_{\mathsf{CP}}\boldsymbol{K_u}\boldsymbol{F}_{\mathsf{CP}}^*\ ,\ \tilde{\boldsymbol{H}}_{\mathsf{R}} = \boldsymbol{H}_{\mathsf{R}}\boldsymbol{F}_{\mathsf{CP}}^{-1}\ ,\ \tilde{\boldsymbol{H}}_{\mathsf{E}} = \boldsymbol{H}_{\mathsf{E}}\boldsymbol{F}_{\mathsf{CP}}^{-1} \tag{4.23}$$

whereas, for ZS, with $\boldsymbol{F}_{\mathsf{ZS}} = \boldsymbol{F}\sqrt{\boldsymbol{D}_{\mathsf{ZS}}}$,

$$\tilde{\boldsymbol{K}}_{\boldsymbol{u}} = \boldsymbol{K}_{\boldsymbol{u}} \ , \ \tilde{\boldsymbol{H}}_{\mathsf{R}} = \boldsymbol{F}_{\mathsf{ZS}}^{-1}\boldsymbol{H}_{\mathsf{R}} \ , \ \tilde{\boldsymbol{H}}_{\mathsf{E}} = \boldsymbol{H}_{\mathsf{E}}. \tag{4.24}$$

It is well known, however, that the maximization problem in (4.22) is nonconvex [69], and a closed form solution in the presence of a total power constraint can only be computed for the high and low-SNR limits.

4.2 Secrecy capacity in the high-SNR regime

In this section we investigate the behavior of the secrecy capacity for the OFDM system and the fading channel when $P \to \infty$. Fading channels are assumed to be independent and fixed during the transmission of an entire packet. We denote the power delay profile by $\sigma^2_{\mathsf{R},\mathsf{n}} = \mathbb{E}\left\{|g_{\mathsf{R}}(n)|^2\right\}$ and $\sigma^2_{\mathsf{E},\mathsf{n}} = \mathbb{E}\left\{|g_{\mathsf{E}}(n)|^2\right\}$; thus, the average SNRs at the legitimate receiver and the eavesdropper are $\Lambda_{\mathsf{R}} = \frac{1}{M}\sum_{n=0}^{L_{\mathsf{R}}-1}\sigma^2_{\mathsf{R},\mathsf{n}}$ and $\Lambda_{\mathsf{E}} = \frac{1}{M}\sum_{n=0}^{L_{\mathsf{E}}-1}\sigma^2_{\mathsf{E},\mathsf{n}}$, respectively. The ratio between the average SNR on the main channel and that on the eavesdropper channel is denoted by $\Lambda_{\mathsf{RE}} = \Lambda_{\mathsf{R}}/\Lambda_{\mathsf{E}}$.

4.2.1 OFDM transmission with generic eavesdropper

In the following, we will apply to the OFDM case the approach described in [61] to calculate the high-SNR secrecy capacity of a MIMO Gaussian wiretap channel and we will compute the solution of the maximization problem in (4.22) when $P \to \infty$.

Lemma 2. *[61, Theorem 2] Let $\boldsymbol{H}_1 \in \mathbb{C}^{n_1\times m}$ and $\boldsymbol{H}_2 \in \mathbb{C}^{n_2\times m}$ with $n_1, n_2 \geq m$. Let $\boldsymbol{X} \in \mathbb{C}^{m\times m}$ be positive semidefinite. If $\mathrm{rank}(\boldsymbol{H}_2) = m$, the limit solution for $P \to \infty$, of the maximization problem*

$$C_{\mathsf{s}}(P) = \max_{\mathrm{tr}(\boldsymbol{X})\leq P}[\log|\boldsymbol{I} + \boldsymbol{H}_1\boldsymbol{X}\boldsymbol{H}_1^*| - \log|\boldsymbol{I} + \boldsymbol{H}_2\boldsymbol{X}\boldsymbol{H}_2^*|], \tag{4.25}$$

is given by

$$\lim_{P\to\infty} C_{\mathsf{s}}(P) = \sum_i [\log\sigma_i^2]^+, \tag{4.26}$$

where $\{\sigma_i\}$ are the generalized singular values of $(\boldsymbol{H}_1, \boldsymbol{H}_2)$.

By assuming that $g_{\mathsf{E}}(n)$ are continuous random variables it follows that $\mathrm{rank}(\tilde{\boldsymbol{H}}_{\mathsf{E}}) = M$ almost surely. Then the null space of $\tilde{\boldsymbol{H}}_{\mathsf{E}}$ is $\{\boldsymbol{0}\}$ and, from Lemma 2, the asymptotic secrecy capacity for high SNR is

$$\lim_{P\to\infty} C_{\mathsf{s}} = \sum_{i=1}^{M}\left[\log\sigma_i^2\right]^+ \tag{4.27}$$

where $\{\sigma_i\}$ are the generalized singular values of $\tilde{\boldsymbol{H}}_{\mathsf{R}}$ and $\tilde{\boldsymbol{H}}_{\mathsf{E}}$. In particular [61], the generalized singular value decomposition (GSVD) of $(\tilde{\boldsymbol{H}}_{\mathsf{R}}, \tilde{\boldsymbol{H}}_{\mathsf{E}})$ yields unitary $\boldsymbol{\Psi}_{\mathsf{R}}$ and $\boldsymbol{\Psi}_{\mathsf{E}}$, and a nonsingular $\boldsymbol{\Omega}$ such that

$$\boldsymbol{\Psi}_{\mathsf{R}}^{*}\tilde{\boldsymbol{H}}_{\mathsf{R}}\boldsymbol{\Omega} = \boldsymbol{D}_{\mathsf{R}},\ \boldsymbol{\Psi}_{\mathsf{E}}^{*}\tilde{\boldsymbol{H}}_{\mathsf{E}}\boldsymbol{\Omega} = \begin{bmatrix} \boldsymbol{D}_{\mathsf{E}} \\ \boldsymbol{0} \end{bmatrix}. \tag{4.28}$$

In (4.28), the diagonal matrices $\boldsymbol{D}_{\mathsf{R}} = \operatorname{diag}(d_{\mathrm{R}1}, \ldots, d_{\mathrm{R}M})$ and $\boldsymbol{D}_{\mathsf{E}} = \operatorname{diag}(d_{\mathrm{E}1}, \ldots, d_{\mathrm{E}M})$ contain the values that give the generalized singular values $\sigma_i = d_{\mathrm{R}i}/d_{\mathrm{E}i},\ i = 1, \ldots, M$, which we assume to be sorted in increasing order. Moreover, the generalized singular values turn out to be the standard singular values of the product $\tilde{\boldsymbol{H}}_{\mathsf{R}}\tilde{\boldsymbol{H}}_{\mathsf{E}}^{\dagger}$. Note that the squares of the nonzero singular values of $\tilde{\boldsymbol{H}}_{\mathsf{R}}\tilde{\boldsymbol{H}}_{\mathsf{E}}^{\dagger}$ are also the nonzero eigenvalues of $\tilde{\boldsymbol{H}}_{\mathsf{R}}(\tilde{\boldsymbol{H}}_{\mathsf{E}}^{*}\tilde{\boldsymbol{H}}_{\mathsf{E}})^{-1}\tilde{\boldsymbol{H}}_{\mathsf{R}}^{*}$.

4.2.2 Generic transmission and generic eavesdropper

In order to evaluate the high-SNR secrecy capacity provided by the frequency selective fading channel without imposing constraints on the modulation format, we apply the approach described in the previous paragraph directly on the MIMO channel

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{G}_{\mathsf{R}}\boldsymbol{x} + \boldsymbol{w}_{\mathsf{R}} \\ \text{and} \quad \boldsymbol{z} &= \boldsymbol{G}_{\mathsf{E}}\boldsymbol{x} + \boldsymbol{w}_{\mathsf{E}}. \end{aligned} \tag{4.29}$$

Like $\boldsymbol{H}_{\mathsf{E}}$ above, $\boldsymbol{G}_{\mathsf{E}}$ has full column rank (equal to N) almost surely, so the high-SNR secrecy capacity is determined by the eigenvalues of the matrix $\boldsymbol{G}_{\mathsf{R}}(\boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}})^{-1}\boldsymbol{G}_{\mathsf{R}}^{*}$, or equivalently of $\boldsymbol{C}_{\mathsf{R}}\boldsymbol{C}_{\mathsf{E}}^{-1}$, where $\boldsymbol{C}_{\mathsf{R}} = \boldsymbol{G}_{\mathsf{R}}^{*}\boldsymbol{G}_{\mathsf{R}}$ and $\boldsymbol{C}_{\mathsf{E}} = \boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}}$ are Hermitian and Toeplitz matrices. Similarly to $\boldsymbol{G}_{\mathsf{R}}$ and $\boldsymbol{G}_{\mathsf{E}}$, they represent the matrix equivalent of the convolution with the deterministic autocorrelations of the channel impulse responses $c_{\mathsf{R}}(n) = g_{\mathsf{R}} * g_{\mathsf{R},-}^{*}(n)$ and $c_{\mathsf{E}}(n) = g_{\mathsf{E}} * g_{\mathsf{E},-}^{*}(n)$, respectively.

Once we fix a channel model, with its bandwidth $F_0 = 1/T_0 = MF_{\mathsf{u}}$ and its lengths L_{R} and L_{E}, the sampling period and the length of the cyclic prefix (zero padding suffix) μ are determined. Then, we aim to investigate the limiting behavior of C_{s} for $N \to \infty$, that is when the number of samples in the transmitted symbol goes to infinity. In this way, we characterize the full potential of the frequency selective fading channel in transmitting secure messages regardless of the structure and complexity of the transceivers adopted by the legitimate users and the eavesdropper. We leverage on the asymptotic eigenvalue characterization of Toeplitz matrices to determine the limiting secrecy capacity of the system. By

letting $\boldsymbol{C}_N = \boldsymbol{C}_{\mathsf{R}}\boldsymbol{C}_{\mathsf{E}}^{-1}$ so that the dependency on N is explicitly indicated and noting that

$$|G_{\mathsf{R}}(f)|^2 = \sum_{n=-L_{\mathsf{R}}+1}^{L_{\mathsf{R}}-1} T_0\, c_{\mathsf{R}}(n) e^{-j2\pi f n T_0}, \tag{4.30}$$

(the same holds for the eavesdropper channel), we can use [70, Theorem 5.3] to write

$$\lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} [\log \lambda_i(\boldsymbol{C}_N)]^+ = \frac{1}{F_0} \int_{\mathcal{B}} \left[\log \frac{|G_{\mathsf{R}}(f)|^2}{|G_{\mathsf{E}}(f)|^2}\right]^+ df, \tag{4.31}$$

where $\mathcal{B} = (-\frac{F_0}{2}, \frac{F_0}{2})$. Comparing the integral in (4.31) with the high-SNR limit of the secrecy capacity (4.1) of parallel Gaussian channels, we observe that both the unconstrained and the OFDM eavesdropper scenarios converge to the same value of secrecy capacity. Moreover, it seems reasonable to assume that also for the case of OFDM transmission with generic eavesdropper the high-SNR secrecy capacity converges to (4.31) when $N \to \infty$ and the quantity μ is fixed, as the matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ can be approximated with increasing precision by identity matrices.

A further relationship between the secrecy performance of the dispersive channel can be derived by using the semi-blind masked MIMO approach [61]. In this case, the transmitter makes no use of information regarding the eavesdropper channel to distribute power across the antennas[1], and transmits power isotropically over the orthogonal complement of the kernel of the main channel matrix. In our scenario, since $\mathrm{rank}(\boldsymbol{G}_{\mathsf{R}}) = \mathrm{rank}(\boldsymbol{G}_{\mathsf{E}}) = N$ almost surely, this scheme translates to a simple uniform power allocation, and the high-SNR secrecy rate achieved by this method is given by, when $N \to \infty$,

$$R_\infty = \lim_{N\to\infty} \frac{1}{N} \left[\sum_{i=1}^{N} \log \lambda_i(\boldsymbol{C}_N)\right]^+ = \frac{1}{F_0} \left[\int_{\mathcal{B}} \log \frac{|G_{\mathsf{R}}(f)|^2}{|G_{\mathsf{E}}(f)|^2} df\right]^+. \tag{4.32}$$

Hence, the asymptotical secrecy rate obtained can be easily computed in terms of the power cepstra [71, Chapter 12] of the channel impulse responses

$$R_\infty = \left[\sqrt{\hat{g}_{\mathsf{R}}(0)} - \sqrt{\hat{g}_{\mathsf{E}}(0)}\right]^+, \tag{4.33}$$

where $\hat{g}$ denotes the power cepstrum of the signal $g(nT_0)$, i.e.,

$$\hat{g}(k) = \left| \int_{\mathcal{B}} \log |G(f)|^2\, e^{-j2\pi f k T_0} df \right|^2, \tag{4.34}$$

with

$$G(f) = \sum_n T_0 g(nT_0) e^{-j2\pi f n T_0}. \tag{4.35}$$

[1] However, the masked MIMO is a *semi-blind* approach, as the eavesdropper channel state information is used to determine the coding strategy.

Furthermore, the average rates obtained with the masked MIMO strategy when averaging over different channel realizations can be easily expressed in terms of the ratio between the SNRs in the legitimate and eavesdropper channels. Then, on denoting by $\tilde{g}_{\mathsf{R}}(n) = g_{\mathsf{R}}(n)/\sqrt{\Lambda_{\mathsf{R}}}$, $\tilde{g}_{\mathsf{E}}(n) = g_{\mathsf{E}}(n)/\sqrt{\Lambda_{\mathsf{E}}}$ the channel impulse responses normalized over the average SNR, and by $\tilde{G}_{\mathsf{R}}(f)$ and $\tilde{G}_{\mathsf{R}}(f)$ the corresponding normalized frequency responses, we can write

$$\mathbb{E}\left\{R_\infty\right\} = \mathbb{E}\left\{\left[\log\Lambda_{\mathsf{RE}} + \frac{1}{F_0}\int_{\mathcal{B}} \log\frac{|\tilde{G}_{\mathsf{R}}(f)|^2}{|\tilde{G}_{\mathsf{E}}(f)|^2} df\right]^+\right\}. \tag{4.36}$$

We observe that the average secrecy rate $\mathbb{E}\left\{R_\infty\right\}$ scales with $\log\Lambda_{\mathsf{RE}}$ when $\Lambda_{\mathsf{RE}} \to \infty$. In fact, a lower bound on the average secrecy rate is given by

$$\mathbb{E}\left\{R_\infty\right\} \geq \log\Lambda_{\mathsf{RE}} + \mathbb{E}\left\{\frac{1}{F_0}\int_{\mathcal{B}} \log\frac{|\tilde{G}_{\mathsf{R}}(f)|^2}{|\tilde{G}_{\mathsf{E}}(f)|^2} df\right\} = \log\Lambda_{\mathsf{RE}}, \tag{4.37}$$

where the last equality in (4.37) is due to the fact that $\tilde{G}_{\mathsf{R}}(f), \tilde{G}_{\mathsf{E}}(f)$ are independent and identically distributed (iid) random variables. On the other hand, the average secrecy rate is upper bounded by

$$\mathbb{E}\left\{R_\infty\right\} \leq \left[\log\Lambda_{\mathsf{RE}}\right]^+ + \mathbb{E}\left\{\left[\frac{1}{F_0}\int_{\mathcal{B}} \log\frac{|\tilde{G}_{\mathsf{R}}(f)|^2}{|\tilde{G}_{\mathsf{E}}(f)|^2} df\right]^+\right\}, \tag{4.38}$$

and hence we can write

$$\mathbb{E}\left\{R_\infty\right\} \asymp \log\Lambda_{\mathsf{RE}}, \tag{4.39}$$

as the second term in the right hand side of (4.38) does not increase with Λ_{RE}.

A similar observation can be made to evaluate the asymptotic values of the average secrecy capacity as $\Lambda_{\mathsf{RE}} \to \infty$. It can then be shown that the average secrecy capacity for the generic transmission case, measured in bit/s/Hz, is asymptotic to

$$\mathbb{E}\left\{C_{\mathsf{s}}\right\} \asymp N\log\Lambda_{\mathsf{RE}} \quad , \quad \text{as } \Lambda_{\mathsf{RE}} \to \infty\,. \tag{4.40}$$

while for both the OFDM and the parallel channels case,

$$\mathbb{E}\left\{C_{\mathsf{s}}\right\} \asymp M\log\Lambda_{\mathsf{RE}} \quad , \quad \text{as } \Lambda_{\mathsf{RE}} \to \infty\,. \tag{4.41}$$

4.2.3 Numerical results

In this section we present numerical results illustrating the high-SNR secrecy capacity of CP and ZS transmissions over fading channels. We give results for Rayleigh fading channels with an exponential power delay profile.

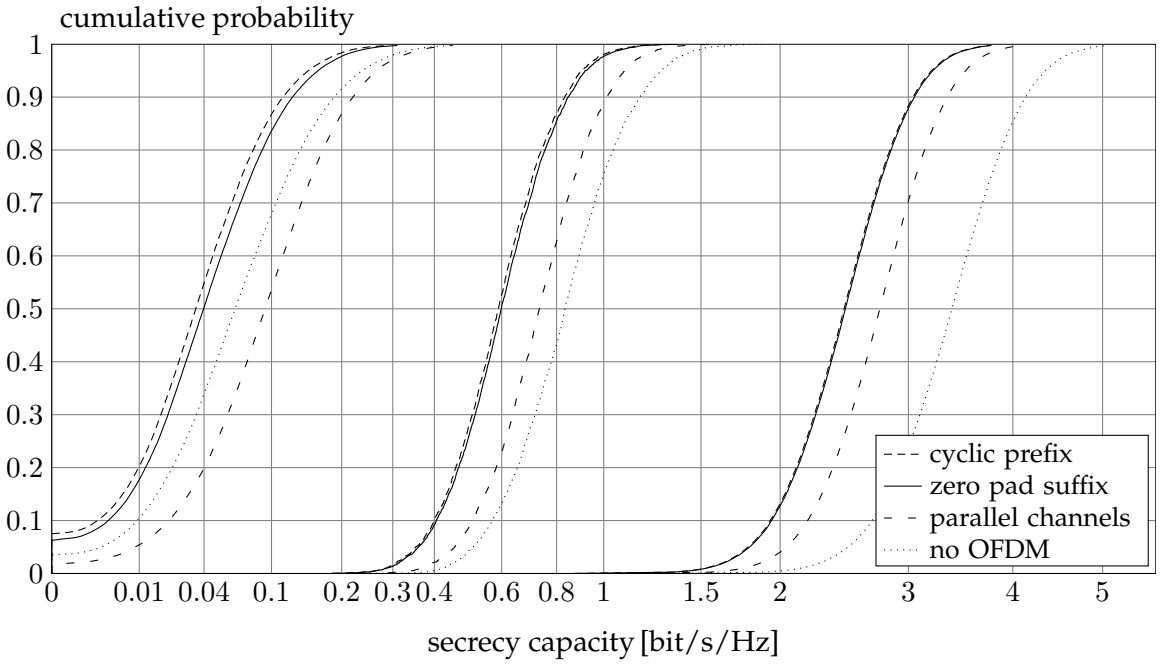

Figure 4.1. *Cumulative distribution functions of the high SNR secrecy capacity for different ratios between the SNRs in the legitimate channel and the eavesdropper channel,* $\Lambda_{\mathsf{RE}} = -10, 0, 10$ *dB. Results are plotted for the parameters* $M = 64$ *and* $N = 80$*.*

In Figure 4.1 we show the cumulative distribution function (CDF) of the secrecy capacity achieved over an OFDM system with $M = 64$ subcarriers, length of the cyclic prefix (zero-padding suffix) $\mu = 16$ and channel delay spreads $L_{\mathsf{R}} = L_{\mathsf{E}} = \mu = 16$. Here we can easily notice that the assumption of an OFDM demodulator at the eavesdropper can lead to optimistically incorrect performance predictions. In fact, the wiretapper can take significant advantage of the information leaked by the cyclic prefix. On the other hand, the ZS and CP schemes yield nearly equivalent results in terms of secrecy capacity. Also, we notice that the loss in secrecy capacity caused by the adoption of OFDM modulation with respect to the general transmitter case is higher than the redundancy $\rho = \mu/M$ introduced by the transmitter.

It is interesting to note that, when the legitimate receiver experiences better channel conditions (that is $\Lambda_{\mathsf{RE}} = 10\,\mathrm{dB}$), the highest secrecy capacity is achieved by the fading channel itself without constraints. On the other hand, the results obtained with $\Lambda_{\mathsf{RE}} = -10\,\mathrm{dB}$ show that in the reverse condition, the parallel channels setup allows higher secrecy rates. This fact can be easily explained by observing that imposing the OFDM structure on both the legitimate receiver and the eavesdropper has a worse impact on the user with better channel

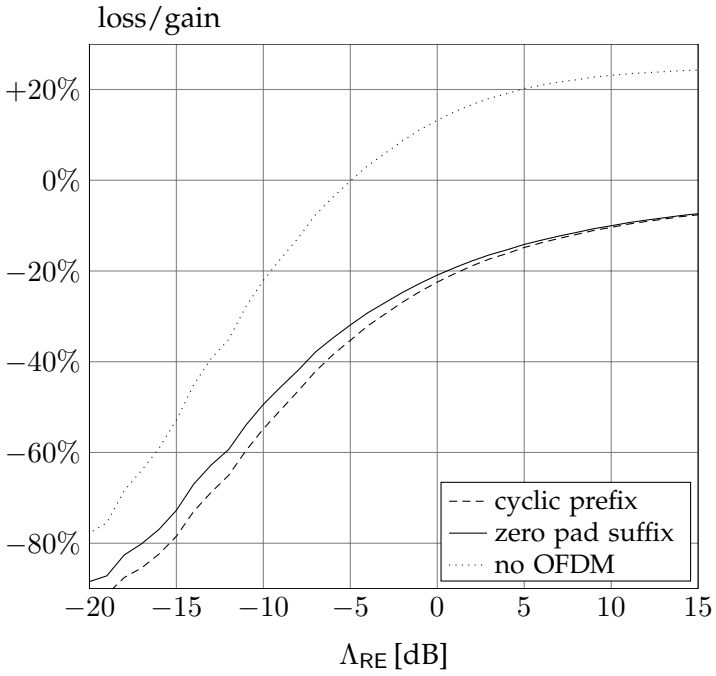

Figure 4.2. *Percentage loss of the average high SNR secrecy capacity with respect to the parallel channels scenario as a function of the ratios between the SNRs in the main and eavesdropper channel.*

conditions.

This observation is also clearly visualized in Figure 4.2 with the representation of the average high SNR secrecy capacity percentage loss with respect to the parallel channels scenario for different values of the SNR ratio. As expected, when the receiver starts to enjoy a better SNR compared to the eavesdropper, the curve for the fading channel case crosses the zero. Moreover, we are able to observe the loss incurred with respect to the previously analyzed setups when we consider a DMT transmission overheard by a more sophisticated adversary. In particular, when the channel conditions for the legitimate receiver and the eavesdropper are the same ($\Lambda_{\mathsf{RE}} = 0\,\text{dB}$), the loss on the average capacity is about 20 %. On the other hand, when the eavesdropper has a clear SNR advantage over the main channel, the loss increases dramatically and the use of a more capable receiver can drop the secrecy capacity down by 90 % with respect to the result obtained in the parallel channels assumption. Notice that as $\Lambda_{\mathsf{RE}} \to \infty$, the gain of the generic transmission case with respect to the parallel channels setup attains the value of ρ, as can be derived from the equations in (4.40) and (4.41). Similarly the percentage loss in the generic eavesdropper case vanishes, as the absolute loss approaches a constant value while C_{s} increases logarithmically with Λ_{RE}.

We now focus our attention on how design parameters affect the secrecy capacity of

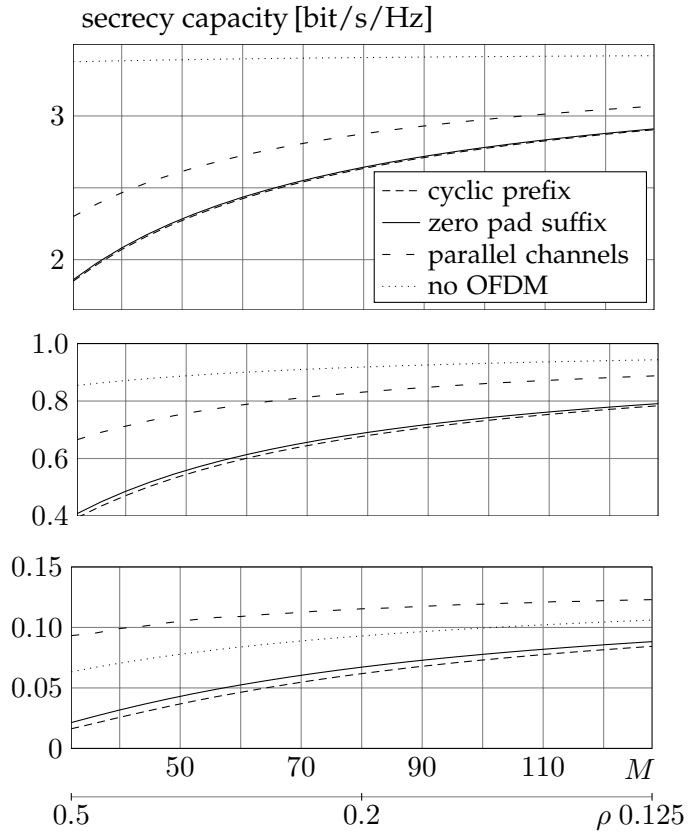

Figure 4.3. *High SNR secrecy capacity versus number of subcarriers for different SNR ratios between the legitimate receiver and the eavesdropper,* $\Lambda_{\mathsf{RE}} = -10, 0, 10\,dB$*. The quantity* $\rho = \mu/M$ *represents the spectral redundancy of the system.*

OFDM systems. As explained in Section 4.2, we consider F_0 and μ fixed and evaluate the results obtained for different values of the symbol length N, or equivalently for different values of the number of OFDM subcarriers M. We want to determine whether there is a trade off between augmenting the legitimate receiver capacity and leaking of information towards the eavesdropper. As depicted in Figure 4.3, we see that the secrecy capacity of the system increases monotonically with M. Thus, our results show that it is desirable to increase the number of subcarriers of DMT systems even under an information-theoretic security point of view. Moreover, the comparison with the secrecy capacity obtained with parallel Gaussian channels shows how the information the eavesdropper can gain from the observation of the cyclic prefix or the symbol dispersion in the padding suffix is relevant even when the prefix/suffix covers only a small fraction of the OFDM symbol.

4.3 Probability of a positive secrecy capacity

In this section we characterize the probability that according to the channel model introduced at the beginning of Section 4.2 the pair of fading channels $g_{\mathsf{R}}(\cdot), g_{\mathsf{E}}(\cdot)$ offers a nonzero secrecy capacity.

4.3.1 Parallel channels

First, we consider the case in which legitimate users and eavesdropper deploy OFDM transceivers. Given the formulation of the secrecy capacity in (4.1), the probability of nonzero secrecy capacity is the probability that the main channel has higher amplitude than the eavesdropper at some subcarrier frequency:

$$P[C_{\mathsf{s}} > 0] = P\left[\bigcup_{i=1}^{M} \{|G_{\mathsf{R}}(f_i)| > |G_{\mathsf{E}}(f_i)|\}\right]. \tag{4.42}$$

Since the channel delay spread is assumed to be much shorter than the useful symbol length, the M subcarrier complex gains are correlated even in the case in which the L_{R} (or L_{E}) time domain channel taps are statistically independent. However, the above probability can be approximately estimated by neglecting the gain correlation, as

$$P[C_{\mathsf{s}} > 0] = 1 - P\left[\bigcap_{i=1}^{M} \{|G_{\mathsf{R}}(f_i)| \leq |G_{\mathsf{E}}(f_i)|\}\right] \tag{4.43}$$

$$\simeq 1 - \prod_{i=1}^{M} P[|G_{\mathsf{R}}(f_i)| \leq |G_{\mathsf{E}}(f_i)|]. \tag{4.44}$$

If we assume that both channels have independent taps with Rayleigh fading, then $|G_{\mathsf{R}}(f_i)|^2$ and $|G_{\mathsf{E}}(f_i)|^2$ are two independent random variables exponentially distributed with means $\Lambda_{\mathsf{R}} = \frac{1}{M}\sum_{n=0}^{L_{\mathsf{R}}-1} \sigma^2_{\mathsf{R},\mathsf{n}}$ and $\Lambda_{\mathsf{E}} = \frac{1}{M}\sum_{n=0}^{L_{\mathsf{E}}-1} \sigma^2_{\mathsf{E},\mathsf{n}}$ respectively, and the approximation is obtained from the outage probability in [72] as

$$P[C_{\mathsf{s}} > 0] \simeq 1 - \left(\frac{1}{1+\Lambda_{\mathsf{RE}}}\right)^M \tag{4.45}$$

in which we recall that $\Lambda_{\mathsf{RE}} = \Lambda_{\mathsf{R}}/\Lambda_{\mathsf{E}}$ is the ratio between the SNRs at the legitimate receiver and that at the eavesdropper.

Even without assuming independence among the subcarrier gains, we can write the asymptotic probability of nonzero secrecy capacity for infinite length of the transmitted symbols as

$$\lim_{N\to\infty} P[C_{\mathsf{s}} > 0] = P\left[\exists f \in \mathcal{B} : |G_{\mathsf{R}}(f)| \geq |G_{\mathsf{E}}(f)|\right] \tag{4.46}$$

$$= 1 - P[|G_{\mathsf{E}}(f)|^2 - |G_{\mathsf{R}}(f)|^2 \geq 0,\ \forall f \in \mathcal{B}]. \tag{4.47}$$

The last term in (4.47) suggests an effective criterion to link the secrecy outage probability with the time domain expression of the channel. Namely, from Bochner's theorem [73] we can state that the asymptotic probability of nonzero secrecy capacity is equal to the probability that the function $c_{\mathsf{E}}(n) - c_{\mathsf{R}}(n)$ is not positive semidefinite.

4.3.2 Generic transmission and generic eavesdropper

In order to derive the probability of positive secrecy capacity for the scenarios of unconstrained modulation format, we can leverage again the results on the secrecy capacity for a MIMO Gaussian wiretap channel. First, we recall that for a MIMO Gaussian wiretap channel it holds that [61, Claim 1]

$$\lim_{P\to\infty} C_{\mathsf{s}} > 0 \quad \Leftrightarrow \quad C_{\mathsf{s}} > 0, \ \forall P > 0. \tag{4.48}$$

Hence, the outage probability can be determined by limiting the analysis to the high-SNR regime. In particular, it depends on the largest eigenvalue of $\boldsymbol{C}_{\mathsf{R}}\boldsymbol{C}_{\mathsf{E}}^{-1}$, as

$$P[C_{\mathsf{s}} > 0] = P[\lambda_{\max}(\boldsymbol{C}_{\mathsf{N}}) > 1]. \tag{4.49}$$

Its value does not depend on the individual SNRs of the main and eavesdropper channels, but it is in fact a function of their ratio. In this case, it is also possible to characterize the asymptotic probability of positive secrecy capacity for $N \to \infty$. Then, by applying [70, Corollary 4.2 and Theorem 5.3] we can state that

$$\lim_{N\to\infty} \lambda_{\max}(\boldsymbol{C}_{\mathsf{N}}) = \max_{f\in(-F_0/2,F_0/2)} |G_{\mathsf{R}}(f)|^2/|G_{\mathsf{E}}(f)|^2; \tag{4.50}$$

thus, for the unconstrained case, the asymptotic probability of nonzero secrecy capacity is given again by (4.47).

4.3.3 OFDM transmission with generic eavesdropper

For this case we can repeat the same analysis as above. The high-SNR regime analysis of the achievable rates for the OFDM system with generic eavesdropper provides us with a physical interpretation of the probability of having nonzero secrecy capacity in this scenario. For the ease of analytical tractability, when considering the zero-padding system we neglect the effects of the noise correlation at the receiver output. Moreover, we notice that, for the CP case it holds that

$$\tilde{\boldsymbol{H}}_{\mathsf{R}}(\tilde{\boldsymbol{H}}_{\mathsf{E}}^{*}\tilde{\boldsymbol{H}}_{\mathsf{E}})^{-1}\tilde{\boldsymbol{H}}_{\mathsf{R}}^{*} = \boldsymbol{H}_{\mathsf{R}}(\boldsymbol{H}_{\mathsf{E}}^{*}\boldsymbol{H}_{\mathsf{E}})^{-1}\boldsymbol{H}_{\mathsf{R}}^{*}. \tag{4.51}$$

Thus, we can address the secrecy capacity starting from the definition of the channels $\boldsymbol{H}_{\mathsf{R}}$ and $\boldsymbol{H}_{\mathsf{E}}$. In particular, from the expression of the high-SNR secrecy capacity in terms of the generalized singular values of the couple $(\boldsymbol{H}_{\mathsf{R}}, \boldsymbol{H}_{\mathsf{E}})$ we have that the secrecy capacity of the system is zero if and only if the maximum generalized singular value is less than 1; that is [61]

$$\sigma^2_{\max}(\boldsymbol{H}_{\mathsf{R}}\boldsymbol{H}_{\mathsf{E}}^{\dagger}) = \sup_{\boldsymbol{u}\in\mathbb{C}^M} \frac{\|\boldsymbol{H}_{\mathsf{R}}\boldsymbol{u}\|^2}{\|\boldsymbol{H}_{\mathsf{E}}\boldsymbol{u}\|^2} \leq 1. \tag{4.52}$$

Since the channel is shorter than the CP (ZS), the norm in the numerator can be written as

$$\|\boldsymbol{H}_{\mathsf{R}}\boldsymbol{u}\|^2 = \sum_{i=1}^{M} |G_{\mathsf{R}}(f_i)|^2 |u_i|^2 \tag{4.53}$$

whereas the denominator represents the energy of the output of the eveasdropper channel when the M subcarriers are loaded with the symbols in the vector $\boldsymbol{u}$. Thus, by Parseval's relation we can express that energy as

$$\|\boldsymbol{H}_{\mathsf{E}}\boldsymbol{u}\|^2 = \int_{\mathcal{B}} \left| \sum_{i=1}^{M} u_i \Gamma_0(f - f_i) G_{\mathsf{E}}(f) \right|^2 df \tag{4.54}$$

where $\Gamma_0(f - f_i)$ is the frequency response of the i-th subcarrier transmission filter that appears in (1.3) for CP systems and in (1.5) for ZS. The expression in (4.54) tells us that the probability of nonzero secrecy capacity is closely related to the probability that there exists at least one index i for which

$$|G_{\mathsf{R}}(f_i)|^2 > \int_{\mathcal{B}} |\Gamma_0(f - f_i)|^2 |G_{\mathsf{E}}(f)|^2 df. \tag{4.55}$$

From (4.55) we can deduce a practical interpretation of the advantage of a general eavesdropper compared to one equipped with an OFDM receiver. The information carried on the i-th subcarrier is spread over the spectrum of the eavesdropper channel and the information leakage is proportional to the shape of the corresponding transmission filter, namely a $\mathrm{sinc}(\cdot)$ waveform centered over the subcarrier central frequency. Thus, even if the eavesdropper channel frequency response is lower than that of the legitimate receiver at all the subcarrier central frequencies, the adversary can nevertheless take advantage of the information spread over all the subchannels to reduce the secrecy capacity.

4.3.4 Numerical results

We consider again OFDM systems deploying $M = 64$ subcarriers, with CP length $\mu = 16$. The transmission takes place over Rayleigh fading channels with exponential power delay profiles and delay spread $L_{\mathsf{R}} = L_{\mathsf{E}} = \mu$.

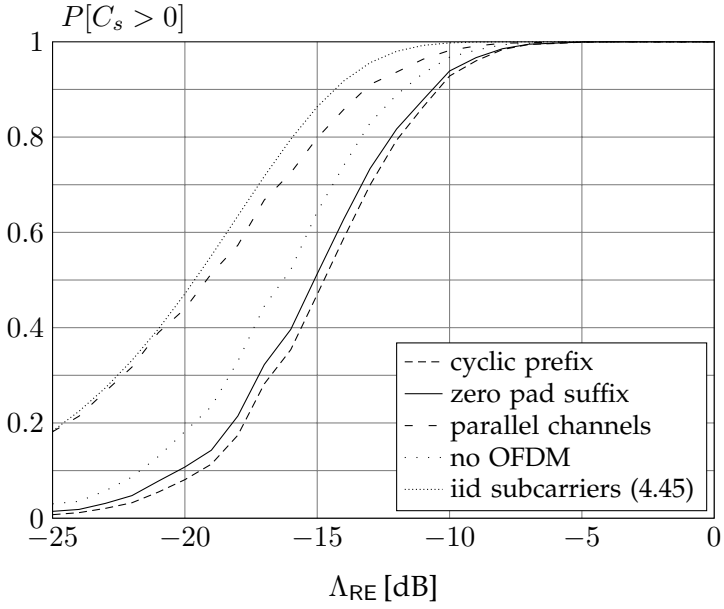

Figure 4.4. *Probability of nonzero secrecy capacity as a function of the ratio between the SNRs in the main channel and the eavesdropper channel. Results are given for the three modulation scenarios analyzed in this chapter and using the statistically independent subcarriers approximation.*

The probabilities of positive secrecy capacity for the SNR range favorable to the eavesdropper are reported in Figure 4.4. The small gap between the channel curve and the DMT results shows that the adoption of OFDM modulation for the transmission represents an insurmountable barrier for secret communications only for a small fraction of the channel realizations. On the other hand, the parallel channels scenario achieves higher probabilities due to the detrimental effects of modulation constraints over the physical advantage of the eavesdropper. In this scenario, the analytical result obtained under the approximation of statistically independent subcarriers in (4.45) represents a tight upper bound especially when the main channel has a much lower SNR than the eavesdropper, and the single events $\{|G_{\mathsf{R}}(f_i)| > |G_{\mathsf{E}}(f_i)|\}$ become less and less probable.

Nevertheless, it is interesting to note that, despite its widespread use in the literature [56], the independent carriers assumption turns out to be misleading in evaluating the asymptotic probability of positive secrecy capacity of the parallel channels setup even as $N \to \infty$. The probabilities in Figure 4.5 are computed for transmissions over Rayleigh fading channels of length $L_{\mathsf{R}} = L_{\mathsf{E}} = \mu = 8$ with $\Lambda_{\mathsf{RE}} = -10$ dB. The approximation in (4.45) always approaches 1 when $N \gg \max\{L_{\mathsf{R}}, L_{\mathsf{E}}\}$ regardless of the actual values of Λ_{RE} and the channel impulse responses. On the other hand, the correlation among subcarriers is shown

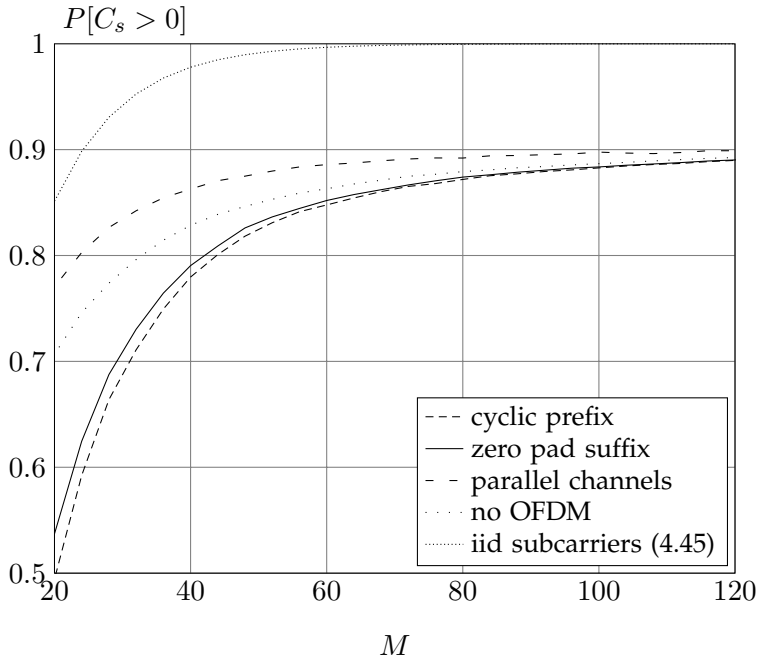

Figure 4.5. *Probability of nonzero secrecy capacity versus number of subcarriers M. Numerical results are given for the three modulation scenarios analyzed in this paper and using the statistically independent subcarriers approximation obtained for SNR ratio $\Lambda_{\mathsf{RE}} = -10\,dB$.*

to limit the available diversity at the transmitter even when the number of subchannels increases. As a consequence of the argument in Section 4.3.1, the asymptotic probability of nonzero secrecy capacity over frequency selective channels is determined by the difference in the channel autocorrelations and may be bounded away from 1.

4.4 Secrecy capacity derivative in the low-SNR regime

Analogously to the investigation for the high-SNR secrecy capacity, we are now able to use the expressions for the equivalent channels $\tilde{\boldsymbol{H}}_{\mathsf{R}}$ and $\tilde{\boldsymbol{H}}_{\mathsf{E}}$ for both CP and ZS systems to gain insight into the behavior of the secrecy capacity in the low-SNR regime, i.e. for $P \to 0$. In particular, we can use the result in [62] and claim that the first derivative of the secrecy capacity for $P = 0$ is proportional to the maximal eigenvalue of the pencil $\boldsymbol{\Phi} = \tilde{\boldsymbol{H}}_{\mathsf{R}}^{*}\tilde{\boldsymbol{H}}_{\mathsf{R}} - \tilde{\boldsymbol{H}}_{\mathsf{E}}^{*}\tilde{\boldsymbol{H}}_{\mathsf{E}}$. Namely,

$$\dot{C}_{\mathsf{s}}|_{P=0} = \frac{1}{(1+\rho)\ln 2}\left[\lambda_{\max}(\boldsymbol{\Phi})\right]^{+}. \tag{4.56}$$

The same can be stated for the generic transmission case with $\boldsymbol{G}_{\mathsf{R}}, \boldsymbol{G}_{\mathsf{E}}$ replacing $\tilde{\boldsymbol{H}}_{\mathsf{R}}, \tilde{\boldsymbol{H}}_{\mathsf{E}}$ respectively.

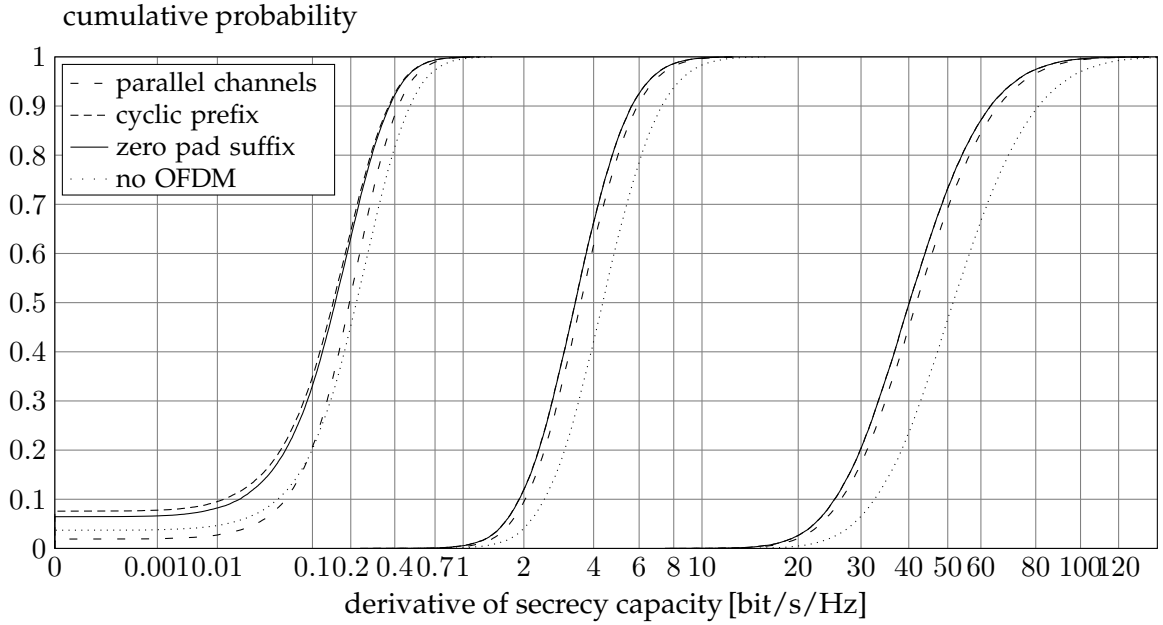

Figure 4.6. *Cumulative distribution function of the first derivative of the secrecy capacity for different ratios between the SNRs in the legitimate channel and the eavesdropper channel,* $\Lambda_{\mathsf{RE}} = -10, 0, 10\,dB$. *The curves for CP and ZS overlap, whereas slight differences can be observed among the two OFDM implementations and the parallel channels assumption.*

In Figure 4.6 we show the CDF of the first derivative of the low-SNR secrecy capacity for the CP and the ZS systems. The results are almost coincident, and moreover, the slope of the secrecy capacity is also very close to that obtained when considering the parallel Gaussian wiretap channels in which also the eavesdropper adopts OFDM demodulation. Instead, there is an appreciable loss with respect to the generic modulation case.

4.5 Achievable secrecy rates

The secrecy capacity for a MIMO Gaussian wiretap channel lacks complete characterization with a finite total power trace constraint. However, we can focus on the secrecy rates that are achievable with particular input strategies. We consider three possible strategies in the following three subsections.

4.5.1 Optimal input for high SNR

First we consider the performance obtained with the Gaussian input that achieves the secrecy capacity at high SNR. Recall that the secrecy capacity was established in Section 4.2.1,

starting form the GSVD of $(\tilde{\boldsymbol{H}}_{\mathsf{R}}, \tilde{\boldsymbol{H}}_{\mathsf{E}})$. The corresponding input covariance is given by [69]

$$\tilde{\boldsymbol{K}}_{\boldsymbol{u}} = \zeta P \boldsymbol{\Omega}_{\xi} \boldsymbol{\Omega}_{\xi}^{*} \tag{4.57}$$

where $\boldsymbol{\Omega}_{\xi}$ gathers the last ξ columns of $\boldsymbol{\Omega}$ in the GSVD (4.28), and ξ is the number of generalized singular values that are greater than one. In (4.57), $\zeta = 1/\mathrm{tr}(\boldsymbol{\Omega}_{\xi}\boldsymbol{\Omega}_{\xi}^{*})$ is set in order to satisfy the trace constraint. Although optimal asymptotically, this scheme gives, in general suboptimal results for finite SNR, and it is interesting to investigate how it behaves for low SNR compared to other allocations.

4.5.2 Water-filling solution

Next, we evaluate the results provided by the power allocation scheme of [63]. Its derivation is based on the assumption that the eavesdropper implements OFDM demodulation, and hence the entire system can be regarded as the parallel of M Gaussian wiretap channels. For this scenario, independent coding across the channels is known to reach the secrecy capacity [56], and hence the optimal input covariance matrix $\boldsymbol{K}_{\boldsymbol{u}}$ is diagonal. This fact turns out to be useful in handling the total power trace constraint for the CP system. In fact, since $\boldsymbol{K}_{\boldsymbol{u}} = \mathrm{diag}(P_1, \ldots, P_M)$ is diagonal, the matrix $\boldsymbol{F}^{*}\boldsymbol{K}_{\boldsymbol{u}}\boldsymbol{F}$ is circulant and its diagonal elements are equal to $\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{u}})/M$. Thus, the total power constraint can be easily expressed as

$$\mathrm{tr}(\boldsymbol{T}\boldsymbol{K}_{\boldsymbol{u}}\boldsymbol{T}^{*}) = \mathrm{tr}(\boldsymbol{A}\boldsymbol{F}^{*}\boldsymbol{K}_{\boldsymbol{u}}\boldsymbol{F}\boldsymbol{A}^{*}) = (M - \mu + 2\mu)\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{u}})/M = (1+\rho)\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{u}}) \tag{4.58}$$

with $\rho = \mu/M$ representing the spectral redundancy of the system. For the sake of a compact notation, we define $a_i = 1/|G_{\mathsf{E}}(f_i)|^2 - 1/|G_{\mathsf{R}}(f_i)|^2$ and $b_i = 1/|G_{\mathsf{E}}(f_i)|^2 + 1/|G_{\mathsf{R}}(f_i)|^2$. Thus, the optimal power allocation for parallel Gaussian channels is a water-filling type solution [63] for which $P_i^{*} = 0$ when $|G_{\mathsf{R}}(f_i)| \leq |G_{\mathsf{E}}(f_i)|$, otherwise

$$P_i^{*} = \left[\sqrt{\frac{a_i^2}{4} + \frac{a_i}{\nu}} - \frac{b_i}{2}\right]^{+} \tag{4.59}$$

with $\nu > 0$ such that

$$\sum_{i=1}^{M} P_i^{*} = P'. \tag{4.60}$$

We observe that, in order to fulfil the time-domain power constraint we have to impose $P' = P/(1+\rho)$ for the CP system, whereas $P' = P$ when zero-padding suffix transmission is adopted. Here, we address the problem of evaluating the loss caused by the fact that in our scenario the eavesdropper can decide the best decoding strategy to retrieve the secret message from the entire received signal. Moreover we look for a different power allocation scheme that can suit this scenario.

4.5.3 Optimal power allocation with independent inputs

Finally we propose an optimal power allocation method. The idea is to restrict the search for the maximum in (4.16) to diagonal input covariance matrices $\boldsymbol{K_u}$, and hence obtain a lower complexity, close to that of the algorithm in [63]. Nevertheless, the difference with respect to the water-filling solution is that here we consider the worst case and maximize the secrecy rate without imposing restrictions on the eavesdropper. Namely, we choose the M input powers on the subcarriers in order to maximize the difference between mutual information at the legitimate receiver and eavesdropper, $\mathbb{I}(\boldsymbol{u};\boldsymbol{v}) - \mathbb{I}(\boldsymbol{u};\boldsymbol{z})$, under the constraint that $\mathrm{tr}(\boldsymbol{K_x}) \leq P$. Then, if we denote the set of diagonal covariance matrices that satisfy the trace constraint as

$$\mathcal{K}'_P = \left\{ \boldsymbol{K} = \mathrm{diag}(P_1, \ldots, P_M) : P_i \geq 0, \sum_{i=1}^{M} P_i \leq P \right\}, \tag{4.61}$$

from (4.58), we can write the optimal power allocation for the CP system as

$$R_{\mathsf{s}}^{\mathrm{cp}} = \max_{\boldsymbol{K_u} \in \mathcal{K}'_{P'}} \left[\log |\boldsymbol{I} + \boldsymbol{H}_{\mathsf{R}} \boldsymbol{K_u} \boldsymbol{H}_{\mathsf{R}}^*| - \log |\boldsymbol{I} + \boldsymbol{H}_{\mathsf{E}} \boldsymbol{K_u} \boldsymbol{H}_{\mathsf{E}}^*| \right]. \tag{4.62}$$

Analogously, the achievable rate for ZS transmission can be expressed as

$$R_{\mathsf{s}}^{\mathrm{zp}} = \max_{\boldsymbol{K_u} \in \mathcal{K}'_P} \left[\log |\boldsymbol{I} + \tilde{\boldsymbol{H}}_{\mathsf{R}} \boldsymbol{K_u} \tilde{\boldsymbol{H}}_{\mathsf{R}}^*| - \log |\boldsymbol{I} + \boldsymbol{H}_{\mathsf{E}} \boldsymbol{K_u} \boldsymbol{H}_{\mathsf{E}}^*| \right] \tag{4.63}$$

where $\tilde{\boldsymbol{H}}_{\mathsf{R}} = \boldsymbol{F}_{\mathsf{ZS}}^{-1} \boldsymbol{H}_{\mathsf{R}}$ takes into account also the effects of the correlated noise at the receiver output.

4.5.4 Numerical results

In this section, we describe the results of simulations that compare these three different approaches and measure how the introduction of the OFDM modulation affects the secrecy characteristics of the inner frequency selective channel. We consider a ZS system with $M = 64$ subcarriers and $\rho = 1/4$. The legitimate receiver and eavesdropper listen to the outputs of two different Rayleigh fading channels of lengths $L_{\mathsf{R}} = L_{\mathsf{E}} = \mu = 16$ with exponentially decaying power delay profiles. The legitimate and eavesdropper channel are given with the same statistical description in order to represent a scenario in which neither the receiver nor the adversary can exploit a clear advantage in terms of channel conditions. The optimal power allocations are derived via numerical solution of the maximization problems in (4.62) and (4.63).

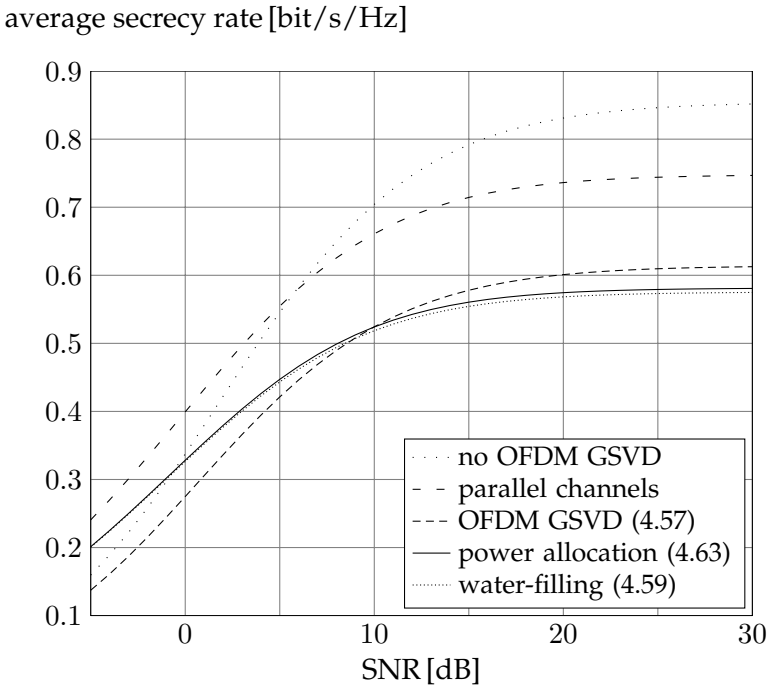

Figure 4.7. *Average secrecy rates achieved by the three different strategies in Section 4.5 for ZS and performance of the inner channel and the parallel channels assumption.*

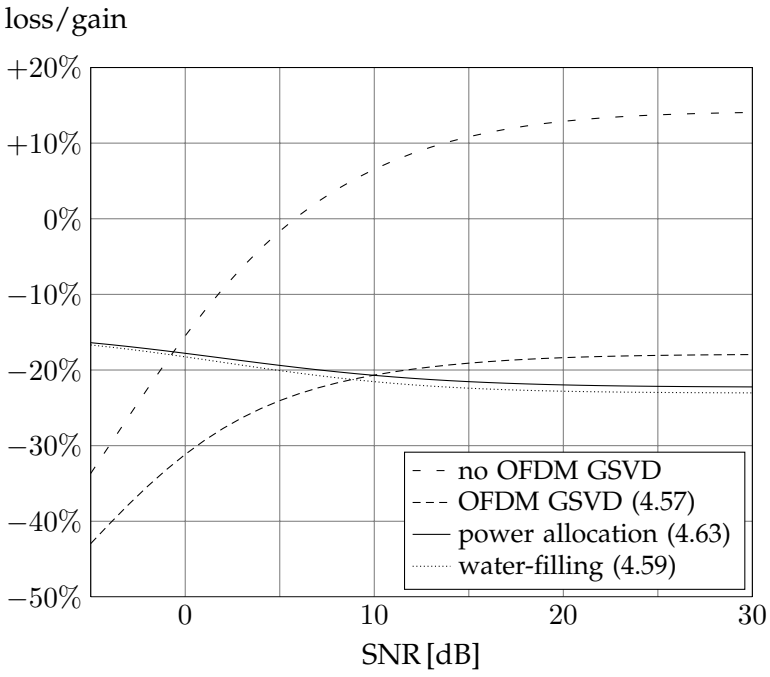

Figure 4.8. *Percentage loss of the average secrecy rates achieved by the three different strategies in Section 4.5 with respect to the parallel channel scenario.*

In Figure 4.7 the average secrecy rates achieved by the different methods are shown. The results were averaged over 4000 channels realizations. We can see that, when no constraints are imposed on the eavesdropper receiver architecture, the performance obtained by the water-filling allocation (4.59) are degraded with respect to the corresponding result in [63] for the OFDM eavesdropper. In particular, as shown in Figure 4.8, the loss is about the 20 % and it is almost constant for different SNR values. This factor appears to be closely related to the spectral redundancy ρ introduced by the OFDM structure. On the other hand, the GSVD, although proven to be optimal in the high-SNR limit, provides lower secrecy rates than the other schemes at low SNR.

Although the optimal power allocation (4.63) shows only a very slight improvement with respect to (4.59) when the average secrecy rate is taken as the performance metric, the proposed method can guarantee appreciable improvement.

Chapter 5

Secret-key agreement over MIMO channels

Secret-key agreement over wireless channels is perhaps one of the most promising applications of physical-layer security because the noise, interference and fading affecting wireless communications provide a convenient source of randomness. The objective of secret-key agreement strategies is to design methods to extract secrecy from the noise itself, in the form of a secret key. More specifically, the legitimate parties and the eavesdropper are assumed to observe the realizations of correlated random variables and the legitimate parties attempt to agree on a secret-key oblivious to the eavesdropper. A remarkable difference between this scenario and the wiretap channel model is that the legitimate terminals can distill their key by communicating over a *two-way*, *public*, *noiseless* and *authenticated* channel at no cost. The fundamental information-theoretic limits of secret-key agreement by public discussion from common randomness were first investigated by Ahslwede and Csiszár [14] and Maurer [15]. More recently, alternative bounds have been presented in [74, 75]. We are interested in the problem of secret-key agreement under the *channel model* description [14], that is, we assume that the source of common randomness can be driven by one of the legitimate terminals. In other words, the legitimate transmitter broadcasts over the wireless medium the randomness from which the secret-key will be distilled.

The ability to harness this randomness and to distill secret keys depends heavily on the statistical model of fading, the knowledge of channel state information, and the identification of the optimal signaling strategy. Then, the problem of secret-key agreement over Gaussian channel was investigated in [76–78]. On the other hand, for ergodic wireless chan-

nels, in which the fading realization changes randomly at every channel use, [79] shows that instantaneous channel state information is not required because the fading process can be treated as part of the source randomness; [79] also provides the secret-key capacity of MIMO channels but does not characterize the optimal signaling strategy explicitly. For quasi-static wireless channels, in which the fading realization changes independently and randomly from one block to another, secret-key capacity is zero without channel state information. Nevertheless, under the assumption of full channel state information (CSI), [80] proposes practical key-distillation strategies for single-input single-output systems.

In this thesis, we are interested in evaluating the performance of OFDM transmissions in sharing secret keys over wireless channels in the presence of a passive eavesdropper. In Chapter 4, we have shown that a description of OFDM communications as a particular instance of MIMO channels can be leveraged in order to gain insight in the secrecy performance of such systems. In this chapter, we provide general results that can be applied to generic MIMO Gaussian channels, and hence, also to OFDM transmissions. Specifically, we study the problem of secret-key agreement over quasi-static MIMO fading channels. Although channel state information about the eavesdropper's channel is ultimately required to distill secret keys, we show that, in certain regimes, the optimal signaling is independent of the eavesdropper's channel realization and depends on the main channel realization alone. By combining this optimal signaling with a reconciliation phase and a privacy amplification phase [81], we obtain a *semi-blind* optimal key-distillation strategy, in which the CSI of the eavesdropper's channel is required during the privacy amplification phase only.

5.1 Problem statement

We consider the problem of secret-key agreement between a transmitter and a legitimate receiver in a wireless network in presence of an eavesdropper who overhears transmissions broadcasted over the wireless medium. We assume that the transmitter, the legitimate receiver and the eavesdropper are equipped with n_{T}, n_{R} and n_{E} antennas, respectively. Transmission takes place over quasi-static fading channels, that is the MIMO channel matrices $\boldsymbol{G}_{\mathsf{R}} \in \mathbb{C}^{n_{\mathsf{R}} \times n_{\mathsf{T}}}, \boldsymbol{G}_{\mathsf{E}} \in \mathbb{C}^{n_{\mathsf{E}} \times n_{\mathsf{T}}}$ are fixed during the transmission of an entire codeword and they are assumed to be known to all three terminals.[1] We note that full knowledge

[1] We remark that the results in this chapter are valid for generic, quasi static, MIMO Gaussian channels. Therefore, the matrices $\boldsymbol{G}_{\mathsf{R}}, \boldsymbol{G}_{\mathsf{E}}$ are not supposed to have any particular structure.

of channel state information is a strong assumption but we will see in subsequent sections that secret-key agreement can operate in a semi-blind fashion without requiring the knowledge of the eavesdropper channel at all stages of the distillation process. The transmitter broadcasts symbols $\boldsymbol{x} \in \mathbb{C}^{n_{\mathsf{T}} \times 1}$ so that the received signals at the legitimate receiver and the eavesdropper are

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{G}_{\mathsf{R}} \boldsymbol{x} + \boldsymbol{w}_{\mathsf{R}} \\ \text{and} \quad \boldsymbol{z} &= \boldsymbol{G}_{\mathsf{E}} \boldsymbol{x} + \boldsymbol{w}_{\mathsf{E}}, \end{aligned} \tag{5.1}$$

where the vectors $\boldsymbol{w}_{\mathsf{R}}$ and $\boldsymbol{w}_{\mathsf{E}}$ contain i.i.d., zero-mean, circularly symmetric, complex Gaussian random variables with unit variance. Channel uses are subject to the average power constraint

$$\frac{1}{n} \sum_{i=1}^{n} \|\boldsymbol{x}(i)\|^2 \leq P, \tag{5.2}$$

in which i denotes the index of the channel use. When n is sufficiently large, the power constraint is equivalent to a trace constraint on the input covariance matrix $\boldsymbol{K}_{\boldsymbol{x}} = \mathbb{E}\{\boldsymbol{x}\boldsymbol{x}^*\}$. In addition, the transmitter and the receiver are allowed to communicate over a two way, public, noiseless and authenticated channel to distill a secret-key from the symbols transmitted over the noisy channel.

We refer the reader to [14] for a precise description of a key-distillation strategy. Suffice to say that it consists of transmissions over the noisy channel as well as exchanges of messages over the public channel. A secret-key rate is defined as the ratio between the number of key bits k obtained at the end of a key-distillation strategy and the number of noisy channel uses n required to obtain it. A secret-key rate $R = k/n$ is achievable if there exists a secret-key distillation strategy such that,

- on denoting the secret key distilled at the transmitter and that at the legitimate receiver by K and $\hat{K}$, the error probability is zero asymptotically, that is:

$$\lim_{n \to \infty} \mathrm{P}\left[K \neq \hat{K}\right] = 0; \tag{5.3}$$

- the mutual information between the secret key and the eavesdropper observations is arbitrarily low (strong secrecy constraint [82]); that is, if we denote the messages sent on the public two-way channel by the the random variable D and we collect the outputs of the eavesdropper channel in the random vector $\boldsymbol{z}^n \in \mathbb{C}^{nn_{\mathsf{E}} \times 1}$, it holds that

$$\lim_{n \to \infty} \mathbb{I}(K; \boldsymbol{z}^n D) = 0; \tag{5.4}$$

- the distilled random key is asymptotically uniformly distributed, that is:

$$\lim_{n\to\infty} |\mathbb{H}(K) - k| = 0. \tag{5.5}$$

The supremum of achievable secret-key rates is called the secret-key capacity. Since the signals received by the legitimate receiver and the eavesdropper are conditionally independent given the transmitted signal $\boldsymbol{x}$, that is $\boldsymbol{y} \to \boldsymbol{x} \to \boldsymbol{z}$ forms a Markov chain, the secret-key capacity is known [79] and given by

$$S = \max_{\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{x}})\leq P} \mathbb{I}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{z})\,. \tag{5.6}$$

Maurer and Wolf [82] showed that one can achieve all secret-key rates below secret-key capacity with a *sequential key-distillation strategy*, by which the reliability and secrecy requirements are handled (and optimized) independently in successive phases. Specifically, a sequential secret-key distillation strategy consists of the following phases.

1. *Randomness sharing.* The transmitter sends through the noisy channel random information that is received by the legitimate receiver and the eavesdropper.
2. *Advantage distillation.* If needed, the legitimate parties exchange information over the public channel in order to process the noisy observations gathered by the legitimate receiver and collect the ones for which it has an advantage over the eavesdropper. The concept of advantage distillation was introduced by [15] to show that key-distillation strategies with two-way communication are, in general, more powerful than key-distillation strategies with one-way communication.
3. *Information reconciliation.* The transmitter and the legitimate receiver exchange messages over the public channel to agree on a common bit sequence. Information reconciliation protocols for secret-key agreement were first introduced in [83] for discrete random variables. In essence, these protocols are simple error-correcting codes that rely two-way communications to exchange parity checks and identify the location of errors. Reconciliation protocols for continuous random variables were developed subsequently in [76–78].
4. *Privacy amplification.* [81] The transmitter and the legitimate receiver publicly agree on a deterministic function they apply to their common sequence to generate a secret key.

In this work, we focus primarily on the first phase of the key-distillation process and we investigate the optimal transmission strategy to adopt when the terminals in the network deploy multiple antennas.

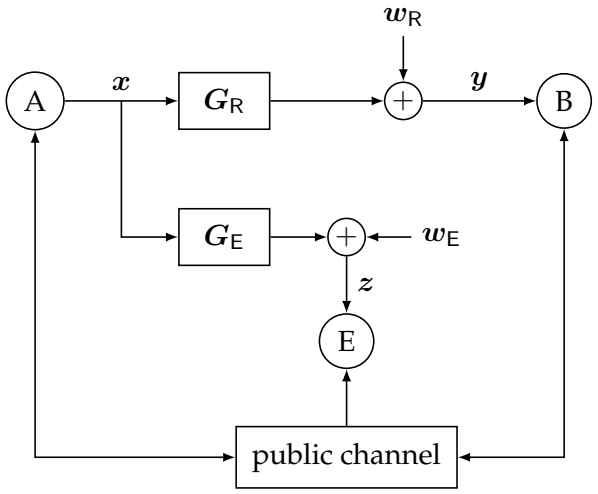

Figure 5.1. *Secret-key agreement over quasi-static MIMO fading channels.*

5.2 Secret-key capacity in the high-SNR regime

We first analyze the asymptotic behavior of secret-key capacity in the high-power regime as $P \to \infty$. Our approach follows closely the lines of Khisti *et al.* [61]. For simplicity, we assume throughout that the eavesdropper's channel matrix $\boldsymbol{G}_{\mathsf{E}}$ has full column rank.

Proposition 1. *The high-power secret-key capacity of the quasi-static fading MIMO Gaussian channel is*

$$\lim_{P\to\infty} S(P) = \sum_{i=1}^{s} \log(1+\sigma_i^2), \tag{5.7}$$

in which $\sigma_1, \ldots, \sigma_s$ are the generalized singular values of the channel matrices $\boldsymbol{G}_{\mathsf{R}}$ and $\boldsymbol{G}_{\mathsf{E}}$.

In the remainder of this section we provide the achievability part and the converse part of the proof of Proposition 1. In the process, we also establish the expression of the beamforming strategy used to achieve secret-key capacity.

5.2.1 Achievability

If we assume that the input $\boldsymbol{x}$ has a Gaussian distribution, by using the block determinant formula [84], the conditional mutual information in (5.6) becomes

$$\begin{aligned}
\mathbb{I}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{z}) &= h(\boldsymbol{y},\boldsymbol{z}) - h(\boldsymbol{z}) - h(\boldsymbol{w}_{\mathsf{R}}) && (5.8)\\
&= \log(2\pi e)^{n_{\mathsf{R}}+n_{\mathsf{E}}}|\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*}+\boldsymbol{I}| && (5.9)\\
&\quad\cdot|\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{R}}^{*}+\boldsymbol{I}-\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*}(\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*}+\boldsymbol{I})^{-1}\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{R}}^{*}| && (5.10)\\
&\quad-\log(2\pi e)^{n_{\mathsf{E}}}|\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*}+\boldsymbol{I}|-\log(2\pi e)^{n_{\mathsf{R}}}|\boldsymbol{I}| && (5.11)\\
&= \log|\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{R}}^{*}+\boldsymbol{I}-\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*}(\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*}+\boldsymbol{I})^{-1}\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{R}}^{*}|. && (5.12)
\end{aligned}$$

Moreover, on defining $\tilde{\boldsymbol{G}}_{\mathsf{R}}=\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}$ and $\tilde{\boldsymbol{G}}_{\mathsf{E}}=\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}$ we have

$$\begin{aligned}
\mathbb{I}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{z}) &= \log|\boldsymbol{I}+\tilde{\boldsymbol{G}}_{\mathsf{R}}\tilde{\boldsymbol{G}}_{\mathsf{R}}^{*}-\tilde{\boldsymbol{G}}_{\mathsf{R}}\tilde{\boldsymbol{G}}_{\mathsf{E}}^{*}(\tilde{\boldsymbol{G}}_{\mathsf{E}}\tilde{\boldsymbol{G}}_{\mathsf{E}}^{*}+\boldsymbol{I})^{-1}\tilde{\boldsymbol{G}}_{\mathsf{E}}\tilde{\boldsymbol{G}}_{\mathsf{R}}^{*}| && (5.13)\\
&= \log|\boldsymbol{I}+\tilde{\boldsymbol{G}}_{\mathsf{R}}(\boldsymbol{I}-\tilde{\boldsymbol{G}}_{\mathsf{E}}^{*}(\tilde{\boldsymbol{G}}_{\mathsf{E}}\tilde{\boldsymbol{G}}_{\mathsf{E}}^{*}+\boldsymbol{I})^{-1}\tilde{\boldsymbol{G}}_{\mathsf{E}})\tilde{\boldsymbol{G}}_{\mathsf{R}}^{*}| && (5.14)\\
&= \log|\boldsymbol{I}+\tilde{\boldsymbol{G}}_{\mathsf{R}}(\boldsymbol{I}+\tilde{\boldsymbol{G}}_{\mathsf{E}}^{*}\tilde{\boldsymbol{G}}_{\mathsf{E}})^{-1}\tilde{\boldsymbol{G}}_{\mathsf{R}}^{*}| && (5.15)\\
&= \log|\boldsymbol{I}+(\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}\boldsymbol{G}_{\mathsf{R}}^{*}\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}})(\boldsymbol{I}+\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}\boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}})^{-1}| && (5.16)\\
&= \log|\boldsymbol{I}+\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}(\boldsymbol{G}_{\mathsf{R}}^{*}\boldsymbol{G}_{\mathsf{R}}+\boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}})\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}|-\log|\boldsymbol{I}+\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}\boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}^{\frac{1}{2}}|, && (5.17)
\end{aligned}$$

where we have used the identity

$$\boldsymbol{I}-\boldsymbol{X}^{*}(\boldsymbol{X}\boldsymbol{X}^{*}+\boldsymbol{I})^{-1}\boldsymbol{X}=(\boldsymbol{I}+\boldsymbol{X}^{*}\boldsymbol{X})^{-1} \tag{5.18}$$

and the fact that $|\boldsymbol{I}+\boldsymbol{X}\boldsymbol{Y}|=|\boldsymbol{I}+\boldsymbol{Y}\boldsymbol{X}|$ for matrices $\boldsymbol{X},\boldsymbol{Y}$ with compatible dimensions.

The expression in (5.17) resembles that obtained for the secrecy capacity of a MIMO Gaussian wiretap channel. Specifically, if we introduce an equivalent channel matrix $\boldsymbol{G}_{\mathsf{K}}$ as[2]

$$\boldsymbol{G}_{\mathsf{K}}^{*}\boldsymbol{G}_{\mathsf{K}}=\boldsymbol{G}_{\mathsf{R}}^{*}\boldsymbol{G}_{\mathsf{R}}+\boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}}, \tag{5.19}$$

then (5.17) is the objective function of the maximization problem leading to the secrecy capacity of a MIMO Gaussian wiretap channel with main channel gain $\boldsymbol{G}_{\mathsf{K}}$ and eavesdropper channel gain $\boldsymbol{G}_{\mathsf{E}}$:

$$S=\max_{\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{x}})\leq P}\log|\boldsymbol{I}+\boldsymbol{G}_{\mathsf{K}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{K}}^{*}|-\log|\boldsymbol{I}+\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*}|. \tag{5.20}$$

[2]The existence of $\boldsymbol{G}_{\mathsf{K}}$ is guaranteed by the fact that the set of positive semidefinite matrices is closed with respect to addition and by the existence of the square root of a positive semidefinite matrix.

We notice that the different nature of the secret-key agreement problem with respect to the standard wiretap channel allows a symmetric role for the transmitter and the receiver, due to the presence of two-way communications over the public channel. As observed in [15] for the case of secret-key agreement over broadcast binary symmetric channels with public discussion, the receiver can create a conceptual broadcast channel to the transmitter and the eavesdropper, such that the conceptual main channel is equivalent to the real main channel but the adversary's conceptual channel is equivalent to a cascade of the real main and eavesdropper channel. Analogously, in our case the public channel allows the creation of a conceptual main channel $\boldsymbol{G}_{\mathsf{K}}$ which has square modulus (in matrix polar decomposition terms) given by the sum of the square modulus of the actual main and eavesdropper channel $\boldsymbol{G}_{\mathsf{R}}$ and $\boldsymbol{G}_{\mathsf{E}}$. Then, this relationship suggests also a geometrical counterpart of the information-theoretic intuition for which the main and the eavesdropper channel convey orthogonal information streams when the secrecy capacity is attained.

The similarity between the two problems suggests that the channel input achieving secret-key capacity has a structure identical to that achieving secrecy capacity. Therefore, following [85], we consider the GSVD of $(\boldsymbol{G}_{\mathsf{R}}, \boldsymbol{G}_{\mathsf{E}})$, and, analogously to (4.28), we write

$$\boldsymbol{\Psi}_{\mathsf{R}}^{*}\boldsymbol{G}_{\mathsf{R}}\boldsymbol{\Omega} = \boldsymbol{\Sigma}_{\mathsf{R}} = \begin{bmatrix} \mathbf{0} & \\ & \boldsymbol{D}_{\mathsf{R}} \end{bmatrix} \quad , \quad \boldsymbol{\Psi}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\Omega} = \boldsymbol{\Sigma}_{\mathsf{E}} = \begin{bmatrix} \boldsymbol{I} & \\ & \boldsymbol{D}_{\mathsf{E}} \\ & \mathbf{0} \end{bmatrix} \tag{5.21}$$

where $\boldsymbol{\Psi}_{\mathsf{R}}, \boldsymbol{\Psi}_{\mathsf{E}}$ are unitary matrices, $\boldsymbol{\Omega}$ is invertible and $\boldsymbol{D}_{\mathsf{R}}, \boldsymbol{D}_{\mathsf{E}}$ are diagonal matrices with real nonnegative entries $d_{\mathrm{R}1}, \ldots, d_{\mathrm{R}s}$ and $d_{\mathrm{E}1}, \ldots, d_{\mathrm{E}s}$, respectively. The number s is determined by the two matrices $\boldsymbol{G}_{\mathsf{R}}, \boldsymbol{G}_{\mathsf{E}}$. The generalized singular values of $(\boldsymbol{G}_{\mathsf{R}}, \boldsymbol{G}_{\mathsf{E}})$ are defined as $\sigma_i = d_{\mathrm{R}i}/d_{\mathrm{E}i}$ for $i = 1, \ldots, s$. To transmit power along the channel direction determined by the GSVD, we define the input signal as

$$\boldsymbol{x} = \boldsymbol{\Omega}\boldsymbol{u} = \boldsymbol{\Omega} \begin{bmatrix} \mathbf{0}_{\mathsf{n_T}-\mathsf{s}} \\ \boldsymbol{t} \end{bmatrix}, \tag{5.22}$$

where the random vector $\boldsymbol{t}$ contains s i.i.d., zero mean, complex Gaussian random variables. The variance of each of these variables is set to $\frac{P}{n_{\mathsf{T}}\sigma_{\max}(\boldsymbol{\Omega})}$ in order to satisfy the input power constraint. We denote the diagonal covariance matrix of $\boldsymbol{u}$ by $\boldsymbol{K}_{\boldsymbol{u}} = \mathbb{E}\{\boldsymbol{u}\boldsymbol{u}^{*}\}$, so that $\boldsymbol{K}_{\boldsymbol{x}} =$

$\boldsymbol{\Omega K_u \Omega}^*$ and the achievable secret-key rate becomes

$$R = \log \frac{|\boldsymbol{I} + \boldsymbol{K_x}(\boldsymbol{G}_{\mathsf{R}}^* \boldsymbol{G}_{\mathsf{R}} + \boldsymbol{G}_{\mathsf{E}}^* \boldsymbol{G}_{\mathsf{E}})|}{|\boldsymbol{I} + \boldsymbol{K_x} \boldsymbol{G}_{\mathsf{E}}^* \boldsymbol{G}_{\mathsf{E}}|} \tag{5.23}$$

$$= \log |\boldsymbol{I} + \boldsymbol{\Omega K_u \Omega}^* (\boldsymbol{\Omega}^{-*} (\boldsymbol{\Sigma}_{\mathsf{R}}^* \boldsymbol{\Sigma}_{\mathsf{R}} + \boldsymbol{\Sigma}_{\mathsf{E}}^* \boldsymbol{\Sigma}_{\mathsf{E}}) \boldsymbol{\Omega}^{-1})|$$

$$- \log |\boldsymbol{I} + \boldsymbol{\Omega K_u \Omega}^* \boldsymbol{\Omega}^{-*} \boldsymbol{\Sigma}_{\mathsf{E}}^* \boldsymbol{\Sigma}_{\mathsf{E}} \boldsymbol{\Omega}^{-1}| \tag{5.24}$$

$$= \log \frac{|\boldsymbol{I} + \boldsymbol{K_u}(\boldsymbol{\Sigma}_{\mathsf{R}}^* \boldsymbol{\Sigma}_{\mathsf{R}} + \boldsymbol{\Sigma}_{\mathsf{E}}^* \boldsymbol{\Sigma}_{\mathsf{E}})|}{|\boldsymbol{I} + \boldsymbol{K_u} \boldsymbol{\Sigma}_{\mathsf{E}}^* \boldsymbol{\Sigma}_{\mathsf{E}}|}. \tag{5.25}$$

In the limit $P \to \infty$, we obtain

$$\lim_{P \to \infty} R(P) = \sum_{i=1}^{s} \log \frac{d_{\mathrm{R}i}^2 + d_{\mathrm{E}i}^2}{d_{\mathrm{E}i}^2} = \sum_{i=1}^{s} \log(1 + \sigma_i^2), \tag{5.26}$$

where $\{\sigma_i^2\}_{i=1\ldots s}$ is the set of squared generalized singular values of $(\boldsymbol{G}_{\mathsf{R}}, \boldsymbol{G}_{\mathsf{E}})$. Since we assumed that $\boldsymbol{G}_{\mathsf{E}}$ has full column rank, the set $\{\sigma_i^2, \sigma_i > 0\}$ also represents the set of nonzero eigenvalues of $\boldsymbol{G}_{\mathsf{R}} (\boldsymbol{G}_{\mathsf{E}}^* \boldsymbol{G}_{\mathsf{E}})^{-1} \boldsymbol{G}_{\mathsf{R}}^*$.

For comparison, we recall the result in Lemma 2, that yields the corresponding high-power secrecy capacity of the MIMO Gaussian channel:

$$\lim_{P \to \infty} C_{\mathsf{s}}(P) = \sum_{i=1}^{s} [\log \sigma_i^2]^+. \tag{5.27}$$

The value in (5.27) is achieved if power is allocated only along the directions corresponding to generalized singular values greater than one. In contrast, for secret-key capacity, *all* the directions obtained with the GSVD decomposition of the channels are used, and secret-key capacity is always nonnegative, since the transmitter can use also those directions in which the eavesdropper channel is "better" than the main channel. Moreover, in the high-power regime every transmission strategy achieves the secret-key capacity, provided that power is transmitted over all the available directions.

5.2.2 Converse

We now show that the secret-key rate given in (5.26) is indeed the high-power secret-key capacity by following an approach similar to that used in [61] for the high-power secrecy capacity. The converse in [61] is based on a "Sato type" upper bound obtained by providing the legitimate receiver with the signal observed by the eavesdropper. The resulting channel is degraded and its secrecy capacity is given by the conditional mutual information $\mathbb{I}(\boldsymbol{x}; \boldsymbol{y}|\boldsymbol{z})$, where the noises at the legitimate receiver $\boldsymbol{w}_{\mathsf{R}}$ and that at the eavesdropper $\boldsymbol{w}_{\mathsf{E}}$ are arbitrarily correlated. In [85] and [86], it is shown that the upper bound obtained by minimizing

the conditional mutual information over all possible noise correlations coincides with the secrecy capacity of the original channel.

The converse proof for secret-key capacity turns out to be much simpler because it is based on the *direct* evaluation of the mutual information $\mathbb{I}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{z})$ with $\boldsymbol{w}_{\mathsf{R}}$ and $\boldsymbol{w}_{\mathsf{E}}$ independent from each other. We will make use of the following lemma.

Lemma 3. *The secret-key capacity of a MIMO quasi-static fading channel is achieved with Gaussian inputs.*

Proof. Given the expression of mutual information and the independence between the main channel noise $\boldsymbol{w}_{\mathsf{R}}$ and the transmitted signal $\boldsymbol{x}$, we can write

$$\mathbb{I}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{z}) = h(\boldsymbol{y}|\boldsymbol{z}) - h(\boldsymbol{y}|\boldsymbol{x},\boldsymbol{z}) = h(\boldsymbol{y}|\boldsymbol{z}) - h(\boldsymbol{w}_{\mathsf{R}})\,. \tag{5.28}$$

Therefore, the maximum in (5.6) is obtained by maximizing the conditional entropy $h(\boldsymbol{y}|\boldsymbol{z})$. Moreover, for a fixed input covariance matrix $\boldsymbol{K}_{\boldsymbol{x}}$ it holds

$$\begin{aligned} h(\boldsymbol{y}|\boldsymbol{z}) &= h(\boldsymbol{y} - \hat{\boldsymbol{y}}_{\mathsf{LMMSE}}(\boldsymbol{z})|\boldsymbol{z}) && (5.29)\\ &\leq h(\boldsymbol{y} - \hat{\boldsymbol{y}}_{\mathsf{LMMSE}}(\boldsymbol{z})) && (5.30)\\ &\leq \log(2\pi e)^{n_{\mathsf{R}}}|\boldsymbol{K}_{\mathsf{err}}|, && (5.31) \end{aligned}$$

where $\hat{\boldsymbol{y}}_{\mathsf{LMMSE}}(\boldsymbol{z})$ is the linear minimum mean squared error (LMMSE) estimate of $\boldsymbol{y}$ given the observation $\boldsymbol{z}$ and $\boldsymbol{K}_{\mathsf{err}}$ is the corresponding LMMSE estimation error covariance matrix. The equality is due to the fact that a constant shift does not change differential entropy, whereas the first inequality is a consequence of the fact that conditioning does not increase entropy. Finally, the second inequality is explained by considering that the Gaussian distribution maximizes the entropy of a random vector with given covariance matrix [87, Theorem 8.6.5]. We also recall that, for a given $\boldsymbol{K}_{\boldsymbol{x}}$, the error covariance matrix $\boldsymbol{K}_{\mathsf{err}}$ is univocally determined and does not depend on the input distribution. If the input is Gaussian, then the LMMSE estimation error is Gaussian as well, and statistically independent from the observation $\boldsymbol{z}$. In this case, both inequalities (5.30) and (5.31) hold as equalities and the conditional entropy is maximal.

□

Hence, since we can assume $\boldsymbol{x}$ has a Gaussian distribution, we can write

$$\begin{aligned} \mathbb{I}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{z}) &= \min_{\boldsymbol{\Theta}} h(\boldsymbol{y} - \boldsymbol{\Theta}\boldsymbol{z}) - h(\boldsymbol{w}_{\mathsf{R}}) && (5.32)\\ &= \min_{\boldsymbol{\Theta}} \log|\boldsymbol{I} + \boldsymbol{\Theta}\boldsymbol{\Theta}^{*} + \boldsymbol{\Delta}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{\Delta}^{*}|, && (5.33) \end{aligned}$$

where $\boldsymbol{\Delta} = \boldsymbol{G}_{\mathsf{R}} - \boldsymbol{\Theta}\boldsymbol{G}_{\mathsf{E}}$, and the minimum is attained by the LMMSE estimator

$$\boldsymbol{\Theta}_{\mathsf{LMMSE}} = (\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*})(\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K}_{\boldsymbol{x}}\boldsymbol{G}_{\mathsf{E}}^{*} + \boldsymbol{I})^{-1}.$$

Based on this expression, we upper bound the secret-key capacity as

$$\begin{aligned} S &= \max_{\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{x}})\leq P} \mathbb{I}(\boldsymbol{x};\boldsymbol{y}|\boldsymbol{z}) && (5.34)\\ &= \max_{\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{x}})\leq P} \min_{\boldsymbol{\Theta}} h(\boldsymbol{y}-\boldsymbol{\Theta}\boldsymbol{z}) - h(\boldsymbol{w}_{\mathsf{R}}) && (5.35)\\ &\leq \max_{\mathrm{tr}(\boldsymbol{K}_{\boldsymbol{x}})\leq P} h(\boldsymbol{y}-\boldsymbol{\Theta}_0\boldsymbol{z}) - h(\boldsymbol{w}_{\mathsf{R}})\,, && (5.36)\end{aligned}$$

for any $\boldsymbol{\Theta}_0 \neq \boldsymbol{\Theta}_{\mathsf{LMMSE}}$ in (5.36). In particular, if we choose $\boldsymbol{\Theta}_0 = \boldsymbol{G}_{\mathsf{R}}\boldsymbol{G}_{\mathsf{E}}^{\dagger}$ then $\boldsymbol{\Delta} = \boldsymbol{G}_{\mathsf{R}} - \boldsymbol{\Theta}_0\boldsymbol{G}_{\mathsf{E}} = \boldsymbol{0}$ and, as seen from (5.33), the maximization over $\boldsymbol{K}_{\boldsymbol{x}}$ becomes ineffective. In this case, the upper bound on the secret-key capacity reads

$$\begin{aligned} S &\leq \log|\boldsymbol{I} - \boldsymbol{\Theta}_0\boldsymbol{\Theta}_0^{*}| && (5.37)\\ &= \log|\boldsymbol{I} + \boldsymbol{G}_{\mathsf{R}}\boldsymbol{G}_{\mathsf{E}}^{\dagger}(\boldsymbol{G}_{\mathsf{R}}\boldsymbol{G}_{\mathsf{E}}^{\dagger})^{*}|. && (5.38)\end{aligned}$$

However, since $\boldsymbol{G}_{\mathsf{E}}$ is full column rank, then $\boldsymbol{G}_{\mathsf{R}}\boldsymbol{G}_{\mathsf{E}}^{\dagger}(\boldsymbol{G}_{\mathsf{E}}^{\dagger})^{*}\boldsymbol{G}_{\mathsf{R}}^{*} = \boldsymbol{G}_{\mathsf{R}}(\boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}})^{-1}\boldsymbol{G}_{\mathsf{R}}^{*}$, and the secret-key capacity is bounded by

$$\begin{aligned} S &\leq \log|\boldsymbol{I} + \boldsymbol{G}_{\mathsf{R}}(\boldsymbol{G}_{\mathsf{E}}^{*}\boldsymbol{G}_{\mathsf{E}})^{-1}\boldsymbol{G}_{\mathsf{R}}^{*}| && (5.39)\\ &= \sum_{i=1}^{s}\log(1+\sigma_i^2), && (5.40)\end{aligned}$$

which is exactly the high-power secret-key rate achieved in (5.26).

5.3 Secret-key capacity derivative in the low-SNR regime

We now turn our attention to the behavior of S as $P \to 0$. We exploit again the similarity between the expressions of secret-key capacity and secrecy capacity in (5.20) to obtain a closed-form characterization of secret-key capacity. Our analysis relies on the following key result.

Proposition 2. *The low-power first derivative with respect to the input power of the secret-key capacity of the MIMO Gaussian channel is proportional to the maximal eigenvalue of the matrix* $\boldsymbol{\Phi} = \boldsymbol{G}_{\mathsf{R}}^{*}\boldsymbol{G}_{\mathsf{R}}$, *namely*

$$\dot{S}(0) = \frac{1}{\ln 2}\lambda_{\mathsf{max}}(\boldsymbol{\Phi}), \tag{5.41}$$

and it can be achieved by transmitting in the direction of the maximal eigenvalue eigenvector of the main channel. Moreover, the second derivative of the secret-key capacity for $P = 0$ is given by

$$\ddot{S}(0) = -\min_{\{\alpha_i\}} \frac{1}{\ln 2} \sum_{i=1}^{\ell} \alpha_i^2 \left(\lambda_{\mathsf{max}}^2(\boldsymbol{\Phi}) + 2\lambda_{\mathsf{max}}(\boldsymbol{\Phi}) \|\boldsymbol{G}_{\mathsf{E}} \boldsymbol{\psi}_i\|^2 \right), \tag{5.42}$$

and it is achieved by the input covariance matrix $\boldsymbol{K}_{\boldsymbol{x}} = P \sum_{i=1}^{\ell} \alpha_i \boldsymbol{\psi}_i \boldsymbol{\psi}_i^*$, in which the vectors $\boldsymbol{\psi}_i$ form an orthonormal basis of the maximal eigenvalue eigenspace of $\boldsymbol{\Phi}$ and the coefficients α_i are such that $\alpha_i \in [0, 1]$ and $\sum \alpha_i = 1$.

Before proving Proposition 2, we discuss its implications for secret-key capacity. Note that the first order and second order derivatives of secret-key capacity can be used to approximate secret-key capacity in the low-power regime by using a Taylor expansion of the function $S(P)$ in $P = 0$:

$$S(P) = \dot{S}(0)P + \frac{\ddot{S}(0)}{2} P^2 + o(P^2). \tag{5.43}$$

Perhaps surprisingly, for a first order approximation, Proposition 2 tells us that secret-key capacity is determined by the main channel realization only. In fact, since $\boldsymbol{\Phi} = \boldsymbol{G}_{\mathsf{R}}^* \boldsymbol{G}_{\mathsf{R}}$, the optimal low-power signaling scheme is the same that achieves the low-power unconstrained capacity. In other words, the transmitter can beamform his signals based on the knowledge of the main channel alone. Therefore, the optimal low-power signaling scheme does not require any CSI for the eavesdropper channel at the transmitter. This result is particularly relevant for the design of practical secret-key agreement schemes because it means that the randomness sharing phase can be performed without worrying about the presence of the eavesdropper.

We note that it is also possible to determine the second derivative of the secret-key capacity; however, although secret-key capacity is still achieved by beamforming the transmitted signal in the direction of the maximal eigenvalue eigenspace of $\boldsymbol{\Phi}$, the eigenspace may have dimension $\ell > 1$ and the power allocation over the different dimensions may depend on the actual value of the eavesdropper channel matrix $\boldsymbol{G}_{\mathsf{E}}$.

To prove Proposition 2, we follow the lines of the method used in [62, Theorem 1]. However, we point out that the derivation of the low-SNR secrecy capacity in [62] seems to be affected by a logical flaw. To clarify this claim we introduce the compact notation

$$I_{\boldsymbol{G}}(\boldsymbol{K}_{\boldsymbol{x}}) \,:\, \boldsymbol{K}_{\boldsymbol{x}} \to \log |\boldsymbol{I} + \boldsymbol{G} \boldsymbol{K}_{\boldsymbol{x}} \boldsymbol{G}^*|. \tag{5.44}$$

and we start focusing on the first-order approximation of the secrecy capacity $C_{\mathsf{s}}(P) =$

$\dot{C}_{\mathsf{s}}(0)P + o(P)$, which, we recall, is the solution of the maximization problem

$$C_{\mathsf{s}} = \max_{\mathrm{tr}(\boldsymbol{K_x})\leq P} I_{\boldsymbol{G}_{\mathsf{R}}}(\boldsymbol{K_x}) - I_{\boldsymbol{G}_{\mathsf{E}}}(\boldsymbol{K_x}). \tag{5.45}$$

Then, for any fixed input covariance matrix $\boldsymbol{K_x}$ such that $\mathrm{tr}(\boldsymbol{K_x}) = P$, [62] defines the secrecy rate achieved with such an input covariance matrix as $I_{\mathsf{s}}(\boldsymbol{K_x}, P) = I_{\boldsymbol{G}_{\mathsf{R}}}(\boldsymbol{K_x}, P) - I_{\boldsymbol{G}_{\mathsf{E}}}(\boldsymbol{K_x}, P)$ and computes the first order approximation as

$$I_{\mathsf{s}}(\boldsymbol{K_x}, P) = \dot{I}_{\mathsf{s}}(\boldsymbol{K_x}, 0)P + o(P). \tag{5.46}$$

Nevertheless, this does not guarantee that $\dot{C}_{\mathsf{s}}(0) = \max_{\boldsymbol{K_x}} \dot{I}_{\mathsf{s}}(\boldsymbol{K_x}, 0)$. In general, we can only argue that

$$C_{\mathsf{s}}(P) \geq \left(\max_{\boldsymbol{K_x}} \dot{I}_{\mathsf{s}}(\boldsymbol{K_x}, 0) \right) P + o(P). \tag{5.47}$$

Proof. To circumvent the issue just highlighted, we might rely on a result of [88, Section III-D] which shows that the first-order expansion of the mutual information $I_{\boldsymbol{G}}(\boldsymbol{K_x})$ around $\boldsymbol{K_x} = \boldsymbol{0}$ is

$$I_{\boldsymbol{G}}(\boldsymbol{K_x}) = \mathrm{tr}(\boldsymbol{G}\boldsymbol{K_x}\boldsymbol{G}^*) + o(\|\boldsymbol{K_x}\|_{\mathsf{F}}), \tag{5.48}$$

where $\|\boldsymbol{K_x}\|_{\mathsf{F}} = \sqrt{\mathrm{tr}(\boldsymbol{K_x}\boldsymbol{K_x^*})}$. This expansion is also a low-SNR regime expression, but it is in term of $\boldsymbol{K_x}$ directly. Notice that, for any matrix $\boldsymbol{K_x}$ such that $\mathrm{tr}(\boldsymbol{K_x}) \leq P$, if P goes to zero then $\|\boldsymbol{K_x}\|_{\mathsf{F}}$ goes to zero as well. In fact, since $\boldsymbol{K_x}$ is positive semidefinite (with eigenvalues $\{\lambda_i\}_{i=1}^{n_{\mathsf{T}}}$, $\lambda_i \geq 0$), we have $\|\boldsymbol{K_x}\|_{\mathsf{F}} \leq \mathrm{tr}(\boldsymbol{K_x})$, as $\|\boldsymbol{K_x}\|_{\mathsf{F}}^2 = \sum_{i=1}^{n_{\mathsf{T}}} \lambda_i^2 \leq (\sum_{i=1}^{n_{\mathsf{T}}} \lambda_i)^2 \leq (\mathrm{tr}(\boldsymbol{K_x}))^2$. Hence, the low-SNR first-order approximation of the secrecy capacity is

$$\begin{aligned} C_{\mathsf{s}} &= \max_{\mathrm{tr}(\boldsymbol{K_x})\leq P} \mathrm{tr}(\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K_x}\boldsymbol{G}_{\mathsf{R}}^*) - \mathrm{tr}(\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K_x}\boldsymbol{G}_{\mathsf{E}}^*) + o(\|\boldsymbol{K_x}\|_{\mathsf{F}}) && (5.49)\\ &= \max_{\mathrm{tr}(\boldsymbol{K_x})\leq P} \mathrm{tr}(\boldsymbol{G}_{\mathsf{R}}\boldsymbol{K_x}\boldsymbol{G}_{\mathsf{R}}^*) - \mathrm{tr}(\boldsymbol{G}_{\mathsf{E}}\boldsymbol{K_x}\boldsymbol{G}_{\mathsf{E}}^*) + o(P). && (5.50) \end{aligned}$$

Based on this expression we can obtain the result of [62, Theorem 1]. Moreover, we can adapt this approach to the calculation of the secret-key capacity in (5.20). We first use the spectral decomposition to the input covariance matrix and we write it as

$$\boldsymbol{K_x} = P \sum_{i=1}^{n_{\mathsf{T}}} \alpha_i \boldsymbol{\psi}_i \boldsymbol{\psi}_i^*, \tag{5.51}$$

where P is the average transmitted power, the vectors $\boldsymbol{\psi}_i$ are columns of a unitary matrix and the coefficients α_i are such that $\alpha_i \in [0, 1]$ and $\sum \alpha_i = 1$, in order to preserve the positive semidefinite nature of $\boldsymbol{K_x}$ and to satisfy the trace constraint. Then, the first derivative of the

secret-key rate achieved with such $\boldsymbol{K}_{\boldsymbol{x}}$ reads

$$\dot{R}(0) = \frac{1}{\ln 2}\sum_{i=1}^{n_{\mathsf{T}}} \alpha_i (\mathrm{tr}(\boldsymbol{G}_{\mathsf{K}}\boldsymbol{\psi}_i\boldsymbol{\psi}_i^*\boldsymbol{G}_{\mathsf{K}}^*) - \mathrm{tr}(\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i\boldsymbol{\psi}_i^*\boldsymbol{G}_{\mathsf{E}}^*)) \tag{5.52}$$

$$= \frac{1}{\ln 2}\sum_{i=1}^{n_{\mathsf{T}}} \alpha_i (\boldsymbol{\psi}_i^*(\boldsymbol{G}_{\mathsf{R}}^*\boldsymbol{G}_{\mathsf{R}} + \boldsymbol{G}_{\mathsf{E}}^*\boldsymbol{G}_{\mathsf{E}})\boldsymbol{\psi}_i - \boldsymbol{\psi}_i^*\boldsymbol{G}_{\mathsf{E}}^*\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i) \tag{5.53}$$

$$= \frac{1}{\ln 2}\sum_{i=1}^{n_{\mathsf{T}}} \alpha_i \boldsymbol{\psi}_i^*\boldsymbol{G}_{\mathsf{R}}^*\boldsymbol{G}_{\mathsf{R}}\boldsymbol{\psi}_i, \tag{5.54}$$

in which we have used the property of the trace operator, $\mathrm{tr}(\boldsymbol{AB}) = \mathrm{tr}(\boldsymbol{BA})$ [84], and the characterization of $\boldsymbol{G}_{\mathsf{K}}$ in (5.19). Note that the first derivative of the secret-key rate in (5.54) is maximized by choosing $\alpha_1 = 1$, $\alpha_i = 0$ for $i \neq 1$ and $\boldsymbol{\psi}_1$ an eigenvector corresponding to the maximal eigenvalue of the matrix $\boldsymbol{\Phi} = \boldsymbol{G}_{\mathsf{R}}^*\boldsymbol{H}_{\mathsf{R}}$. Hence, we obtain the secret-key capacity first derivative as

$$\dot{S}(0) = \frac{1}{\ln 2}\lambda_{\mathsf{max}}(\boldsymbol{\Phi}). \tag{5.55}$$

Analogously, we can evaluate a second-order expansion of the secret-key capacity. In fact, the first derivative of the low-SNR secret-key capacity is achieved by transmitting over the maximal eigenvalue eigenspace. Hence, if the maximal eigenvalue of $\boldsymbol{\Phi}$ has multiplicity ℓ, then $\dot{S}(0)$ is achieved by all the input covariance matrices of the form

$$\boldsymbol{K}_{\boldsymbol{x}} = P\sum_{i=1}^{\ell} \alpha_i \boldsymbol{\psi}_i\boldsymbol{\psi}_i^*, \tag{5.56}$$

where the coefficients α_i are such that $\alpha_i \in [0,1]$ and $\sum \alpha_i = 1$, and the vectors $\boldsymbol{\psi}_i$ are taken from an orthonormal basis of the maximal eigenvalue eigenspace. Given this input covariance matrix it is possible to optimally select the coefficients α_i in order to reach also the second derivative of the secret-key capacity. Therefore, we can write the second derivative of the secret-key rate achieved with the input covariance matrix (5.56) as

$$\ddot{R}(0) = -\frac{1}{\ln 2}\mathrm{tr}\left(\left(\sum_{i=1}^{\ell}\alpha_i\boldsymbol{G}_{\mathsf{K}}\boldsymbol{\psi}_i\boldsymbol{\psi}_i^*\boldsymbol{G}_{\mathsf{K}}^*\right)^2\right) + \frac{1}{\ln 2}\mathrm{tr}\left(\left(\sum_{i=1}^{\ell}\alpha_i\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i\boldsymbol{\psi}_i^*\boldsymbol{G}_{\mathsf{E}}^*\right)^2\right) \tag{5.57}$$

$$= -\frac{1}{\ln 2}\sum_{i,j}\alpha_i\alpha_j\left(|\boldsymbol{\psi}_j^*\boldsymbol{G}_{\mathsf{K}}^*\boldsymbol{G}_{\mathsf{K}}\boldsymbol{\psi}_i|^2 - |\boldsymbol{\psi}_j^*\boldsymbol{G}_{\mathsf{E}}^*\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i|^2\right) \tag{5.58}$$

$$= -\frac{1}{\ln 2}\sum_{i,j}\alpha_i\alpha_j\left(|\boldsymbol{\psi}_j^*(\boldsymbol{G}_{\mathsf{R}}^*\boldsymbol{G}_{\mathsf{R}} + \boldsymbol{G}_{\mathsf{E}}^*\boldsymbol{G}_{\mathsf{E}})\boldsymbol{\psi}_i|^2 - |\boldsymbol{\psi}_j^*\boldsymbol{G}_{\mathsf{E}}^*\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i|^2\right) \tag{5.59}$$

$$= -\frac{1}{\ln 2}\sum_{i,j}\alpha_i\alpha_j\left(|\boldsymbol{\psi}_j^*\boldsymbol{G}_{\mathsf{R}}^*\boldsymbol{G}_{\mathsf{R}}\boldsymbol{\psi}_i|^2 + 2\mathrm{Re}\left\{(\boldsymbol{\psi}_j^*\boldsymbol{G}_{\mathsf{R}}^*\boldsymbol{G}_{\mathsf{R}}\boldsymbol{\psi}_i)(\boldsymbol{\psi}_j^*\boldsymbol{G}_{\mathsf{E}}^*\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i)^*\right\}\right). \tag{5.60}$$

Moreover, since the vectors $\{\boldsymbol{\psi}_i\}$ are taken from an orthonormal basis of the maximal eigenvalue eigenspace of $\boldsymbol{\Phi}$, we can simplify the expression of the second derivative of the secret-

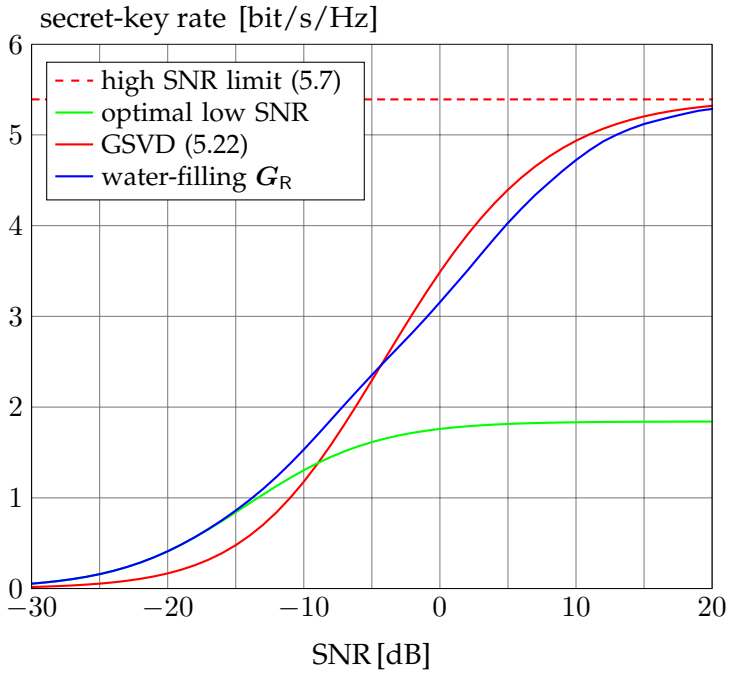

Figure 5.2. *Average secret-key rate as a function of the SNR.* $n_{\mathsf{T}} = n_{\mathsf{R}} = n_{\mathsf{E}} = 3$. *The semi-blind beamforming over the legitimate channel is optimal in both low and high-SNR regime and it performs closely to the GSVD input for intermediate SNRs.*

key rate as

$$\ddot{R}(0) = -\frac{1}{\ln 2}\sum_{i,j}\alpha_i\alpha_j\left(|\lambda_{\mathsf{max}}(\boldsymbol{\Phi})\boldsymbol{\psi}_j^*\boldsymbol{\psi}_i|^2 + 2\mathrm{Re}\left\{(\lambda_{\mathsf{max}}(\boldsymbol{\Phi})\boldsymbol{\psi}_j^*\boldsymbol{\psi}_i)(\boldsymbol{\psi}_j^*\boldsymbol{G}_{\mathsf{E}}^*\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i)^*\right\}\right) \quad (5.61)$$

$$= -\frac{1}{\ln 2}\sum_{i}\alpha_i^2\left(\lambda_{\mathsf{max}}^2(\boldsymbol{\Phi}) + 2\lambda_{\mathsf{max}}(\boldsymbol{\Phi})\|\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i\|^2\right). \quad (5.62)$$

Then, the second derivative of the secret-key capacity is obtained by maximizing (5.62) over the set of admittable ℓ-tuplas $\{\alpha_i\}$, that is

$$\ddot{S}(0) = -\min_{\{\alpha_i\}}\frac{1}{\ln 2}\sum_{i}\alpha_i^2\left(\lambda_{\mathsf{max}}^2(\boldsymbol{\Phi}) + 2\lambda_{\mathsf{max}}(\boldsymbol{\Phi})\|\boldsymbol{G}_{\mathsf{E}}\boldsymbol{\psi}_i\|^2\right). \quad (5.63)$$

□

5.4 Numerical results

We conclude our analysis with numerical results that illustrate the secret-key rates achieved with different signaling schemes. We consider a MIMO system in which $n_{\mathsf{T}} = n_{\mathsf{R}} = n_{\mathsf{E}} = 3$, and the main and the eavesdropper channels exhibit flat Rayleigh fading, that is the entries of both $\boldsymbol{G}_{\mathsf{R}}$ and $\boldsymbol{G}_{\mathsf{E}}$ are realizations of iid, zero mean, circularly symmetric, complex

Gaussian variables with unit variance. Figure 5.2 shows the secret-key rates obtained with three different signaling strategies: the GSVD input of (5.22), which was shown to be capacity achieving in the high-power regime; the optimal low-power input, which consists in beamforming the signal in the direction corresponding to the maximal eigenvalue of the matrix $\mathbf{\Phi}$; the semi-blind beamforming and water-filling over the legitimate channel $\boldsymbol{G}_{\mathsf{R}}$. Note that the optimal low-power input performs poorly as the available power at the transmitter increases, since it does not exploit all the degrees of freedom of the system. In fact, information is transmitted only along the directions corresponding to the maximal singular value of the legitimate channel and all the other directions are left unemployed. On the other hand, beamforming and water-filling on the legitimate channel coincides with the optimal low-power solution when $P \to 0$, and it conveys information over all the available directions of the main channel as the available power increases. This input turns out to be optimal also in the high-power regime. Actually, based on the derivation of the high-power secret-key capacity achieving scheme in Section 5.2.1, we have pointed out that all the subchannels defined by the GSVD of $(\boldsymbol{G}_{\mathsf{R}}, \boldsymbol{G}_{\mathsf{E}})$ can be used to transmit the common randomness from which the secret key will be distilled. Hence, as $P \to \infty$, all the input strategies associated to a full rank input covariance matrix attain the secret key capacity. This is highlighted in Figure 5.2, where it can be seen that the beamforming over $\boldsymbol{G}_{\mathsf{R}}$ achieves the same performance guaranteed by the GSVD input for high-power and it outperforms it in the low-power regime.

In Figure 5.3 we show that optimizing the input over $\boldsymbol{G}_{\mathsf{R}}$ turns out to be effective even if the eavesdropper enjoys better channel conditions than the legitimate receiver. The curves represent the 1% outage secret-key rates obtained for a MIMO Gaussian wiretap channel with $n_{\mathsf{T}} = n_{\mathsf{R}} = 3$ and $n_{\mathsf{E}} = 10$. In other words, the eavesdropper is equipped with a more powerful receiver and the outage analysis takes into account the worst 1% channel realizations for the main channel. Note that water-filling over the legitimate channel performs well compared to the optimal low-power and optimal high-power solutions.

Finally, in Figure 5.4 we compare the secret-key rates achieved by the different input strategies under exam, when the main and the eavesdropper channel enjoy different average SNR, Λ_{R} and Λ_{E}, respectively. The water-filling on the main channel and the GSVD input are capacity achieving for a wide range of SNR ratios $\Lambda_{\mathsf{RE}} = \Lambda_{\mathsf{R}}/\Lambda_{\mathsf{E}}$ between the two channels. Nevertheless, From Figure 5.5 it can be seen that the beamforming over $\boldsymbol{G}_{\mathsf{R}}$ significantly outperforms the GSVD input in the region where the receiver has a high SNR while the eavesdropper has a low SNR. On the other hand, in the opposite case the GSVD input

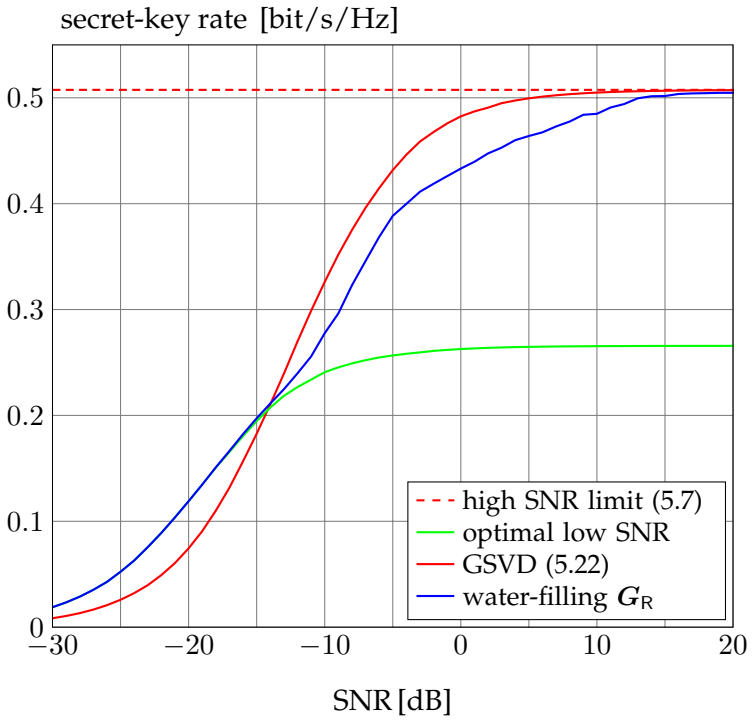

Figure 5.3. *1% outage secret-key rate as a function of the SNR.* $n_T = n_R = 3$ *and* $n_E = 10$.

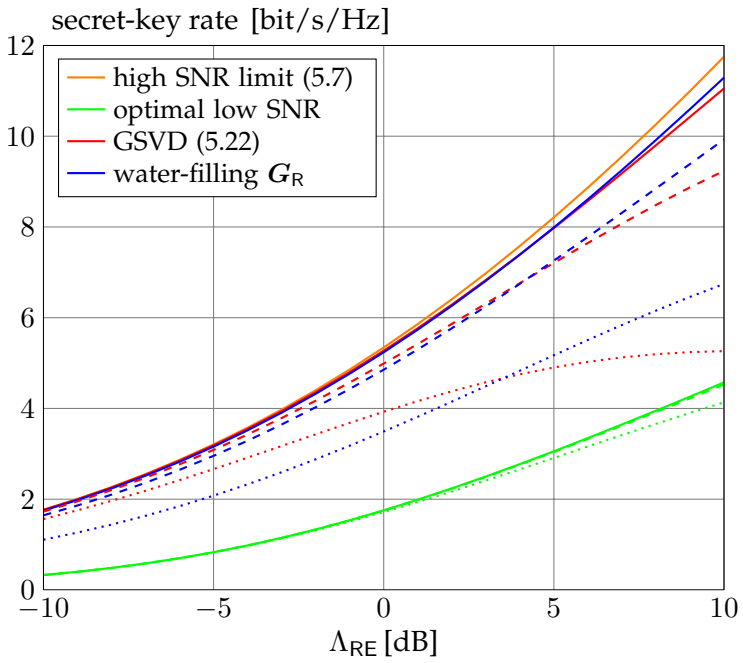

Figure 5.4. *Average secret-key rate as a function of the SNR ratio,* $\Lambda_{RE} = \Lambda_R/\Lambda_E$. $n_T = n_R = n_E = 3$. *Data are reported for different values of the main channel SNR,* $\Lambda_R = 10$ *dB (dotted lines),* $\Lambda_R = 20$ *dB (dashed lines),* $\Lambda_R = 30$ *dB (solid lines).*

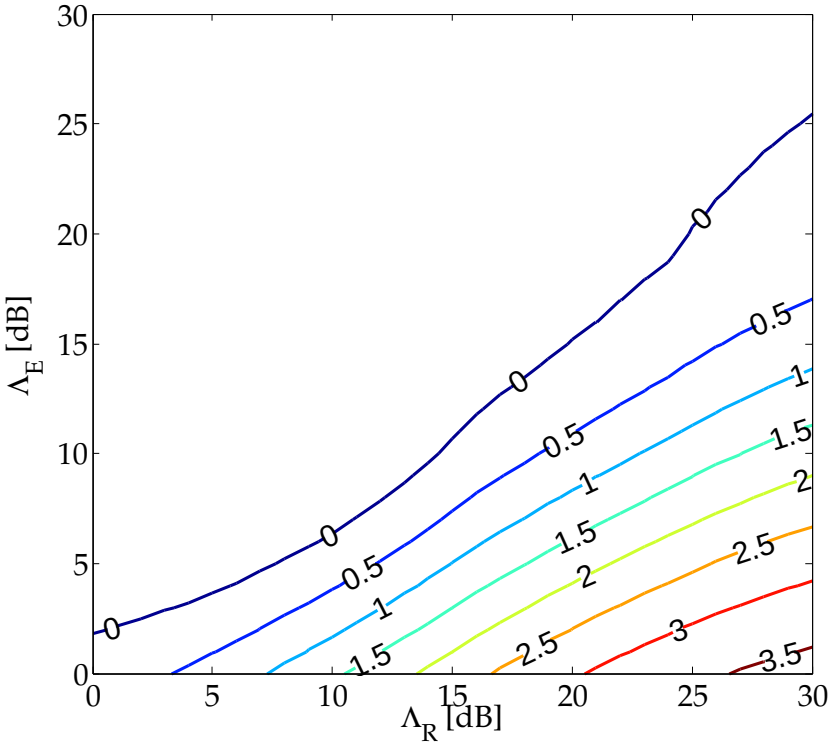

Figure 5.5. *Contour lines of the secret-key rate advantage (in [bit/s/Hz]) obtained using water-filling over the main channel with respect to the GSVD input of Eq. (5.22).*

shows a slight advantage.

Chapter 6

The jamming game in an OFDM setting

Jamming has traditionally represented a serious attack to the availability of transmission over wireless links, and hence a lot of attention has been devoted since the previous century to devise effective strategies to repel it, especially in the field of military communications.

However, a game-theoretic formulation of the jamming problem has only been proposed in the '80s [16, 17]. Such formulations describe it as a zero-sum game played by two adversaries: the transmitter/receiver pair on one side, and the jammer on the other. The payoff function, which the transmitter seeks to maximize, and the jammer to minimize, is the mutual information between the transmitted and received signals, while constraints on the possible strategies are set by power and energy limitations. From the first results on the Gaussian channel, many others have been found in scenarios such as MIMO channels [89–91], or the wideband channel limit [18], and fading channels [90, 92, 93]. In most cases the jamming game has a saddle point solution, that is a pair of strategies (one for the transmitter, the other for the jammer) that are each one optimal for the corresponding player, given that the opponent follows his optimal strategy. Thus they represent a Nash equilibrium, although convergence to it is not guaranteed.

When expressing the jamming game in information-theoretic terms, it is not customary to consider a particular modulation format. Little has been done in the literature with respect to the jamming problem within an OFDM framework: for example [94, 95] consider the robustness of the multicarrier scheme to certain given types of jammers (single tone, narrowband Gaussian, etc.). To our knowledge, the only attempt so far to apply an information-

theoretic jamming game to the OFDM channel is given in [96], where, however the system is modeled as the parallel of M channels, each independently jammed. We prefer to relax this assumption and allow abitrarily correlated inputs for both the transmitter and the jammer, and look for saddle point solution in this model. Then, in this chapter we start from the general system model in Section 1.1 and we build an equivalent vector representation of OFDM transmission in the presence of an active attacker, i.e., the jammer. Our aim is to formulate the jamming game as a minimax problem under trace constraints and to characterize the Nash equilibrium for such game.

6.1 Problem statement

In this analysis we use the general, continuous-time, system model in Section 1.1 to comprise both the DMT systems with CP and ZS, as well as the FMT systems, both CS and NS . Then, we recall that the (baseband equivalent of the) transmitted signal for a packet of L symbols can be written as the combination of the transmit waveforms

$$x(t) = \sum_{n=1}^{L} \sum_{i=1}^{M} u_i(nT)\gamma_i(t - nT) \tag{6.1}$$

Similarly, the demodulator produces the symbols $v_i(nT)$ by taking the inner product between the received signal and the receiver waveforms

$$v_i(nT) = \int \varphi_i^*(t - nT)y(t)\,dt \quad , \quad \begin{matrix} i = 1, \ldots, M \\ n = 1, \ldots, L \end{matrix} . \tag{6.2}$$

The channel g_{R} is assumed to be linear and time-invariant and hence its output is

$$x'(t) = x * g_{\mathsf{R}}\,(t) = \sum_{n=1}^{L} \sum_{i=1}^{M} u_i(nT)\gamma_i'(t - nT) \tag{6.3}$$

with $\gamma_i' = \gamma_i * g_{\mathsf{R}}$.

Along with legitimate transmission the receiver is also subject to jamming, that is an unwanted signal $s(t)$ transmitted by an adversary, which, through another linear time-invariant channel g_{J}, reaches the receiver as $s'(t) = s * g_{\mathsf{J}}\,(t)$. Hence, by also including the noise $w_{\mathsf{R}}(t)$, modeled as circularly symmetric complex Gaussian with power spectral density (PSD) $2N_0$ we get the time-domain received signal

$$y(t) = x'(t) + s'(t) + w_{\mathsf{R}}(t) \tag{6.4}$$

By gathering all data symbols of a packet into a single column vector $\boldsymbol{u} = [u_1(T), \ldots, u_M(LT)]^{\mathrm{T}}$, and all transmit waveforms into a row $\boldsymbol{\gamma}(t) = [\gamma_1(t-T), \ldots, \gamma_M(t-LT)]$ we can rewrite (6.1) as

$$x(t) = \boldsymbol{\gamma}(t)\boldsymbol{u} \tag{6.5}$$

Hence, we express the instantaneous transmitted power as

$$|x(t)|^2 = \boldsymbol{\gamma}(t)\boldsymbol{u}\boldsymbol{u}^*\boldsymbol{\gamma}^*(t) = \mathrm{tr}\left(\boldsymbol{u}\boldsymbol{u}^*\boldsymbol{\gamma}^*(t)\boldsymbol{\gamma}(t)\right) \tag{6.6}$$

and the mean energy per packet as

$$E_x = \mathbb{E}\left\{\int |x(t)|^2 \, dt\right\} = \mathbb{E}\left\{\int \mathrm{tr}\left(\boldsymbol{u}\boldsymbol{u}^*\boldsymbol{\gamma}^*(t)\boldsymbol{\gamma}(t)\right) \, dt\right\} \tag{6.7}$$

$$= \mathrm{tr}\left(\mathbb{E}\left\{\boldsymbol{u}\boldsymbol{u}^*\right\} \int \boldsymbol{\gamma}^*(t)\boldsymbol{\gamma}(t)\, dt\right) = \mathrm{tr}\left(\boldsymbol{K}_{\boldsymbol{u}}\boldsymbol{E}_{\boldsymbol{\gamma}}\right) \tag{6.8}$$

where $\boldsymbol{K}_{\boldsymbol{u}}$ is the covariance matrix of $\boldsymbol{u}$ and $\boldsymbol{E}_{\boldsymbol{\gamma}}$ is the matrix of cross energies between waveforms in $\boldsymbol{\gamma}(t)$. Similarly, the output of the legitimate channel can be written as $x'(t) = \boldsymbol{\gamma}'(t)\boldsymbol{u}$ with $\boldsymbol{\gamma}'(t) = \int \boldsymbol{\gamma}(u) g_{\mathsf{R}}(t-u)\, du$.

If we write the receiver output as a column vector $\boldsymbol{v} = [v_1(T), \ldots, v_M(LT)]^{\mathrm{T}}$ and the waveforms as a row vector $\boldsymbol{\varphi}(t) = [\varphi_1(t-T), \ldots, \varphi_M(t-LT)]$, from the decomposition of the received signal in (6.4), we have

$$\boldsymbol{v} = \int \boldsymbol{\varphi}^*(t) y(t)\, dt = \bar{\boldsymbol{x}} + \bar{\boldsymbol{s}} + \bar{\boldsymbol{w}}$$

with

$$\bar{\boldsymbol{x}} = \int \boldsymbol{\varphi}^*(t) x'(t)\, dt = \int \boldsymbol{\varphi}^*(t)\boldsymbol{\gamma}'(t)\boldsymbol{u}\, dt = \boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}}\boldsymbol{u} \tag{6.9}$$

$$\bar{\boldsymbol{w}} = \int \boldsymbol{\varphi}^*(t) w_{\mathsf{R}}(t)\, dt \;,\; \bar{\boldsymbol{w}} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{K}_{\bar{\boldsymbol{w}}}) \;,\; \boldsymbol{K}_{\bar{\boldsymbol{w}}} = 2N_0\boldsymbol{E}_{\boldsymbol{\varphi}} \tag{6.10}$$

$$\bar{\boldsymbol{s}} = \int \boldsymbol{\varphi}^*(t) s'(t)\, dt = \int \boldsymbol{\varphi}'^*(t) s(t)\, dt \tag{6.11}$$

In (6.11) we have introduced $\boldsymbol{\varphi}'(t) = \int \boldsymbol{\varphi}(u) g_{\mathsf{J}}^*(u-t)\, du$, so it is easy to see that only the components of $s(t)$ lying in the span of the waveforms $\varphi_i'(t-nT)$ give a nonzero contribution to the receiver output, and can influence the receiver performance. Without loss of generality, we can therefore assume $s(t) = \boldsymbol{\varphi}'(t)\boldsymbol{r}$, with $\boldsymbol{r}$ a column vector chosen by the jammer. Analogously to (6.8) and (6.9), we can then write

$$E_s = \mathrm{tr}\left(\boldsymbol{K}_{\boldsymbol{r}}\boldsymbol{E}_{\boldsymbol{\varphi}'}\right) \quad , \quad \bar{\boldsymbol{s}} = \boldsymbol{E}_{\boldsymbol{\varphi}'}\boldsymbol{r}$$

The so reduced vector-based model is illustrated in Figure 6.1.

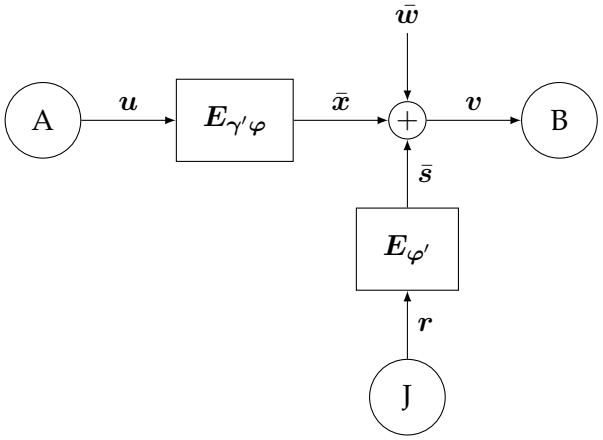

Figure 6.1. *OFDM transmission in the presence of a jamming attacker. Equivalent block diagram of the system in Figure 1.1, corresponding to (6.9) and (6.1). Here the blocks represents matrix multiplications.*

Observe that the above model, introduced with a continuous-time notation can be converted to discrete-time by properly sampling the waveforms and replacing integrals with summations.

We consider a zero-sum game between the transmitter/receiver pair on one side, and the jammer on the other, where the payoff function is the mutual information $\mathbb{I}(\boldsymbol{u};\boldsymbol{v})$ beetwen the input to the OFDM transmitter and the output of the OFDM receiver. All the players in the game have complete knowledge about both channels and the strategy adopted by the adversary. However, neither the legitimate transmitter nor the jammer can observe the signal transmitted by the other. Given that the channel is linear and Gaussian, and the energy constraints, the optimal strategies for both the transmitter and jammer are Gaussian [16, 91]. Moreover we look for the existance of a common maximin and minimax solution, so that

$$\max_{\boldsymbol{u}} \min_{\boldsymbol{r}} \mathbb{I}(\boldsymbol{u};\boldsymbol{v}) = \min_{\boldsymbol{r}} \max_{\boldsymbol{u}} \mathbb{I}(\boldsymbol{u};\boldsymbol{v}) \tag{6.12}$$

represent a saddle point in the payoff function. When assuming independent Gaussian $\boldsymbol{u}, \boldsymbol{r}$ the mutual information between $\boldsymbol{u}$ and $\boldsymbol{v}$ is given by

$$\mathbb{I}(\boldsymbol{u};\boldsymbol{v}) = \log \frac{|\boldsymbol{K}_{\bar{\boldsymbol{x}}} + \boldsymbol{K}_{\bar{\boldsymbol{w}}} + \boldsymbol{K}_{\bar{\boldsymbol{s}}}|}{|\boldsymbol{K}_{\bar{\boldsymbol{w}}} + \boldsymbol{K}_{\bar{\boldsymbol{s}}}|} \tag{6.13}$$

where

$$\boldsymbol{K}_{\bar{\boldsymbol{x}}} = \boldsymbol{E}_{\gamma'\varphi} \boldsymbol{K}_{\boldsymbol{u}} \boldsymbol{E}^*_{\gamma'\varphi} \quad , \quad \boldsymbol{K}_{\bar{\boldsymbol{s}}} = \boldsymbol{E}_{\varphi'} \boldsymbol{K}_{\boldsymbol{r}} \boldsymbol{E}_{\varphi'} \tag{6.14}$$

as $\boldsymbol{E}_{\varphi'}$ is Hermitian.

The average energy per packet for the transmitter and the jammer are constrained by E_{T} and E_{J}. For a later use, we also define the transmission SNR and jammer to noise ratio (JNR) as the transmitted signal energy constraints normalized over the noise energy, $\rho_{\mathsf{T}} = E_{\mathsf{T}}/(2N_0ML)$ and $\rho_{\mathsf{J}} = E_{\mathsf{J}}/(2N_0ML)$, respectively.

Formally, we can then write the minimax problem as

$$\min_{\boldsymbol{K_r}} \max_{\boldsymbol{K_u}} \left\{ \log |\boldsymbol{I} + \boldsymbol{K}_{\bar{\boldsymbol{x}}} (\boldsymbol{K}_{\bar{\boldsymbol{w}}} + \boldsymbol{K}_{\bar{\boldsymbol{s}}})^{-1}| \right\} \tag{6.15}$$

subject to:

$$\boldsymbol{K_u} \succ \boldsymbol{0} \quad , \quad \mathrm{tr}(\boldsymbol{K_u} \boldsymbol{E_\gamma}) \leq E_{\mathsf{T}} \tag{6.16}$$

$$\boldsymbol{K_r} \succ \boldsymbol{0} \quad , \quad \mathrm{tr}(\boldsymbol{K_r} \boldsymbol{E_{\varphi'}}) \leq E_{\mathsf{J}} \tag{6.17}$$

The payoff function (6.15) is convex with respect to $\boldsymbol{K_r}$ and concave with respect to $\boldsymbol{K_u}$, hence within the convex set determined by the constraints (6.16) and (6.17) it admits a saddle point solution.

By assuming that $\boldsymbol{E_{\gamma'\varphi}}$ and $\boldsymbol{E_{\varphi'}}$ are nonsingular and defining the Hermitian matrices

$$\boldsymbol{P} = \sqrt{\boldsymbol{E}_{\gamma'\varphi}^{-1} \boldsymbol{E}_\gamma \boldsymbol{E}_{\gamma'\varphi}^{-*}} \quad , \quad \boldsymbol{Q} = \sqrt{\boldsymbol{E}_{\varphi'}^{-1}} \tag{6.18}$$

we can express the traces in the energy constraints (6.16)–(6.17) as

$$\mathrm{tr}(\boldsymbol{K_u} \boldsymbol{E_\gamma}) = \mathrm{tr}(\boldsymbol{P} \boldsymbol{K}_{\bar{\boldsymbol{x}}} \boldsymbol{P}) \quad , \quad \mathrm{tr}(\boldsymbol{Q} \boldsymbol{K}_{\bar{\boldsymbol{s}}} \boldsymbol{Q}) = \mathrm{tr}(\boldsymbol{K_r} \boldsymbol{E_{\varphi'}}). \tag{6.19}$$

Then, with the substitutions

$$\bar{\boldsymbol{H}} = \boldsymbol{Q} \boldsymbol{P}^{-1} \quad , \quad \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}} = \boldsymbol{P} \boldsymbol{K}_{\bar{\boldsymbol{x}}} \boldsymbol{P} \tag{6.20}$$

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}} = \boldsymbol{Q} \boldsymbol{K}_{\bar{\boldsymbol{s}}} \boldsymbol{Q} \quad , \quad \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} = \boldsymbol{Q} \boldsymbol{K}_{\bar{\boldsymbol{w}}} \boldsymbol{Q} = 2N_0 \boldsymbol{Q} \boldsymbol{E}_{\boldsymbol{\varphi}} \boldsymbol{Q} \quad , \tag{6.21}$$

the minimax problem can be written as

$$\min_{\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}} \max_{\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}} \left\{ \log |\boldsymbol{I} + \bar{\boldsymbol{H}} \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}} \bar{\boldsymbol{H}}^* (\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} + \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}})^{-1}| \right\} \tag{6.22}$$

subject to:

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}} \succ \boldsymbol{0} \quad , \quad \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}) \leq E_{\mathsf{T}} \tag{6.23}$$

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}} \succ \boldsymbol{0} \quad , \quad \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}) \leq E_{\mathsf{J}} \tag{6.24}$$

which is the form of a jamming game for the MIMO transmission channel $\bar{\boldsymbol{H}}$, with ideal jamming channel and noise covariance matrix $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}$.

6.2 Saddle-point solution in the high-JNR regime

Allow us, for the time being, to introduce one more rewriting of the minimax problem, by letting $\bar{\boldsymbol{z}} = \bar{\boldsymbol{s}} + \bar{\boldsymbol{w}}$. Then, with $\boldsymbol{K}_{\bar{\boldsymbol{z}}} = \boldsymbol{K}_{\bar{\boldsymbol{s}}} + \boldsymbol{K}_{\bar{\boldsymbol{w}}}$ and $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}} = \boldsymbol{Q}\boldsymbol{K}_{\bar{\boldsymbol{z}}}\boldsymbol{Q}$ the problem (6.22)–(6.24) becomes

$$\min_{\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}}} \max_{\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}} f(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}}) \tag{6.25}$$

with

$$f(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}}) = \log|\boldsymbol{I} + \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}}^{-1/2}\bar{\boldsymbol{H}}\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}\bar{\boldsymbol{H}}^*\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}}^{-1/2}|, \tag{6.26}$$

subject to:

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}} \succ \boldsymbol{0} \quad , \quad \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}) \leq E_{\mathsf{T}} \tag{6.27}$$

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}} \succ \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} \quad , \quad \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}) \leq E_{\mathsf{J}} + \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}) \tag{6.28}$$

Now, if we relax the first constraint in (6.28) to $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}} \succ \boldsymbol{0}$, we can use the results in [91], [97, Theorem 8] to obtain the saddle-point solution

$$f(\tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{z}}}) = \log|\boldsymbol{I} + \Lambda\bar{\boldsymbol{H}}\bar{\boldsymbol{H}}^*|, \tag{6.29}$$

where we have denoted with Λ the equivalent signal to jammer plus noise ratio (SJNR),

$$\Lambda = \frac{E_{\mathsf{T}}}{E_{\mathsf{J}} + \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}})}. \tag{6.30}$$

Moreover, on writing as $\bar{\boldsymbol{H}} = \boldsymbol{U}_{\bar{\boldsymbol{H}}}\boldsymbol{\Sigma}_{\bar{\boldsymbol{H}}}^{1/2}\boldsymbol{V}_{\bar{\boldsymbol{H}}}^*$ the singular values decomposition (SVD) of the channel $\bar{\boldsymbol{H}}$, the optimal covariance matrices for the transmitter and the attacker are given by

$$\tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{x}}} = \boldsymbol{V}_{\bar{\boldsymbol{H}}}\boldsymbol{\Sigma}_{\bar{\boldsymbol{x}}}\boldsymbol{V}^*_{\bar{\boldsymbol{H}}} \quad , \quad \tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{z}}} = \boldsymbol{U}_{\bar{\boldsymbol{H}}}\boldsymbol{\Sigma}_{\bar{\boldsymbol{z}}}\boldsymbol{U}^*_{\bar{\boldsymbol{H}}}\,, \tag{6.31}$$

meaning that the transmitter should beamform the information carrying signal along the directions corresponding to the right singular vectors of the channels, whereas the attacker should distribute the jamming power along the left singular vectors of the channel. With such covariance matrices, it is easy too notice that the whole system becomes equivalent to the parallel of Gaussian channels with SNRs determined by the values in the diagonal matrices $\boldsymbol{\Sigma}_{\bar{\boldsymbol{H}}}$, $\boldsymbol{\Sigma}_{\bar{\boldsymbol{x}}}$ and $\boldsymbol{\Sigma}_{\bar{\boldsymbol{z}}}$.

Observe that since we have relaxed the constraint for $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}}$, the optimal solution (6.29) to the relaxed problem will in general yield a value of the payoff function that is lower than or equal to the solution to the original problem. However, if the saddle point (6.31) also

satisfies the constraint (6.28), then it coincides with the solution for the original problem. It is clear that if E_{J} is very high, the feasible region for the original problem will be large and the two solutions will be more likely to coincide. Therefore, we call the solution of the relaxed problem the "high-JNR" solution. In Section 6.3 we will characterize the thresholds on the JNR for which the solution is feasible.

6.2.1 AWGN channel case

We start by considering the simple case in which both channels from the transmitter and the adversary towards the receiver are AWGN channels.

Under this assumption, it is possible to show that the energy matrices for the NS system are all equal to the identity matrix, $\boldsymbol{E}_{\boldsymbol{\gamma}} = \boldsymbol{E}_{\boldsymbol{\varphi}} = \boldsymbol{E}_{\boldsymbol{\varphi}'} = \boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}} = \boldsymbol{I}$, and consequently $\bar{\boldsymbol{H}} = \boldsymbol{I}$ and $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} = 2N_0\boldsymbol{I}$. Hence, the payoff at the saddle point for the NS system over AWGN channels is

$$f(\tilde{\boldsymbol{K}}^{\star}_{\tilde{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}^{\star}_{\tilde{\boldsymbol{z}}}) = LM\log(1+\Lambda), \tag{6.32}$$

with SJNR given by

$$\Lambda = \frac{E_{\mathsf{T}}}{E_{\mathsf{J}} + 2N_0ML}, \tag{6.33}$$

that is the ratio between the available energy at the transmitter and the sum of the available energy of the jammer plus the energy of the receiver thermal noise. The saddle point solution is exactly the capacity of ML parallel Gaussian channels with SNR, equal to Λ and the Nash equilibrium is reached by independent, uniform power allocation for both the transmitter and the attacker

$$\boldsymbol{K}^{\star}_{\tilde{\boldsymbol{x}}} = \tilde{\boldsymbol{K}}^{\star}_{\tilde{\boldsymbol{x}}} = \frac{E_{\mathsf{T}}}{ML}\boldsymbol{I} \quad , \quad \boldsymbol{K}^{\star}_{\tilde{\boldsymbol{z}}} = \tilde{\boldsymbol{K}}^{\star}_{\tilde{\boldsymbol{z}}} = \left(\frac{E_{\mathsf{J}}}{ML} + 2N_0\right)\boldsymbol{I}. \tag{6.34}$$

When CS transmission is adopted, instead, even if the channels are AWGN, ISI does arise, as the CS transmission/reception filters do not comply with the Nyquist criterion. Although this system can not be modeled as parallel Gaussian channels, we can show that the CS architecture yields the same saddle point reached by the NS modulation. In fact, the energy matrices of the transmitter and receiver filters are not diagonal but they are given by $\boldsymbol{E}_{\boldsymbol{\gamma}} = \boldsymbol{E}_{\boldsymbol{\varphi}} = \boldsymbol{E}_{\boldsymbol{\varphi}'} = \boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}} = \boldsymbol{E}_{\mathsf{CS}}$, where the positive semidefinite matrix $\boldsymbol{E}_{\mathsf{CS}}$ can be compactly written in terms of the Kronecker product as

$$\boldsymbol{E}_{\mathsf{CS}} = \boldsymbol{E}_L \otimes \boldsymbol{I}_M, \tag{6.35}$$

with the general entry for $\boldsymbol{E}_L$ being

$$(E_L)_{k,n} = \mathrm{ircos}\left(\rho, \frac{k-n}{1+\rho}\right) \quad , \quad k,n = 1,\ldots,L \tag{6.36}$$

and

$$\mathrm{ircos}(\rho, x) = \mathrm{sinc}(x)\frac{\pi}{4}[\mathrm{sinc}(\rho x + 1/2) + \mathrm{sinc}(\rho x - 1/2)]$$

being the inverse Fourier transform of the raised cosine pulse with roll-off factor ρ. Then, the equivalent MIMO channel matrix $\bar{\boldsymbol{H}}$ is still equal to the identity matrix, as

$$\bar{\boldsymbol{H}} = \boldsymbol{Q}\boldsymbol{P}^{-1} = \sqrt{\boldsymbol{E}_{\mathsf{CS}}^{-1}}\left(\sqrt{\boldsymbol{E}_{\mathsf{CS}}^{-1}\boldsymbol{E}_{\mathsf{CS}}\boldsymbol{E}_{\mathsf{CS}}^{-*}}\right)^{-1} = \boldsymbol{I}, \tag{6.37}$$

and also the noise covariance

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} = 2N_0\sqrt{\boldsymbol{E}_{\mathsf{CS}}^{-1}}\boldsymbol{E}_{\mathsf{CS}}\sqrt{\boldsymbol{E}_{\mathsf{CS}}^{-1}} = 2N_0\boldsymbol{I}. \tag{6.38}$$

Therefore, the CS system provides the same payoff value in (6.32) at the equilibrium, but the optimal covariance matrices for the transmitter and the jammer are now

$$\boldsymbol{K}_{\tilde{\boldsymbol{x}}}^{\star} = \frac{E_{\mathsf{T}}}{ML}\boldsymbol{E}_{\mathsf{CS}} \quad , \quad \boldsymbol{K}_{\tilde{\boldsymbol{z}}}^{\star} = \left(\frac{E_{\mathsf{J}}}{ML} + 2N_0\right)\boldsymbol{E}_{\mathsf{CS}}. \tag{6.39}$$

Under the assumption that the channels are not frequency selective, it is possible to also perform the analysis of the DMT systems. In particular, it is possible to compactly express the energy matrices also for the non-orthogonal families of waveforms of both the architectures; that is, the transmitter waveforms for CP, and the receiver waveforms for ZS. In the ZS case, we have

$$\boldsymbol{E}_{\boldsymbol{\varphi}} = \boldsymbol{E}_{\mathsf{ZS}} = \boldsymbol{I}_K \otimes \boldsymbol{E}_M, \tag{6.40}$$

in which the general entry of the matrix $\boldsymbol{E}_M$ is given by

$$(E_M)_{i,\ell} = \begin{cases} j\dfrac{1 - e^{j2\pi(m_\ell - m_i)\rho}}{2\pi(m_\ell - m_i)} & , \ i \neq \ell \\ 1+\rho & , \ i = \ell \end{cases} . \tag{6.41}$$

On the other hand, in the CP case, we have

$$\boldsymbol{E}_{\boldsymbol{\gamma}} = \boldsymbol{D}\boldsymbol{E}_{\mathsf{ZS}}\boldsymbol{D}^* \quad , \quad \boldsymbol{D} = \boldsymbol{I}_K \otimes \mathrm{diag}(e^{j2\pi m_i \rho})_{i=1,\ldots,M}, \tag{6.42}$$

Hence, for cyclic-prefix transmission it holds $\boldsymbol{P} = \sqrt{\boldsymbol{D}\boldsymbol{E}_{\mathsf{ZS}}\boldsymbol{D}^*}$ and $\boldsymbol{Q} = \boldsymbol{I}$, whereas, when the zero-padding suffix is implemented, we have $\boldsymbol{P} = \boldsymbol{I}$ and $\boldsymbol{Q} = \sqrt{\boldsymbol{E}_{\mathsf{ZS}}^{-1}}$. In both cases

system	$\boldsymbol{E}_{\gamma}$	$\boldsymbol{E}_{\varphi}$	$\boldsymbol{E}_{\gamma\varphi}$	$\boldsymbol{P}$	$\boldsymbol{Q}$
FMT/NS	$\boldsymbol{I}$	$\boldsymbol{I}$	$\boldsymbol{I}$	$\boldsymbol{I}$	$\boldsymbol{I}$
FMT/CS	$\boldsymbol{E}_{\mathsf{CS}}$	$\boldsymbol{E}_{\mathsf{CS}}$	$\boldsymbol{E}_{\mathsf{CS}}$	$\sqrt{\boldsymbol{E}_{\mathsf{CS}}^{-1}}$	$\sqrt{\boldsymbol{E}_{\mathsf{CS}}^{-1}}$
DMT/ZS	$\boldsymbol{I}$	$\boldsymbol{E}_{\mathsf{ZS}}$	$\boldsymbol{I}$	$\boldsymbol{I}$	$\sqrt{\boldsymbol{E}_{\mathsf{ZS}}^{-1}}$
DMT/CP	$\boldsymbol{D}\boldsymbol{E}_{\mathsf{ZS}}\boldsymbol{D}^{*}$	$\boldsymbol{I}$	$\boldsymbol{I}$	$\sqrt{\boldsymbol{D}\boldsymbol{E}_{\mathsf{ZS}}\boldsymbol{D}^{*}}$	$\boldsymbol{I}$

Table 6.1. *Waveform cross-energy matrices for different OFDM systems when both the transmission and jamming channels are AWGN (in this case $\boldsymbol{E}_{\varphi'} = \boldsymbol{E}_{\varphi}$ and $\boldsymbol{E}_{\gamma'\varphi} = \boldsymbol{E}_{\gamma\varphi}$).*

$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} = 2N_0\boldsymbol{I}$ and the eigenvalues of $\bar{\boldsymbol{H}}\bar{\boldsymbol{H}}^{*}$ are equal to the eigenvalues of $\boldsymbol{E}_{\mathsf{ZS}}^{-1}$. Then, the saddle point solution for both DMT architectures is given by

$$f(\tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{x}}}^{\star}, \tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{z}}}^{\star}) = \log|\boldsymbol{I} + \Lambda\boldsymbol{E}_{\mathsf{ZS}}^{-1}| \tag{6.43}$$

$$= L\sum_{i=1}^{M}\log\left(1 + \frac{1}{\lambda_i(\boldsymbol{E}_M)}\Lambda\right) \tag{6.44}$$

where $\{\lambda_i(\boldsymbol{E}_M)\}$ are the eigenvalues of $\boldsymbol{E}_M$. In Table 6.1 we summarize the cross-energy matrices of interest in the AWGN case.

A simplification of the result (6.44) can be obtained by considering the discrete-time model of DMT, with sampling frequency $F_0 = MF_{\mathsf{u}}$ and subcarrier central frequencis $f_i = m_iF_{\mathsf{u}}$, $i = 1, \ldots, M$. Then, the expression of $(E_M)_{i,\ell}$ changes from (6.41) to

$$(E_M)_{i,\ell} = \begin{cases} \dfrac{1 - e^{j2\pi(m_\ell - m_i)\rho}}{1 - e^{j2\pi(m_\ell - m_i)/M}} & , \ i \neq \ell \\ 1 + \rho & , \ i = \ell \end{cases} . \tag{6.45}$$

while (6.42) still holds. Then, it can be easily seen that $\boldsymbol{E}_M$ has only two distinct eigenvalues, $\lambda = 1$ with multiplicity $(1-\rho)M$ and $\lambda = 2$ with multiplicity ρM. So, for both DMT architectures, the saddle point for the AWGN transmission case can be written as[1]

$$f(\tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{x}}}^{\star}, \tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{z}}}^{\star}) = ML\left[(1-\rho)\log(1+\Lambda) + \rho\log(1+\Lambda/2)\right]. \tag{6.46}$$

which clearly shows the loss incurred for the system redundancy.

[1]The differences between (6.44) and (6.46) are due to the fact that the sampling frequency F_0 is smaller than the system bandwidth, strictly speaking. Hence, in this case, the discrete-time model is an approximation of the continuous-time one.

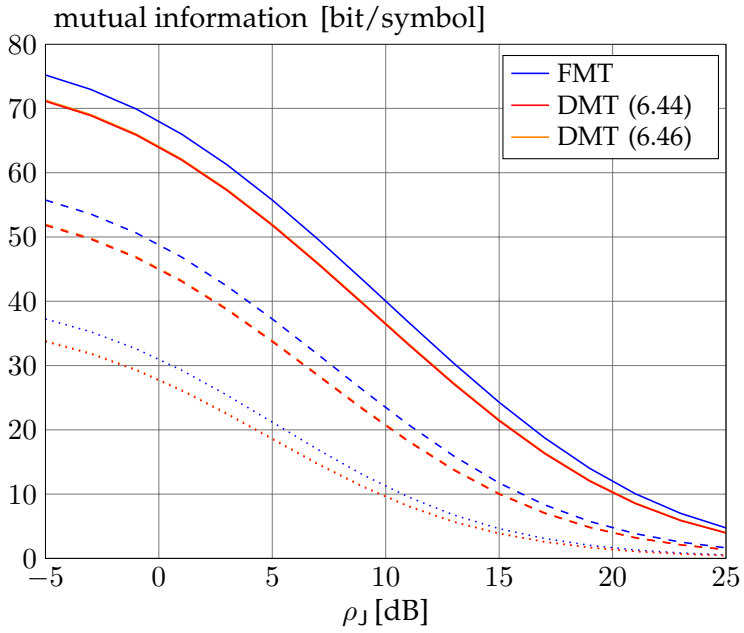

Figure 6.2. *Mutual information vs. JNR at the Nash equilibrium, for OFDM transmissions over AWGN channels. Results are reported for 3 different SNR values, $\rho_{\mathsf{T}} = 10\,dB$ (dotted lines), $\rho_{\mathsf{T}} = 15\,dB$ (dashed lines) and $\rho_{\mathsf{T}} = 20\,dB$ (solid lines). Curves obtained with the continuos time model (6.44) and with the discrete time approximation (6.46) overlap throughout the whole JNR range.*

6.2.2 FMT systems in channels with wide coherence band

The analysis of FMT systems is also tractable when both channels from the transmitter and the jammer are frequency selective, provided their coherence bandwidth is larger than the subcarrier spacing, that is if we assume

$$\begin{cases} G_{\mathsf{R}}(f) = G_{\mathsf{R}}(f_i) \\ |G_{\mathsf{J}}(f)|^2 = |G_{\mathsf{J}}(f_i)|^2 \end{cases} , \quad f \in \left[f_i - \frac{F_{\mathsf{u}}}{2}, f_i + \frac{F_{\mathsf{u}}}{2} \right] \tag{6.47}$$

Under the above assumptions, the energy matrices in the NS system are diagonal that is by letting $\boldsymbol{E}_{\boldsymbol{\gamma}} = \boldsymbol{E}_{\boldsymbol{\varphi}} = \boldsymbol{I}$, $\boldsymbol{E}_{\boldsymbol{\varphi}'} = \boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^*$ and $\boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}} = \boldsymbol{D}_{\mathsf{R}}$, with $\boldsymbol{D}_{\mathsf{R}} = \boldsymbol{I}_K \otimes \mathrm{diag}\{G_{\mathsf{R}}(f_i)\}$ and $\boldsymbol{D}_{\mathsf{J}} = \boldsymbol{I}_K \otimes \mathrm{diag}\{G_{\mathsf{J}}(f_i)\}$. Then, it is straightforward to write

$$\boldsymbol{P} = (\boldsymbol{D}_{\mathsf{R}}\boldsymbol{D}_{\mathsf{R}}^*)^{-1/2}, \boldsymbol{Q} = (\boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^*)^{-1/2} \tag{6.48}$$

$$\tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{w}}} = 2N_0(\boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^*)^{-1}, \bar{\boldsymbol{H}} = (\boldsymbol{D}_{\mathsf{R}}\boldsymbol{D}_{\mathsf{R}}^*)^{1/2}(\boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^*)^{-1/2}. \tag{6.49}$$

Then, the system is equivalent to ML parallel channels and the saddle point solution writes

$$f(\boldsymbol{K}_{\tilde{\boldsymbol{x}}}^\star, \boldsymbol{K}_{\tilde{\boldsymbol{z}}}^\star) = f(\tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{x}}}^\star, \tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{z}}}^\star) = L\sum_{i=1}^{M} \log\left(1 + \Lambda \frac{|G_{\mathsf{R}}(f_i)|^2}{|G_{\mathsf{J}}(f_i)|^2}\right) \tag{6.50}$$

with

$$\Lambda = \frac{E_{\mathsf{T}}}{E_{\mathsf{J}} + 2N_0 L \sum_{i=1}^{M} 1/|G_{\mathsf{J}}(f_i)|^2}. \tag{6.51}$$

Now, we show that the result in (6.50) holds also for CS modulation. In this case, as noticed in Section 6.2.1, the transmit pulses corresponding to different OFDM symbols are not perfectly orthogonal, hence ISI does arise and the energy matrices of the transmitter and receiver filters are not diagonal, but they are given by $\boldsymbol{E}_{\boldsymbol{\gamma}} = \boldsymbol{E}_{\boldsymbol{\varphi}} = \boldsymbol{E}_{\mathsf{CS}}$. Nevertheless, if the coherence bandwidth assumptions (6.47) hold, it is possible to write $\boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}} = \boldsymbol{D}_{\mathsf{R}}\boldsymbol{E}_{\mathsf{CS}} = \boldsymbol{E}_{\mathsf{CS}}\boldsymbol{D}_{\mathsf{R}}$. Moreover, $\boldsymbol{E}_{\boldsymbol{\varphi}'} = \boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^{*}\boldsymbol{E}_{\mathsf{CS}} = \boldsymbol{E}_{\mathsf{CS}}\boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^{*}$ and the equivalent MIMO channel appearing in the payoff function (6.26) is

$$\begin{aligned}
\bar{\boldsymbol{H}} &= \sqrt{\boldsymbol{E}_{\boldsymbol{\varphi}'}^{-1}(\boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}}^{-1}\boldsymbol{E}_{\boldsymbol{\gamma}}\boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}}^{-*})^{-1}} && (6.52)\\
&= \sqrt{\boldsymbol{E}_{\boldsymbol{\varphi}'}^{-1}\boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}}^{*}\boldsymbol{E}_{\boldsymbol{\gamma}}^{-1}\boldsymbol{E}_{\boldsymbol{\gamma}'\boldsymbol{\varphi}}} && (6.53)\\
&= \sqrt{(\boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^{*})^{-1}\boldsymbol{E}_{\mathsf{CS}}^{-1}\boldsymbol{E}_{\mathsf{CS}}^{*}\boldsymbol{D}_{\mathsf{R}}^{*}\boldsymbol{E}_{\mathsf{CS}}^{-1}\boldsymbol{E}_{\mathsf{CS}}\boldsymbol{D}_{\mathsf{R}}} && (6.54)\\
&= \sqrt{(\boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^{*})^{-1}\boldsymbol{D}_{\mathsf{R}}^{*}\boldsymbol{D}_{\mathsf{R}}} && (6.55)
\end{aligned}$$

as for the NS case. Also the energy constraints (6.27) and (6.28) remain unchanged, since

$$\begin{aligned}
\operatorname{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}) &= 2N_0 \operatorname{tr}(\boldsymbol{Q}\boldsymbol{E}_{\boldsymbol{\varphi}}\boldsymbol{Q}) = 2N_0 \operatorname{tr}(\boldsymbol{Q}\boldsymbol{Q}\boldsymbol{E}_{\boldsymbol{\varphi}}) && (6.56)\\
&= 2N_0 \operatorname{tr}(\boldsymbol{E}_{\boldsymbol{\varphi}'}^{-1}\boldsymbol{E}_{\boldsymbol{\varphi}}) = 2N_0 \operatorname{tr}((\boldsymbol{D}_{\mathsf{J}}\boldsymbol{D}_{\mathsf{J}}^{*})^{-1}\boldsymbol{E}_{\mathsf{CS}}^{-1}\boldsymbol{E}_{\mathsf{CS}}) && (6.57)\\
&= 2N_0 L \sum_{i=1}^{M} \frac{1}{|G_{\mathsf{J}}(f_i)|^2}, && (6.58)
\end{aligned}$$

and thus, the payoff at the saddle point is the same for both the FMT architectures.

6.3 Thresholds for the high-JNR regime

In this section we seek how to determine, for given channels, the minimum value of ρ_{J} at which the high-JNR regime saddle point is feasible. We del with FMT and DMT systems separately.

6.3.1 FMT systems

As stated in Section 6.2.2, under the coherence bandwidth assumptions, the NS system is equivalent to ML parallel channels. In this case, with reference to the saddle point solutions (6.31), we have that $\boldsymbol{U}_{\bar{\boldsymbol{H}}} = \boldsymbol{V}_{\bar{\boldsymbol{H}}} = \boldsymbol{I}$, and the optimal covariance matrices are diagonal

$$(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}^{\star}, \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{z}}}^{\star}) = (\boldsymbol{\Sigma}_{\bar{\boldsymbol{x}}}, \boldsymbol{\Sigma}_{\bar{\boldsymbol{z}}}). \tag{6.59}$$

The optimal power allocation strategies, that is, the entries of $\mathbf{\Sigma}_{\bar{\boldsymbol{x}}} = \mathrm{diag}\{\sigma_{x,i}\}$ and $\mathbf{\Sigma}_{\bar{\boldsymbol{z}}} = \mathrm{diag}\{\sigma_{z,i}\}$, can be derived from the results in [96] about the optimal power allocation for the jamming game over parallel Gaussian channels. We denote with $h_i = \lambda_i(\bar{\boldsymbol{H}}\bar{\boldsymbol{H}}^*)$ the diagonal elements (eigenvalues) of the matrix $\bar{\boldsymbol{H}}\bar{\boldsymbol{H}}^*$ and we use the symbol $\tilde{w}_\ell = \lambda_\ell(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}})/(2N_0)$ to denote the diagonal entries of $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}$ normalized over the thermal noise PSD $2N_0$. Then, the application of [96, Lemma 1] [98] yields

$$\sigma_{x,i} = \frac{h_i}{\lambda(h_i + \lambda/\nu)} \tag{6.60}$$

$$\sigma_{z,i} = \frac{h_i}{\nu(h_i + \lambda/\nu)}, \tag{6.61}$$

in which the constants $\lambda, \nu \geq 0$ are chosen in order to satisfy the energy constraints

$$\sum_{i=1}^{ML} \sigma_{x,i} \leq E_{\mathsf{T}} \tag{6.62}$$

$$\sum_{i=1}^{ML} \sigma_{z,i} \leq E_{\mathsf{J}} + 2N_0 \sum_{\ell=1}^{ML} \tilde{w}_\ell. \tag{6.63}$$

Then, we obtain

$$\frac{\nu}{\lambda} = \Lambda = \frac{E_{\mathsf{T}}}{E_{\mathsf{J}} + 2N_0 \sum_\ell \tilde{w}_\ell} \tag{6.64}$$

and

$$\nu = \frac{\sum_i \frac{h_i}{h_i + 1/\Lambda}}{E_{\mathsf{J}} + 2N_0 \sum_\ell \tilde{w}_\ell} \tag{6.65}$$

Hence, (6.61) gives a feasible solution when all the elements of the corresponding diagonal matrix $\boldsymbol{K}_{\bar{\boldsymbol{s}}}^\star$ are non negative, that is when

$$\frac{1}{\tilde{w}_i}\sigma_{z,i} - 2N_0 > 0, \ \forall i. \tag{6.66}$$

It is straightforward to show that the conditions in (6.66) are equivalent to impose $c_i(\rho_{\mathsf{J}}, \rho_{\mathsf{T}}) > 0, \ \forall i$, where

$$c_i(\rho_{\mathsf{J}}, \rho_{\mathsf{T}}) = \rho_{\mathsf{J}} - 2\tilde{w}_i \sum_{k=1}^{LM} \frac{1 + \frac{\rho_{\mathsf{J}} + 2\sum_\ell \tilde{w}_\ell}{\rho_{\mathsf{T}} h_i}}{1 + \frac{\rho_{\mathsf{J}} + 2\sum_\ell \tilde{w}_\ell}{\rho_{\mathsf{T}} h_k}} + 2\sum_\ell \tilde{w}_\ell. \tag{6.67}$$

From the analysis of this constraint we can retrieve a condition on the available JNR at the jammer that is necessary to guarantee the feasibility of this solution in both the low and high-SNR regimes. Namely, when $\rho_{\mathsf{T}} \to 0$, it must be

$$\rho_{\mathsf{J}} > \max_i \left\{ 2\frac{\tilde{w}_i}{h_i} \sum_k h_k - 2\sum_\ell \tilde{w}_\ell \right\}, \tag{6.68}$$

(the threshold depends on the subcarrier of the main channel with maximal attenuation $\max \tilde{w}_i/h_i = \max 1/|G_{\mathsf{R}}(f_i)|^2$) whereas, for $\rho_{\mathsf{T}} \to \infty$, the condition writes

$$\rho_{\mathsf{J}} > \max_i \left\{ 2LM\tilde{w}_i - 2\sum_{\ell} \tilde{w}_\ell \right\}. \tag{6.69}$$

(the threshold depends on the subcarrier of the jammer channel with maximal attenuation $\max \tilde{w}_i = \max 1/|G_{\mathsf{J}}(f_i)|^2$). In Figure 6.3 we show the threshold on the JNR as a function of the SNR ρ_{T} for a single channel realization. The values of the threshold in the intermediate SNR regime are numerically evaluated starting from (6.67).

Now, we show that this threshold on the JNR is the same for the CS system. In Section 6.2.2, we have shown that both FMT architectures share the same expression for the matrices $\bar{\boldsymbol{H}}$, $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}$ and the trace constraints (6.27), (6.28). Hence they share the same minimax solution covariance matrices $(\tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{z}}})$, that are therefore diagonal also for the CS case and whose elements are obtained from equations (6.60) and (6.61). Then, the corresponding optimal covariance matrix for the jamming signal is $\boldsymbol{K}^{\star}_{\bar{\boldsymbol{s}}} = \boldsymbol{Q}^{-1}\tilde{K}^{\star}_{\bar{\boldsymbol{s}}}\boldsymbol{Q}^{-1} = \boldsymbol{Q}^{-1}(\tilde{K}^{\star}_{\bar{\boldsymbol{z}}} - \tilde{K}_{\bar{\boldsymbol{w}}})\boldsymbol{Q}^{-1}$. Then, it is easy to observe that the optimal jammer covariance matrix for the CS system is positive semidefinite if and only if the corresponding matrix of the NS case is positive semidefinite as well, as the matrix $\boldsymbol{Q}$ is positive semidefinite.

6.3.2 DMT systems

For the case of transmission with a DMT system, the conditions that guarantee the feasibility of the high-JNR solution are more complicated to express and must be computed numerically. We recall that the equivalent jammer covariance matrix $\tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{z}}}$ is optimally beamformed along the left singular vectors of the channels $\bar{\boldsymbol{H}}$ and the corresponding transmitter covariance matrix $\tilde{\boldsymbol{K}}^{\star}_{\bar{\boldsymbol{x}}}$ along the right singular vectors of $\bar{\boldsymbol{H}}$. This way, the system is reduced to the parallel of LM orthogonal channels, for which the optimal power allocation strategies are given again by (6.60) and (6.61) with h_i being the i-th element of the main diagonal of $\boldsymbol{\Sigma}_{\bar{\boldsymbol{H}}}$. Then, the condition on the positive semidefinite nature of $\boldsymbol{K}^{\star}_{\bar{\boldsymbol{s}}}$ is numerically checked by expressing this matrix as

$$\boldsymbol{K}^{\star}_{\bar{\boldsymbol{s}}} = \boldsymbol{Q}^{-1}\boldsymbol{U}_{\bar{\boldsymbol{H}}}\boldsymbol{\Sigma}_{\bar{\boldsymbol{z}}}\boldsymbol{U}^{*}_{\bar{\boldsymbol{H}}}\boldsymbol{Q}^{-1} - 2N_0\boldsymbol{E}_{\boldsymbol{\varphi}}. \tag{6.70}$$

The JNR threshold is then evaluated numerically with a binary search method, and is illustrated in Figure 6.3 as a function of the SNR

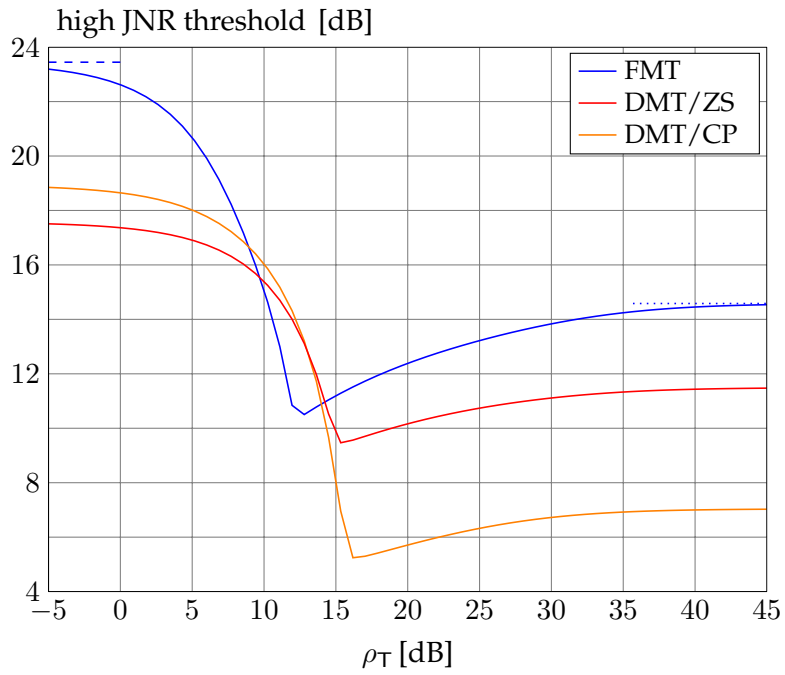

Figure 6.3. *High JNR thresholds on ρ_J for the different OFDM architectures. The threshold limits for FMT given in (6.68) and (6.69) are shown in dashed and dotted blue lines, respectively.*

6.4 General solution

In this case, the matrix $\tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{w}}}$ is fixed and determined by the system, and the jammer can operate only on $\tilde{\boldsymbol{K}}_{\tilde{\boldsymbol{s}}}$ in order to disrupt the communication performance. When the power available to the jammer is limited, and the saddle point solution in Section 6.2 is not feasible, it is still possible to find the optimal jamming strategy for the case when FMT transmission is implemented. For the DMT system we will propose an efficient jamming scheme that is shown to converge to the optimal solution when the JNR enters the feasibility region described in the previous section.

6.4.1 FMT systems in channels with wide coherence band

We start considering the NS case. The parallel channel structure obtained under the coherence bandwidth assumptions can be leveraged to apply to this case the result on the optimal jamming and transmitter power allocation in [96, 98]. Since we want to handle the jamming signal separately and independently from the AWGN at the receiver, we express

the payoff function as

$$f(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}) = \sum_{i=1}^{LM} \log\left(1 + \frac{h_i \sigma_{x,i}}{\sigma_{s,i} + 2N_0\tilde{w}_i}\right) \tag{6.71}$$

subject to the power constraints

$$\sum_i \sigma_{x,i} \leq E_{\mathsf{T}} \tag{6.72}$$

$$\sum_i \sigma_{s,i} \leq E_{\mathsf{J}}, \tag{6.73}$$

in which $\sigma_{x,i}, \sigma_{s,i}$ are the diagonal elements of the (diagonal) matrices $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}$, respectively. The optimal power allocations for the transmitter and the jammer are obtained from [96, Lemma 1], by substituting the noise PSD value with the corresponding element in $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}$, that is with the values $2N_0\tilde{w}_i$. Namely,

$$\sigma_{x,i} = \begin{cases} \left(\frac{1}{\lambda} - \frac{2N_0\tilde{w}_i}{h_i}\right)^+ & , \ h_i \leq \frac{2N_0\tilde{w}_i\lambda}{1-2N_0\tilde{w}_i\nu} \\ \frac{h_i}{\lambda(h_i + \lambda/\nu)} & , \ h_i > \frac{2N_0\tilde{w}_i\lambda}{1-2N_0\tilde{w}_i\nu} \end{cases} \tag{6.74}$$

$$\sigma_{s,i} = \begin{cases} 0 & , \ h_i \leq \frac{2N_0\tilde{w}_i\lambda}{1-2N_0\tilde{w}_i\nu} \\ \frac{h_i}{\nu(h_i + \lambda/\nu)} - 2N_0\tilde{w}_i & , \ h_i > \frac{2N_0\tilde{w}_i\lambda}{1-2N_0\tilde{w}_i\nu} \end{cases} \tag{6.75}$$

with $\lambda, \nu \geq 0$ such that the energy constraints (6.72) and (6.73) are verified.

For what we have seen in the previous sections, the CS system has the same saddle point solution $(\tilde{\boldsymbol{K}}^\star_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}^\star_{\bar{\boldsymbol{s}}})$ and the same payoff function. Moreover, the optimal covariance matrices for CS are obtained as usual as by multiplying the diagonal matrices $(\tilde{\boldsymbol{K}}^\star_{\bar{\boldsymbol{x}}}, \tilde{\boldsymbol{K}}^\star_{\bar{\boldsymbol{s}}})$ by the matrix $\boldsymbol{E}_{\mathsf{CS}}$.

6.4.2 DMT systems

In this case the system can not be modeled as parallel Gaussian channels, and we must rely on the general MIMO expression of the minimax problem (6.22). As explained in Section 6.2, the optimal strategy for the jammer would yield

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} + \tilde{\boldsymbol{K}}^\star_{\bar{\boldsymbol{s}}} = \boldsymbol{U}_{\bar{\boldsymbol{H}}} \boldsymbol{\Sigma}_{\bar{\boldsymbol{z}}} \boldsymbol{U}^*_{\bar{\boldsymbol{H}}}. \tag{6.76}$$

However, in the general case with finite JNR, the energy available at the jammer could be not sufficient to provide a total interference signal (jamming signal plus thermal noise) beamformed along the left singular vectors of the channel $\bar{\boldsymbol{H}}$. Nevertheless, we aim to provide a

jamming strategy that exploits the optimal directions as soon as the JNR enters the feasibility region of Section 6.3

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} = \hat{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} + \boldsymbol{\Delta}_{\bar{\boldsymbol{w}}} = \boldsymbol{U}_{\bar{\boldsymbol{H}}} \hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{w}}} \boldsymbol{U}_{\bar{\boldsymbol{H}}}^{*} + \boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}, \tag{6.77}$$

in which $\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{w}}} = \mathrm{diag}\{\hat{\sigma}_{w,i}\}$, with $\hat{\sigma}_{w,i} \geq 0$, for $i = 1, \ldots, LM$ and

$$\sum_{i=1}^{LM} \hat{\sigma}_{w,i} = \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}). \tag{6.78}$$

Therefore, $\mathrm{tr}(\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}) = 0$ and the Hermitian matrix $\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}$ represents the deviation of the noise covariance matrix from the optimal noise directions. Analogously, we constrain the jammer covariance matrix to be written as

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}} = \boldsymbol{U}_{\bar{\boldsymbol{H}}} \hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{s}}} \boldsymbol{U}_{\bar{\boldsymbol{H}}}^{*} + \boldsymbol{\Delta}_{\bar{\boldsymbol{s}}}, \tag{6.79}$$

in which $\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{s}}} = \mathrm{diag}\{\hat{\sigma}_{s,i}\}$, with $\hat{\sigma}_{s,i} \geq 0$, for $i = 1, \ldots, LM$. Moreover, we choose $\boldsymbol{\Delta}_{\bar{\boldsymbol{s}}}$ as

$$\boldsymbol{\Delta}_{\bar{\boldsymbol{s}}} = -\zeta \boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}, \tag{6.80}$$

with $\zeta \in [0, 1]$. Therefore, $\mathrm{tr}(\boldsymbol{\Delta}_{\bar{\boldsymbol{s}}}) = 0$ and we impose

$$\sum_{i=1}^{LM} \hat{\sigma}_{s,i} \leq E_{\mathsf{J}}. \tag{6.81}$$

The parameter ζ is chosen as the maximum value in $[0, 1]$ such that the corresponding matrix $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}$ is still positive semidefinite. The idea underlying this choice is to obtain the total interference covariance matrix

$$\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}} + \tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}} = \boldsymbol{U}_{\bar{\boldsymbol{H}}} (\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{w}}} + \hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{s}}}) \boldsymbol{U}_{\bar{\boldsymbol{H}}}^{*} + (1 - \zeta) \boldsymbol{\Delta}_{\bar{\boldsymbol{w}}} \tag{6.82}$$

in which the effect of the term $(1 - \zeta)\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}$ is reduced to the minimum, in order to distribute the jamming signal energy across the optimal directions determined by the matrix $\boldsymbol{U}_{\bar{\boldsymbol{H}}}$. In order to achieve this task, we define a two step optimization protocol that leads to the definition of the suitable $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}$ to be adopted by the attacker.

Decomposition of $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}$

The values of the matrix $\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{w}}}$, and the corresponding values of $\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}$ in (6.77), are choosen as the solution of the following optimization problem

$$\begin{aligned} \underset{\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{w}}}}{\text{maximize}} \quad & \zeta_0 = \frac{\min_i\{\hat{\sigma}_{s,i}\}}{\max_\ell\{\lambda_\ell(\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}})\}} \\ \text{subject to} \quad & \hat{\sigma}_{w,i} \geq 0,\ i = 1, \dots, LM, \\ & \hat{\sigma}_{s,i} \geq 0,\ i = 1, \dots, LM, \\ & \sum_i \hat{\sigma}_{w,i} = \mathrm{tr}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{w}}}) \\ & \sum_i \hat{\sigma}_{s,i} \leq E_{\mathsf{J}}. \end{aligned} \tag{6.83}$$

For each value of $\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{w}}}$ in (6.83), the corresponding elements in $\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{s}}}$ are computed according to the optimal power allocation[2] in (6.75), by substituting the terms $2N_0\tilde{w}_i$ with $\hat{\sigma}_{w,i}$.

Definition of ζ

The optimization problem in (6.83) provides the expressions for $\hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{w}}}, \hat{\boldsymbol{\Sigma}}_{\bar{\boldsymbol{s}}}$ and $\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}$. The last parameter to tune in the definition of the jamming strategy is ζ in (6.80). Again, ζ is defined as the solution of a maximization problem, that is numerically solved, and starts from the initial point

$$\zeta_0 = \frac{\min_i\{\hat{\sigma}_{s,i}\}}{\max_\ell\{\lambda_\ell(\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}})\}}. \tag{6.84}$$

On leveraging Weyl's Theorem (4.3.1) and the Corollary (6.3.4) in [84], we can state that

$$\lambda_{\min}(\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}) \geq \min_i\{\hat{\sigma}_{s,i}\} - \zeta\lambda_{\max}(\boldsymbol{\Delta}_{\bar{\boldsymbol{w}}}), \tag{6.85}$$

hence, on choosing $\zeta = \zeta_0$, the corresponding jamming covariance matrix is positive semidefinite and it represents a valid jamming strategy. On top of that, the actual value of ζ adopted by the jammer is further optimized, starting from ζ_0, as the highest value in $[0, 1]$ that provides a positive semidefinite $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}$. This last optimization is performed numerically via an iterative binary search algorithm.

Then, once the adopted $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{s}}}$ is chosen, the corresponding best $\tilde{\boldsymbol{K}}_{\bar{\boldsymbol{x}}}$ for the transmitter is chosen according to the waterfilling principle, as the solution yielding the highest mutual information given the channel, the noise and the jammer expressions.

[2]The optimal jamming power allocation must be computed jointly with the optimal transmitter power allocation (6.74).

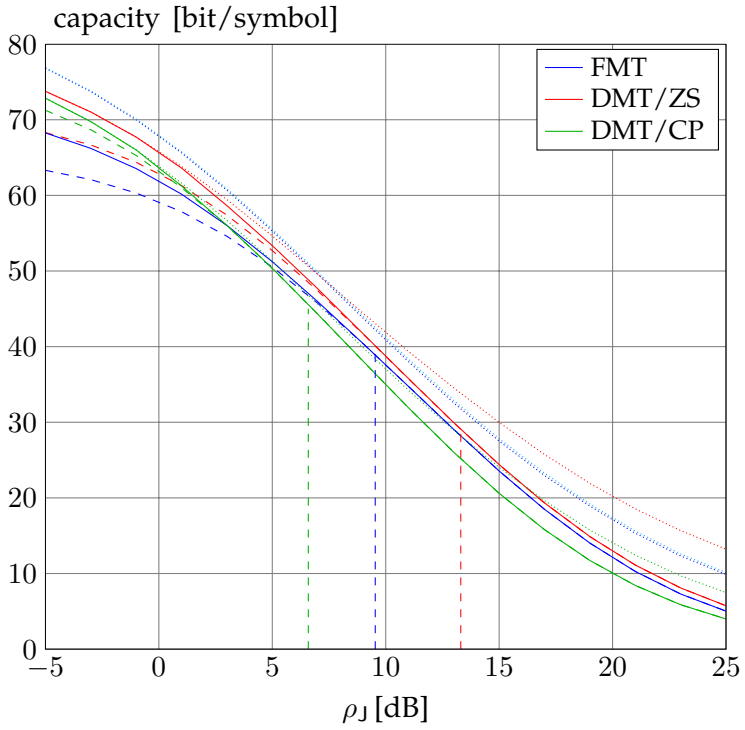

Figure 6.4. *Mutual information at the saddle point vs. JNR, for OFDM transmissions over a single realization of a Rayleigh fading channel for $\rho_T = 20\,dB$ (solid lines). The dashed lines indicate the solution obtained by relaxing the constraint (6.28) and the dashed vertical lines indicate the threshold on JNR beyond which the two solutions coincide. The dotted lines show the optimal solution obtained by the transmitter when the jammer chooses $\boldsymbol{v}$ with iid components, so that $\boldsymbol{K_r} = \sigma_r^2 \boldsymbol{I}$.*

Results for a single realization of a dispersive channel are plotted in Figure 6.4, where we can observe that the high-JNR solutions provide a sensibly lower result as ρ_J moves further back from the thresholds. It is also possible to appreciate the gain for the jammer to use the optimal strategy rather than a simple uniform power allocation across waveforms that are matched to the receiver ones.

Chapter 7

Conclusions

7.1 Contributions of this work

In this thesis, we have addressed different implementation issues for OFDM transmissions, aiming to improve performance of emerging and future wireless networks, by focusing on the two areas of advanced time and frequency synchronization methods (Part I) and physical layer security against passive and active attacks (Part II).

In Chapter 2, we have considered the problem of symbol synchronization for OFDM systems with guard interval shorter than the channel delay spread, that, hence, yield high spectral efficiency. We have identified as the aim of symbol synchronization for this scenario that of maximizing the global SINR after demodulation for each channel realization and derived a practical synchronizer based on a transmitted training sequence. We have also been able to derive tight upper bounds to the performance of practical estimators; the proposed synchronization method is seen by simulation to approach the bounds much closer than existing solutions, both in SIR and SINR performance.

In Chapter 3, we have presented an ML and an LS algorithm to jointly and simultaneously estimate carrier and sampling frequency offsets in OFDM systems. Both algorithms are designed to suit the UWB MB-OFDM scheme specified by the ECMA-368 standard. Different versions are derived for the cases in which, at demodulation, the three carriers of a same FH band group are generated by different oscillators, by a single oscillator, and the case in which the same oscillator also drives the sampling clock, as the standard dictates for the transmitter. From the simulation results, the proposed ML estimator outperforms both the LS and the existing solutions in the literature for sampling frequency estimation in the low and medium SNR regime, and has a much wider acquisition range. On the other

hand, it provides suboptimal performance as regards carrier estimation when the sampling offset is small. On the contrary the LS estimator is seen to offer satisfactory performance only for high SNR values. In the single oscillator scenario, which seems the most practical to implement, the ML estimator is by far the best solution against large offsets.

In Part II, we have analyzed physical layer security methods, applied to OFDM-based transmissions. Chapter 4 has shown how the information theoretic limits on secret communications over multipath fading channels are affected by the adoption of OFDM transmission between the transmitter and the legitimate receiver. We have relaxed the conventional assumption that also the eavesdropper is forced to implement OFDM demodulation and we have quantified the secrecy loss caused by his use of a more sophisticated receiver. For all our results, the secrecy rates obtained within the OFDM scenarios have been compared with the performance of the frequency selective fading channel itself, when no constraints are imposed on the type of modulation adopted and the complexity on the devices used.

Then, in Chapter 5 we have investigated the problem of information-theoretic secret-key agreement over MIMO channels (of which OFDM can be seen as a particular case). Based on the closed-form expressions for secret-key capacity for the low-SNR and high-SNR regimes, as well as numerical results, we have shown that optimizing over the legitimate channel only, is an efficient input strategy to share randomness over a noisy MIMO wireless channel. This result allows us to partly circumvent the need for full CSI at the transmitter and hence provides a *semi-blind* solution to effectively distill secret keys when using MIMO and OFDM transmissions.

Finally, Chapter 6 has addressed the problem of robust transmission strategies against active attacks. We have considered the mutual information jamming game in the particular case of an OFDM system. We have derived the optimal strategies and the value of the payoff function at the saddle point that solves the minimax problem. In particular, we have given closed form expressions for the case in which the channels are AWGN, and a waterfill-like expression for dispersive channels with the FMT system, while for the DMT system in a dispersive channel we have devised a numerical solution.

7.2 Future directions

The results presented in this thesis could be extended along the following directions.

- *Joint time-frequency synchronization for high spectral efficiency OFDM*. The effectiveness

of the time synchronization algorithm presented in this work is sensibly lowered by the presence of residual frequency offsets. Cross-correlation methods specifically designed to cope with the very dispersive channel scenario could provide robust synchronization and a lower computational complexity. Moreover, as emerged from the analysis of existing cross-correlation algorithms, their performance loss in the low-SNR regime has been shown to have negligible detrimental effects, when an overall performance metric, like the receiver SINR, is taken into account. A further step in the optimization of OFDM receivers would be represented by the definition of a joint time and frequency synchronization algorithm, specifically tailored also for channels with delay spread longer than the guard interval.

- *Practical transmission schemes for the OFDM wiretap channel.* The fundamental limits derived for secret transmissions with OFDM modulation have been obtained assuming a Gaussian distributed input. It seems appropriate to further investigate which secrecy performance is achievable within OFDM systems when the transmitted symbols belong to practical constellations (e.g., QPSK, QAM, etc.). The optimal trade-off between bit and power-loading over subcarriers could be investigated. Moreover, the design of practical coding strategies for the wiretap channel remains an open problem. A promising research line is represented by combining the code design with the constellation choice and power allocation optimization for multicarrier transmissions.
- *Practical secret-key agreement protocols for MIMO and OFDM transmissions.* The closed-form expressions of the secret-key capacity in the high-SNR and low-SNR regimes suggest that the complete characterization of secret-key rates for MIMO Gaussian channels could be more tractable than the corresponding description of the MIMO Gaussian wiretap channel secrecy capacity. Hence, a complete solution of this problem also at intermediate SNR regimes could be pursued. Moreover, it would be interesting to evaluate the impact on the fundamental limits described in this thesis due to the transmission of symbols taken from finite alphabets . Finally, the analysis of *information reconciliation* protocols that leverage the MIMO nature of transmission represents a promising tool to guarantee enhanced performance of key distillation strategies.
- *The jamming game in an OFDM setting under partial CSI.* In this area we have presented results obtained by assuming that all terminals have perfect knowledge of the channels, and that the jamming is uncorrelated with the information-bearing signal. As a future work, we could extend our analysis to the case where each player (transmit-

ter or jammer) has knowledge only on the state of his own channel. Subsequently, we could also aim to the case where the jammer can observe the transmitted signal through the channel that links the transmitter to the jammer himself, and choose a correlated jamming.

Bibliography

[1] R. W. Chang, "Synthesis of band-limited orthogonal signals for multichannel data transmissions," *The Bell System Technical Journal*, vol. 45, no. 10, pp. 1775–1796, Dec. 1966.

[2] S. B. Weinstein and P. M. Ebert, "Data transmission by frequency-division multiplexing using the discrete Fourier transform," *IEEE Trans. Commun. Technology*, vol. 19, no. 5, pp. 628–634, Oct. 1961.

[3] L. J. Cimini, "Analysis and performance evaluation of a digital mobile channel using orthogonal frequency division multiplexing," *IEEE Trans. Commun.*, vol. 28, no. 5, pp. 5–14, May 1990.

[4] J. A. C. Bingham, "Multicarrier modulation for data transmission: an idea whose time has come," *IEEE Trans. Commun.*, vol. 33, no. 7, pp. 665–675, Jul. 1985.

[5] *IEEE 802.11b - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE Standard Specifications Std., 1999.

[6] *IEEE 802.16 - Part 16: Air interface for fixed broadband wireless access systems*, IEEE Standard Specification Std., 2004.

[7] *3GPP TR 25.814, Physical Layer Aspects for Evolved UTRA, v.2.0.0*. 3GPP, 2006.

[8] H. Holma and A. Toskala, *LTE for UMTS OFDMA and SC-FDMA Based Radio Access*, Wiley, Ed., 2009.

[9] *Digital Video Broadcasting (DVB); Framing structure, channel coding and modulation for digital terrestrial television*, European Telecomm. Standards Inst. (ETSI) EN 300 744, Jun. 2004.

[10] *Digital Video Broadcasting (DVB); Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system (DVB-T2)*, European Telecomm. Standards Inst. (ETSI) EN 302 755, Sep. 2009.

[11] *High Rate Ultra Wideband PHY and MAC Standard*, 2nd ed., Standard ECMA-368, Dec. 2007.

[12] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[13] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[14] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - Part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[15] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

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

[17] T. Basar and Y.-W. Wu, "A complete characterization of minimax and maximin encoder-decoder policies for communication channels with incomplete statistical description," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 482–489, Apr. 1985.

[18] S. Ray, P. Moulin, and M. Medard, "On jamming in the wideband regime," in *Proc. IEEE Int'l Symp. Inform. Theory*, Seattle, WA, Jul. 2006.

[19] B. Muquet, Z. Wang, G. Giannakis, M. de Courville, and P. Duhamel, "Cyclic prefixing or zero padding for wireless multicarrier transmissions?" *IEEE Trans. Commun*, vol. 50, no. 12, pp. 2136–2148, Dec. 2002.

[20] G. Cherubini, E. Eleftheriou, and S. Olcer, "Filtered multitone modulation for very high-speed digital subscriber lines," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 5, pp. 1016 –1028, Jun. 2002.

[21] J. G. Proakis, *Digital Communications*, 3rd ed. New York: McGraw-Hill, 1995.

[22] N. Benvenuto, S. Tomasin, and L. Tomba, "Equalization methods in OFDM and FMT systems for broadband wireless communications," *IEEE Trans. Commun.*, vol. 50, no. 9, pp. 1413–1418, Sep. 2002.

[23] T. Keller and L. Hanzo, "OFDM synchronisation techniques for wireless LANs," in *Proc. IEEE PIMRC '96*, Taipei, Taiwan, Oct. 1996.

[24] J.-J. van de Beek, M. Sandell, and P. O. Börjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Trans. Sig. Proc.*, vol. 45, no. 7, pp. 1800–1805, Jul. 1997.

[25] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997.

[26] A. Fort, J.-W. Weijers, V. Derudder, W. Eberle, and A. Bourdoux, "A performance and complexity comparison of auto-correlation and cross-correlation for OFDM burst synchronization," in *Proc. IEEE ICASSP '03*, Honk Kong, Apr. 2003.

[27] Z. Ye, C. Duan, P. Orlik, and J. Zhang, "A low-complexity synchronization design for MB-OFDM ultra-wideband systems," in *Proc. IEEE ICC '08*, Beijing, China, May 2008.

[28] L. Hanzo, M. Münster, B. J. Choi, and T. Keller, *OFDM and MC-CDMA for Broadband Multi-user Communications, WLANs and Broadcasting*. John Wiley & Sons, Chichester, 2003.

[29] H. Steendam and M. Moeneclaey, "Analysis and optimization of the performance of OFDM on frequency-selective time-selective fading channels," *IEEE Trans. Commun.*, vol. 47, no. 12, pp. 1811–1819, Dec. 1999.

[30] A. F. Molisch *et al.*, "A comprehensive standardized model for Ultrawideband propagation channels," *IEEE Trans. Antennas Prop.*, vol. 54, no. 11-1, pp. 3151–3166, 2006.

[31] M. Batariere, K. Baum, and T. P. Krauss, "Cyclic prefix length analysis for 4G OFDM systems," in *Proc. IEEE VTC '04-Fall*, Los Angeles, CA, Sep. 2004.

[32] S. Celebi, "Interblock interference (IBI) and time of reference (TOR) computation in OFDM systems," *IEEE Trans. Commun.*, vol. 49, no. 11, pp. 1895–1900, Nov. 2001.

[33] B. S. Krongold, "A method for minimum interference OFDM time synchronization," in *Proc. IEEE SPAWC '03*, Rome, Italy, Jun. 2003.

[34] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*. Artech House, Boston, 2000.

[35] F. Tufvesson, O. Edfors, and M. Faulkner, "Time and frequency synchronization for OFDM using PN-sequence preambles," in *Proc. IEEE VTC '99-Fall*, Amsterdam, The Netherlands, Sep. 1999.

[36] L. Hàzy and M. El-Tanany, "Synchronization of OFDM systems over frequency selective fading channels," in *Proc. IEEE VTC '97*, Phoenix, AZ, May 1997.

[37] S. H. Muller-Weinfurtner, "On the optimality of metrics for coarse frame synchronization in OFDM: a comparison," in *Proc. IEEE PIMRC '98*, Boston, MA, Sep. 1998.

[38] P. H. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. Commun.*, vol. 42, no. 10, pp. 2908–2914, Oct. 1994.

[39] M. Morelli and U. Mengali, "An improved frequency offset estimator for OFDM applications," *IEEE Commun. Lett.*, vol. 3, no. 3, pp. 365–369, Mar. 1999.

[40] H. Bolcskei, "Blind estimation of symbol timing and carrier frequency offset in wireless OFDM systems," *IEEE Trans. Commun.*, vol. 49, no. 6, Jun. 2001.

[41] N. Laurenti, "Implementation issues in OFDM systems," Ph.D. dissertation, Univ. of Padova, Padova, Italy, Feb. 1999. [Online]. Available: http://www.dei.unipd.it/~nil/PDF/Thesis.pdf

[42] J. P. H. Roh, K. Cheun, "An MMSE fine carrier frequency synchronization algorithm for OFDM systems," *IEEE Trans. Consum. Electron.*, vol. 43, no. 3, pp. 761–766, Aug. 1997.

[43] C. W. Yak, Z. Lei, and T. T. Tjhung, "Maximum likelihood frequency offset estimation & Cramer-Rao bound for ultra-wideband (UWB) multi-band OFDM systems," in *Proc. IEEE Veh. Tech. Conf., VTC'06-Spring*, Melbourne, Australia, May 2006.

[44] Y. Li, T. Jacobs, and H. Minn, "Frequency offset estimation for MB-OFDM-based uwb systems," in *Proc. IEEE Int. Conf. Commun., ICC'06*, Istanbul, Turkey, Jun. 2006.

[45] T. M. Schmidl and D. C. Cox, "Low-overhead, low-complexity [burst] synchronization for OFDM," in *Proc. IEEE Int. Conf. Commun., ICC'96*, Dallas, USA, Jun. 1996.

[46] K.-B. Png, X. Peng, and H. F. T. Chin, "Two-dimensional iterative sampling frequency offset estimation for MB-OFDM system," in *Proc. IEEE Veh. Tech. Conf., VTC'06-Spring*, Melbourne, Australia, May 2006.

[47] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Englewood Cliffs: Prentice-Hall, 1993.

[48] P. C. Sapiano and J. D. Martin, "Statistical performance of the first order phase difference digital instantaneous frequency estimator," *IEE Electronics Letters*, vol. 32, no. 18, pp. 1657–1658, Aug. 1996.

[49] D. H. Bailey and P. N. Swarztrauber, "The fractional Fourier transform and applications," *SIAM Review*, vol. 33, no. 3, pp. 389–404, Sep. 1991.

[50] R. S. Owor, K. Dajani, Z. Okonkwo, and J. Hamilton, "An elliptical cryptographic algorithm for RF wireless devices," in *Proc. Winter Simulation Conference*, Washington, DC, Dec. 2007.

[51] D. Reilly and G. Kanter, "Noise-enhanced encryption for physical layer security in an OFDM radio," in *Proc. IEEE Radio and Wireless Symposium*, San Diego, CA, Jan. 2009.

[52] W.-J. Lin and J.-C. Yen, "An integrating channel coding and cryptography design for OFDM based WLANs," in *Proc. IEEE Int'l Symp. Consumer Electronics*, Kyoto, Japan, May 2009.

[53] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 29, pp. 656–715, 1949.

[54] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jun. 1978.

[55] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[56] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Proc. 44th Annual Allerton Conf. Commun., Contr., Computing*, Monticello, IL, Sep. 2006.

[57] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[58] R. Negi and S. Goel, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[59] R. Bustin, R. Liu, H. V. Poor, and S. Shamai (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, article ID 370970, 8 pages.

[60] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "Multiple-input multiple-output Gaussian broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[61] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas-II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[62] M. C. Gursoy, "Secure communication in the low-SNR regime: A characterization of the energy-secrecy tradeoff," in *Proc. IEEE Int'l Symp. Inform. Theory*, Seoul Korea, Jun. 2009.

[63] E. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *Proc. International Workshop on Multiple Access Communications (MACOM)*, St. Petersbutg, Russia, Jun. 2008.

[64] E. Jorswieck and S. Gerbracht, "Secrecy rate region of downlink OFDM systems: efficient resource allocation," in *Proc. of 14th International OFDM-Workshop (InOWo)*, Hamburg, Germany, Sep. 2009.

[65] M. R. D. Rodrigues and P. D. M. Almeida, "Filter design with secrecy constraints: The degraded parallel Gaussian wiretap channel," in *Proc. IEEE GLOBECOM*, New Orleans, LO, Dec. 2008.

[66] G. R. Tsouri and D. Wulich, "Securing OFDM over wireless time-varying channels using subcarrier overloading with joint signal constellations," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, article ID 437824, 18 pages.

[67] M. Kobayashi, M. Debbah, and S. Shamai (Shitz), "Secured communication over frequency-selective fading channels: A practical Vandermonde precoding," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, article ID 386547, 19 pages.

[68] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[69] A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channnel," in *Proc. IEEE Int'l Symp. Inform. Theory*, Nice, France, Jun. 2007.

[70] R. M. Gray, *Toeplitz and Circulant Matrices: A Review*. Dordrecht, The Netherlands: Now Publishers, 2006.

[71] A. V. Oppenheim and R. W. Schafer, *Discrete-Time Signal Processing*. Englewood Cliffs, NJ: Prentice Hall, 1989.

[72] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int'l Symp. Inform. Theory*, Seattle, WA, Jul. 2006.

[73] S. Bochner, *Lectures on Fourier Integrals*. Princeton, NJ: Princeton University Press, 1959.

[74] A. A. Gohari and V. Anantharan, "Information-theoretic key agreement of multiple terminals - Part I," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3973–3996, Aug. 2010.

[75] ——, "Information-theoretic key agreement of multiple terminals - Part II: Channel model," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3997–4010, Aug. 2010.

[76] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum distributed gaussian key," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 2004.

[77] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J. M. Merolla, "LDPC-based Gaussian key reconciliation," in *Proc. IEEE Information Theory Workshop*, Punta del Este, Uruguay, Mar. 2006.

[78] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int'l Symp. Inform. Theory*, Seattle, WA, Jul. 2006.

[79] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast-fading MIMO wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, article ID 506973, 17 pages.

[80] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[81] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, November 1995.

[82] U. M. Maurer and S. Wolf, "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free," in *Advances in Cryptology - Eurocrypt 2000*, Lecture Notes in Computer Science. B. Preneel, 2000, p. 351.

[83] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology - Eurocrypt '93*, Lecture Notes in Computer Science. Springer-Verlag, 1993, pp. 411–423.

[84] R. Horn and C. Johnson, *Matrix Analysis*. Cambridge, UK: Cambridge University Press, 1985.

[85] A. Khisti and G. W. Wornell, "The MIMOME channel," in *Proc. 45th Annual Allerton Conf. Commun., Contr., Computing*, Monticello, IL, Sep. 2007.

[86] F. E. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *CoRR*, vol. abs/0710.1920, 2007. [Online]. Available: http://arxiv.org/abs/0710.1920.

[87] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley-Interscience, 2006.

[88] D. P. Palomar and S. Verdú, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 141–154, Jan. 2006.

[89] A. Bayesteh, M. Ansari, and A. K. Khandani, "Effect of jamming on the capacity of MIMO channels," in *Proc. 42nd Annual Allerton Conf. Commun., Contr., Computing*, Monticello, IL, Sep. 2004.

[90] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 9, pp. 2119–2123, Sep. 2004.

[91] E. A. Jorswieck, H. Boche, and M. Weckerle, "Optimal transmitter and jamming strategies in Gaussian MIMO channels," in *IEEE Vehicular Technology Conference, VTC-Spring*, Stockholm, Sweden, May 2005.

[92] G. T. Amariucai and S. Wei, "Jamming games in fast-fading wireless channels," in *Proc. IEEE GLOBECOM*, New Orleans, LO, Dec. 2008.

[93] ——, "Jamming in fixed-rate wireless systems with power constraints - part I: Fast fading channels," August 2008. [Online]. Available: http://uk.arxiv.org/abs/0808.3431v1.

[94] A. Best and B. Natarajan, "The effect of jamming on the performance of carrier interferometry/OFDM," in *IEEE Int'l Conf. on Wireless And Mobile Computing, Networking And Communications, WiMob*, Montreal, Canada, Aug. 2005.

[95] F. Block, "Comparison of jamming robustness of airborne networking waveforms," in *Proc. of IEEE Military Communications Conference (MILCOM 2005)*, Atlantic City, NJ, Oct. 2005.

[96] S. Wei and R. Kannan, "Jamming and counter-measure strategies in parallel Gaussian fading channels with channel state information," in *Proc. of IEEE Military Communications Conference (MILCOM 2008)*, San Diego, CA, Nov. 2008.

[97] E. Jorswieck, *Unified approach for optimization of single-user and multi-user multiple-input multiple-output wireless systems*, Ph.D. thesis, Technische Universistät Berlin, Sep. 2004.

[98] S. Shafiee and S. Ulukus, "Correlated jamming in multiple access channels," in *Proc. Conference on Information Sciences and Systems*, Princeton, NJ, Mar. 2005.

Acknowledgments

I wish to thank Prof. Nicola Laurenti for his patient guidance and the amazing ability in stimulating my enthusiasm and my curiosity with original observations. I also had the privilege and luck to collaborate with prestigious Universities and highly inspiring research groups: I wish to thank Prof. H. V. Poor for his precious support and Prof. Matthieu Bloch for the enthusiasm and the dedication he transmitted to me. Finally, I wish to thank Prof. Merouane Debbah for his endless capacity of finding new research directions and for the opportunity to collaborate within his lively research team.

I want to express my gratitude also to all the graduating students and researchers who worked with me and helped me with inspiring discussions and kind support: Federico Librino, Simone Del Favero, Paolo Casari, Marco Rotoloni, Marco Maso, Emiliano Dall'Anese, Alberto Vigato, Tomaso Erseghe, Maria Fresia, Luca Scardovi, Deniz Gunduz and Alexandre Pierrot.