Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels

Francesco Renna, *Member, IEEE*, Nicola Laurenti, and H. Vincent Poor, *Fellow, IEEE*

***Abstract*—This paper considers the information theoretic secrecy rates that are achievable by an orthogonal frequency-division multiplexing (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 analysis is made possible by modeling the system as a particular instance of a high dimensional multiple-input multiple-output wiretap channel.**

The secrecy capacity is formulated as a maximization problem under a trace constraint, and simple expressions are given for its high signal-to-noise (SNR) limit. The low rate limit of the secrecy outage probability is also evaluated under a fading channel model. As for the finite SNR case, the secrecy rates that can be achieved with particular inputs are considered.

Numerical results are provided under a Rayleigh fading channel model and under dependence of the main and eavesdropper channels. The secrecy loss due to the OFDM structure constraints, and the information gain for an eavesdropper that uses a more complex receiver, are also considered.

***Index Terms*—Fading channel, orthogonal frequency-division multiplexing (OFDM), physical-layer security, wiretap channel.**

I. Introduction

INFORMATION secrecy has traditionally been guaranteed by protocols and algorithms operating at the higher layers of the communication stack. More specifically, the problem of keeping information secret from malicious eavesdroppers has been tackled starting from the assumption of an underlying reliable end-to-end communication channel. However, the exponentially increasing demand for wireless, ubiquitous communications and the need for a way to securely transmit data are becoming challenging constraints for system designers. For this reason, the physical layer of communications has been addressed as a valuable tool in order to guarantee confidentiality of messages transmitted over the wireless medium.

In recent years, orthogonal frequency-division multiplexing (OFDM) has been chosen as the suitable solution for the physical layer of many major wireless and wired communication standards. The reasons for its widespread adoption as a standard physical-layer solution are the possibility of coping with frequency selective channels with simple and efficiently implemented transceivers and the ability to achieve high spectral efficiency. Thus, it seems appropriate to take into account its impact when investigating physical-layer security.

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 [1] consider the possibility of applying elliptic curve cryptography to the OFDM modulated signal, but the detrimental effects of the dispersive channel on the encrypted signal are not taken into account in the analysis. In [2], 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 this way, reliable symbol detection by the eavesdropper is prevented, while the legitimate receiver, being aware of the secret key, can demap the received symbols back to the sparse constellation. In [3], 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 fact, the base for secrecy of the transmitted message is offered by the randomness and diversity in the transmission channel. In this setting, secrecy is defined within a statistical framework and the concept of perfect secrecy [4] is introduced as the statistical independence between the information bearing message and the eavesdropper's observations.

The seminal works of Wyner [5] and Csiszár and Körner [6] characterized secrecy capacity for a wiretap channel as the maximal rate at which information can be transmitted, while guaranteeing a vanishing mutual information leakage per channel use. Since then, the secrecy capacity has been explored for different channel models and network settings (see [7] for an overview).

Manuscript received December 21, 2011; accepted March 29, 2012. Date of publication April 19, 2012; date of current version July 09, 2012. This work was supported in part by the U.S. National Science Foundation under Grant CNS-09-05398 and in part by the Italian Ministry of Education and Research (MIUR) under Grant "ESCAPADE" RBFR105NLC. This work was presented in part at the European Wireless Conference, April 2010 and in part at the Personal, Indoor and Mobile Radio Communication Symposium, September 2010. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wade Trappe.

F. Renna is with the Instituto de Telecomunicações and the Department of Computer Science, Faculdade de Ciencias da Universidade do Porto, 4169-007 Porto, Portugal (e-mail: frarenna@dcc.fc.up.pt).

N. Laurenti is with the Department of Information Engineering, University of Padova, 35131 Padova, Italy (e-mail: nil@dei.unipd.it).

H. V. Poor is with the Department of Electrical Engineering, Princeton University, Princeton, NJ 08544 USA (e-mail: poor@princeton.edu).

Digital Object Identifier 10.1109/TIFS.2012.2195491

Nevertheless, in the information theoretic security literature, OFDM has usually been modeled as a set of parallel Gaussian channels [8]–[10], with the implicit assumption that also the eavesdropper adopts an OFDM demodulator with cyclic prefix removal and fast Fourier transform (FFT). The secrecy capacity for this scenario and the corresponding power allocation have been derived [8]. Similarly, optimal power allocation strategies for the multiuser broadcast case are derived in [9] and [10]. In [11], the same parallel channels model is used, but secrecy is defined and achieved in terms of minimum mean squared error at the eavesdropper. In [12] 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 [13], although the eavesdropper is still supposed to drop the initial part of each received symbol. Consequently, the scenario is modeled as a more general multiple-input multiple-output (MIMO) Gaussian wiretap channel (such as those in [14] and [15]). In [13], 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 paper is to consider the more conservative case in which the transmitter and the legitimate receiver adopt OFDM transmission, 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. Similarly, we also compare it with achievable secrecy rates and secrecy capacity 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.

The remainder of the paper is organized as follows. In Section II, the system model is described and OFDM is presented first as a filter bank transmission and then as a particular instance of the MIMO Gaussian wiretap channel. The optimization problem that defines the secrecy capacity of OFDM systems with a generic eavesdropper is formulated in Section III. The solution of this problem in the high SNR regime is described in Section IV. Then, in Section V we analyze the nonzero secrecy rate outage probability both for an OFDM eavesdropper and for more sophisticated receivers. In Section VI, we evaluate the loss in secrecy capacity due to the OFDM structure in the low SNR regime. The secrecy rates achieved with three different input strategies are evaluated for the previously described setting in Section VII and finally we draw some conclusions in Section VIII.

Throughout the paper, vectors are indicated with lowercase boldface symbols, whereas uppercase boldface letters are used for matrices. The symbol * indicates the conjugate transpose of a matrix and † denotes its Moore-Penrose pseudo-inverse. $\mathbf{I}_n$ 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. We indicate with $\preceq$ the partial ordering between positive semi-definite matrices, that is we write $\mathbf{A}\succeq\mathbf{B}$ (or $\mathbf{B}\preceq\mathbf{A}$) if $\mathbf{A},\mathbf{B}$ and $\mathbf{A}-\mathbf{B}$ are all positive semi-definite. The ith eigenvalue of the square matrix $\mathbf{A}$ is indicated by $\lambda_i(\mathbf{A})$, whereas the ith singular value of the matrix $\mathbf{A}$ is denoted by $\sigma_i(\mathbf{A})$. The Euclidean norm of a vector $\mathbf{v}$ is written as $\|\mathbf{v}\|$. We indicate the positive part of a real 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 $g*h$. We also use the notation $f(x)\asymp g(x)$ to indicate that $\lim_{x\to\infty} f(x)/g(x)=1$.

II. System Model

A. OFDM as Filter Bank

A general model for OFDM modulation is depicted in Fig. 1 and comprises both the cyclic prefix (CP) and zero pad suffix (ZS) systems [16]. It shows the baseband equivalent of both the transmitter and the receiver filter banks. Each bank is made of M frequency-shifted versions of the same filter $\gamma_i(t),\ i=1,\ldots,M$, for the transmitter, and $\phi_i(t),\ i=1,\ldots,M$, for the receiver, that are centered around the M subcarrier frequencies f_i, multiples of the subcarrier spacing F_u. 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. The asymmetry between the filter shapes $\gamma_i(t)$ and $\phi_i(t)$ provides the redundancy that is necessary to convert the dispersive channel into the parallel of M flat fading subchannels. It was shown in [16] that the ZS system with overlap-add receiver and the CP system with prefix removal are equivalent, that is, they yield identical performance in terms of probability of error, even with dispersive channels. However, this is not guaranteed to hold under a secrecy performance metric, as we shall investigate.

In the remainder of this work we will consider different scenarios depending on whether or not the transmitter/legitimate receiver and the eavesdropper use the OFDM architecture for transmission and reception.

B. OFDM as MIMO Gaussian Channel

In order to assess the performance achieved by the system under analysis in terms of secrecy capacity it is convenient to consider also an alternative matrix representation of the system. This description is based on the discrete time equivalent of the system with N samples per symbol period, and its efficient implementation through the FFT algorithm. We assume that the CP (or ZS) is longer than the delay spread of the main channel g_R in order to avoid intersymbol interference (ISI) and interchannel interference (ICI) at the legitimate receiver. For the sake of compactness, we focus on the transmission of a single OFDM symbol. This scenario can be depicted as a special case of the MIMO Gaussian wiretap channel [13]

$$\mathbf{y}=\mathbf{G}_\mathrm{R}\mathbf{x}+\mathbf{w}_\mathrm{R}\quad\text{and}\quad\mathbf{z}=\mathbf{G}_\mathrm{E}\mathbf{x}+\mathbf{w}_\mathrm{E}\tag{1}$$

in which the vector $\mathbf{x}\in\mathbb{C}^N$ contains the signal samples corresponding to an OFDM symbol, transmitted on both channels,

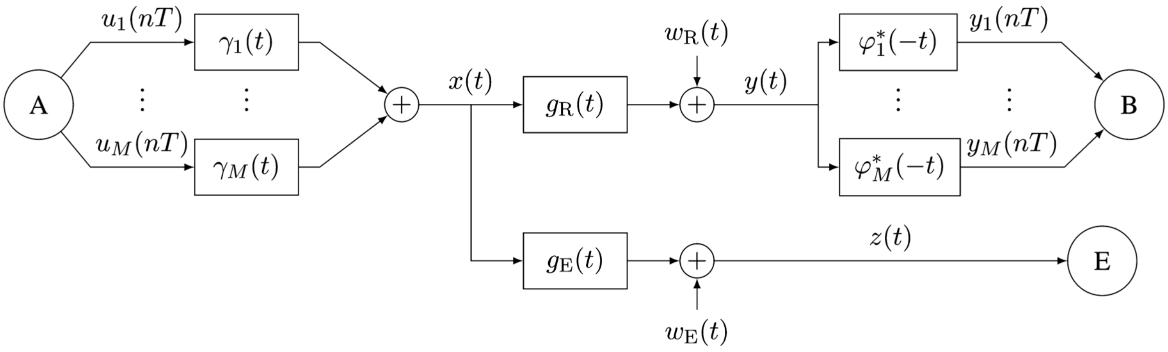

Fig. 1. Filter bank description of an OFDM system with a dispersive channel and a generic eavesdropper E. The OFDM symbol duration is denoted by T.

while $\mathbf{G}_{\mathrm{R}} \in \mathbb{C}^{(N+L_{\mathrm{R}}-1)\times N}$ and $\mathbf{G}_{\mathrm{E}} \in \mathbb{C}^{(N+L_{\mathrm{E}-1})\times N}$ are Toeplitz matrices defined as

$$\mathbf{G}_{\mathrm{R}} = \begin{bmatrix} g_{\mathrm{R}}(0) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ g_{\mathrm{R}}(L_{\mathrm{R}}-1) & \ddots & g_{\mathrm{R}}(0) \\ 0 & \ddots & \vdots \\ \vdots & \ddots & g_{\mathrm{R}}(L_{\mathrm{R}}-1) \end{bmatrix} \quad (2)$$

and analogously for $\mathbf{G}_{\mathrm{E}}$. They represent the convolution of the input signal $\mathbf{x}$ with the channels g_{R} and g_{E}, having lengths L_{R} and L_{E}, respectively.

The noise vectors $\mathbf{w}_{\mathrm{R}}, \mathbf{w}_{\mathrm{E}} \sim \mathcal{CN}(0, \mathbf{I}_{N+L_i-1})$ comprise independent, zero-mean, unit-variance, circularly symmetric complex Gaussian variables. We note that the evaluation of the secrecy capacity of the MIMO Gaussian wiretap channel in (1) leads directly to the secrecy capacity of the frequency selective channel itself when both the legitimate transmitter/receiver and the eavesdropper are not constrained to implement a particular modulation format.

On the other hand, in order to impose the OFDM structure on the transmitted signal, we write

$$\mathbf{x} = \mathbf{T}\mathbf{u} \quad (3)$$

with the vector $\mathbf{u} \in \mathbb{C}^M$ containing the frequency domain symbols loaded on the M subcarriers. The OFDM modulation matrix $\mathbf{T}$ is an $N \times M$ matrix that can be written as $\mathbf{T} = \mathbf{A}\mathbf{F}^*$, in which $\mathbf{F}$ represents the FFT matrix of size M, while $\mathbf{A} \in \mathbb{C}^{N\times M}$ is responsible for inserting $\mu = N - M$ redundant samples that are needed to overcome the delay spread of the dispersive channel. For a CP system

$$\mathbf{A} = \left[\frac{\mathbf{0} \quad \mathbf{I}_\mu}{\mathbf{I}_M}\right] \quad (4)$$

whereas for the ZS system, we have

$$\mathbf{A} = \begin{bmatrix} \mathbf{I}_M \\ \mathbf{0}_{\mu\times M} \end{bmatrix}. \quad (5)$$

Similarly, demodulation at the receiver can be represented by the multiplication $\mathbf{v} = \mathbf{R}\mathbf{y}$ of the legitimate channel output by the matrix $\mathbf{R} = \mathbf{F}\mathbf{B}$. Here $\mathbf{B}$ is such that for either system, owing to the condition $L_{\mathrm{R}} \leq \mu$

$$\mathbf{R}\mathbf{G}_{\mathrm{R}}\mathbf{T} = \mathrm{diag}(\mathcal{G}_{\mathrm{R}}(f_i)) \quad (6)$$

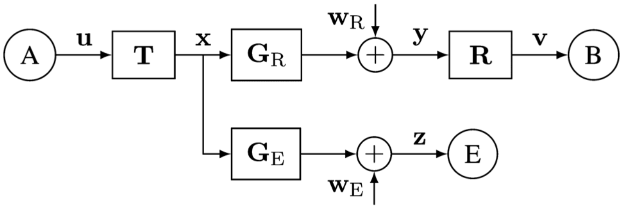
A
$\mathbf{u}$
$\mathbf{T}$
$\mathbf{x}$
$\mathbf{G}_{\mathrm{R}}$
$\mathbf{w}_{\mathrm{R}}$
$\mathbf{y}$
$\mathbf{R}$
$\mathbf{v}$
B
$\mathbf{G}_{\mathrm{E}}$
$\mathbf{w}_{\mathrm{E}}$
$\mathbf{z}$
E

Fig. 2. Block diagram of a discrete-time vector/matrix equivalent of the OFDM system in Fig. 1.

in which $\mathcal{G}_{\mathrm{R}}(f_i)$, $i = 1, \ldots, M$, is the length M FFT of the legitimate channel impulse response. So for the CP system

$$\mathbf{B} = [\,\mathbf{0}_{M\times\mu} \quad \mathbf{I}_M \quad \mathbf{0}_{M\times(L_{\mathrm{R}}-1)}\,] \quad (7)$$

whereas for the ZS system we have

$$\mathbf{B} = \left[\mathbf{I}_M \left| \begin{matrix}\mathbf{I}_\mu \\ \mathbf{0}\end{matrix} \right| \mathbf{0}_{M\times(L_{\mathrm{R}}-1)}\right]. \quad (8)$$

Given the above, the OFDM system scenario of Fig. 2 (OFDM transmission and generic eavesdropper) can be represented as an equivalent MIMO Gaussian wiretap channel [15], [17]

$$\mathbf{v} = \mathbf{H}_{\mathrm{R}}\mathbf{u} + \mathbf{w}'_{\mathrm{R}}$$
$$\text{and} \quad \mathbf{z} = \mathbf{H}_{\mathrm{E}}\mathbf{u} + \mathbf{w}_{\mathrm{E}} \quad (9)$$

with $\mathbf{H}_{\mathrm{R}} = \mathrm{diag}(\mathcal{G}_{\mathrm{R}}(f_i))$, $\mathbf{H}_{\mathrm{E}} = \mathbf{G}_{\mathrm{E}}\mathbf{T}$ and $\mathbf{w}'_{\mathrm{R}} = \mathbf{R}\mathbf{w}_{\mathrm{R}}$. Consequently, the covariance matrix of the demodulated noise at the legitimate receiver is $\mathbf{K}_{\mathbf{w}'_{\mathrm{R}}} = \mathbf{R}\mathbf{R}^*$.

III. Secrecy Capacity of OFDM Systems With Generic Eavesdropper

Our objective in this work 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. This scenario 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 [8] and [18]. Then, the same results are compared with those provided by the fading channels $(\mathbf{G}_{\mathrm{R}}, \mathbf{G}_{\mathrm{E}})$, 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 [8] as

$$C_{\mathrm{s}} = \max_{\sum P_i \le P} \sum_{i=1}^{M} \left[\log \frac{1+|\mathcal{G}_{\mathrm{R}}(f_i)|^2 P_i}{1+|\mathcal{G}_{\mathrm{E}}(f_i)|^2 P_i}\right]^+ \tag{10}$$

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 $|\mathcal{G}_{\mathrm{R}}(f_i)| < |\mathcal{G}_{\mathrm{E}}(f_i)|$.

On the other hand, once we refrain from imposing the OFDM structure on the eavesdropper's receiver, as shown in Section II-B, the system as a whole, comprising the OFDM transmitter, the legitimate channel, the OFDM receiver and the eavesdropper channel, can be regarded as a MIMO Gaussian wiretap channel (9). In this case, we aim to determine the secrecy capacity for the MIMO Gaussian wiretap channel (9) under a total power constraint on the transmitted signal

$$\mathrm{tr}(\mathbf{K}_{\mathbf{x}}) = \mathrm{tr}(\mathbf{T}\mathbf{K}_{\mathbf{u}}\mathbf{T}^*) \le P. \tag{11}$$

By using the general result of Csiszár and Körner [6], in particular its version extended to continuous alphabet problems with average cost constraints, one obtains the single letter expression of the secrecy capacity

$$C_{\mathrm{s}} = \max_{p(q,\mathbf{u})} [I(q;\mathbf{v}) - I(q;\mathbf{z})] \tag{12}$$

where $I(\cdot;\cdot)$ denotes the mutual information between its two arguments and q is an auxiliary random variable satisfying the Markov relation

$$q \longrightarrow \mathbf{u} \longrightarrow (\mathbf{v},\mathbf{z}). \tag{13}$$

However, the following lemma shows that q is not needed in the maximization in (12).

Lemma 1: The secrecy capacity (12) for the MIMO Gaussian wiretap channel (9) under the trace constraint (11) is achieved without channel prefixing (that is with $q = \mathbf{u}$), and the corresponding input $\mathbf{u}$ is Gaussian distributed.

Proof: The result in [19, Th. 3] states that the secrecy capacity of the MIMO Gaussian wiretap channel (9) under the general matrix covariance constraint

$$\mathbf{K}_{\mathbf{u}} \preceq \mathbf{P} \tag{14}$$

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

$$\max_{\substack{p(q,\mathbf{u}):\\ \mathbf{K}_{\mathbf{u}} \preceq \mathbf{P}}} [I(q;\mathbf{v}) - I(q;\mathbf{z})] = \max_{\substack{\mathbf{u}\sim\mathcal{CN}(\mathbf{0},\mathbf{K}_{\mathbf{u}})\\ \mathbf{K}_{\mathbf{u}} \preceq \mathbf{P}}} [I(\mathbf{u};\mathbf{v}) - I(\mathbf{u};\mathbf{z})]. \tag{15}$$

Then, we define the set

$$\mathcal{K}_P = \{\mathbf{K} \succeq \mathbf{0} : \mathrm{tr}(\mathbf{T}\mathbf{K}\mathbf{T}^*) \le P\} \tag{16}$$

and state the equality

$$\bigcup_{\mathbf{P}\in\mathcal{K}_P} \{\mathbf{K} : \mathbf{0} \preceq \mathbf{K} \preceq \mathbf{P}\} = \mathcal{K}_P. \tag{17}$$

To prove (17), we need only to show that $\cup_{\mathbf{P}\in\mathcal{K}_P} \{\mathbf{K} : \mathbf{K} \preceq \mathbf{P}\} \subseteq \mathcal{K}_P$, as the reverse inclusion holds trivially. Then, for any $\mathbf{P} \in \mathcal{K}_P$ and any $\mathbf{K} \preceq \mathbf{P}$, we have

$$\mathrm{tr}(\mathbf{T}\mathbf{K}\mathbf{T}^*) \le \mathrm{tr}(\mathbf{T}\mathbf{P}\mathbf{T}^*) \le P \tag{18}$$

that is $\mathbf{K} \in \mathcal{K}_P$, which proves (17). Hence, we can write (12) under the constraint (11) as

$$\begin{aligned} C_{\mathrm{s}} &= \max_{\mathbf{P}\in\mathcal{K}_P} \max_{p(q,\mathbf{u}):\mathbf{K}_{\mathbf{u}}\preceq\mathbf{P}} [I(q;\mathbf{v}) - I(q;\mathbf{z})] && (19)\\ &= \max_{\mathbf{P}\in\mathcal{K}_P} \max_{\substack{\mathbf{u}\sim\mathcal{CN}(\mathbf{0},\mathbf{K}_{\mathbf{u}})\\ \mathbf{K}_{\mathbf{u}}\preceq\mathbf{P}}} [I(\mathbf{u};\mathbf{v}) - I(\mathbf{u};\mathbf{z})] && (20)\\ &= \max_{\substack{\mathbf{u}\sim\mathcal{CN}(\mathbf{0},\mathbf{K}_{\mathbf{u}})\\ \mathbf{K}_{\mathbf{u}}\in\mathcal{K}_P}} [I(\mathbf{u};\mathbf{v}) - I(\mathbf{u};\mathbf{z})] && (21)\end{aligned}$$

where we have used the set equality (17) in deriving (19) and (21), and (15) in deriving (20). This concludes the proof. ■

We are now ready to state our main result.

Theorem 2: The secrecy capacity of the MIMO Gaussian wiretap channel (9) under the trace constraint (11) is given by

$$C_{\mathrm{s}} = \max_{\mathrm{tr}(\mathbf{K})\le P} \left[\log|\mathbf{I} + \tilde{\mathbf{H}}_{\mathrm{R}}\mathbf{K}\tilde{\mathbf{H}}_{\mathrm{R}}^*| - \log|\mathbf{I} + \tilde{\mathbf{H}}_{\mathrm{E}}\mathbf{K}\tilde{\mathbf{H}}_{\mathrm{E}}^*|\right] \tag{22}$$

where

$$\tilde{\mathbf{H}}_{\mathrm{R}} = \begin{cases} \mathbf{H}_{\mathrm{R}}\mathbf{D}_{\mathrm{CP}}\mathbf{F} & \text{for CP}\\ \mathbf{F}\mathbf{D}_{\mathrm{ZS}}\mathbf{H}_{\mathrm{R}} & \text{for ZS}\end{cases} \tag{23}$$

$$\tilde{\mathbf{H}}_{\mathrm{E}} = \begin{cases} \mathbf{H}_{\mathrm{E}}\mathbf{D}_{\mathrm{CP}}\mathbf{F} & \text{for CP}\\ \mathbf{H}_{\mathrm{E}} & \text{for ZS}\end{cases} \tag{24}$$

and

$$\mathbf{D}_{\mathrm{CP}} = \left[\begin{array}{c|c} \mathbf{I}_{M-\mu} & \mathbf{0}\\ \hline \mathbf{0} & \frac{1}{\sqrt{2}}\mathbf{I}_{\mu}\end{array}\right], \quad \mathbf{D}_{\mathrm{ZS}} = \left[\begin{array}{c|c} \frac{1}{\sqrt{2}}\mathbf{I}_{\mu} & \mathbf{0}\\ \hline \mathbf{0} & \mathbf{I}_{M-\mu}\end{array}\right]. \tag{25}$$

The corresponding input covariance is given by

$$\mathbf{K}_{\mathbf{u}} = \begin{cases} \mathbf{F}\mathbf{D}_{\mathrm{CP}}\mathbf{K}^{\star}\mathbf{D}_{\mathrm{CP}}\mathbf{F} & \text{for CP}\\ \mathbf{K}^{\star} & \text{for ZS}\end{cases} \tag{26}$$

where $\mathbf{K}^{\star}$ maximizes (22).

Proof: From (21) in Lemma 1, we can write the secrecy capacity for the OFDM system with generic eavesdropper as

$$C_{\mathrm{s}} = \max_{\mathbf{K}_{\mathbf{u}}\in\mathcal{K}_P} \left[\log\frac{|\mathbf{R}\mathbf{R}^* + \mathbf{H}_{\mathrm{R}}\mathbf{K}_{\mathbf{u}}\mathbf{H}_{\mathrm{R}}^*|}{|\mathbf{R}\mathbf{R}^*|} - \log|\mathbf{I} + \mathbf{H}_{\mathrm{E}}\mathbf{K}_{\mathbf{u}}\mathbf{H}_{\mathrm{E}}^*|\right]. \tag{27}$$

For the CP system (27) simplifies, as $\mathbf{R}\mathbf{R}^* = \mathbf{I}_M$, while the trace in the constraint (11) can be rewritten from the expression of the transmission matrix (4) as

$$\begin{aligned}\mathrm{tr}(\mathbf{T}\mathbf{K}_{\mathbf{u}}\mathbf{T}^*) &= \mathrm{tr}(\mathbf{A}^*\mathbf{A}\mathbf{F}^*\mathbf{K}_{\mathbf{u}}\mathbf{F})\\ &= \mathrm{tr}(\mathbf{D}_{\mathrm{CP}}^{-1}\mathbf{F}^*\mathbf{K}_{\mathbf{u}}\mathbf{F}\mathbf{D}_{\mathrm{CP}}^{-1})\end{aligned} \tag{28}$$

where $\mathbf{D}_{\mathrm{CP}} = (\sqrt{\mathbf{A}^*\mathbf{A}})^{-1}$ has the expression (25).

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

$$\mathbf{K}_{\mathbf{w}'_{\rm R}} = \mathbf{R}\mathbf{R}^* = \mathbf{F}\mathbf{B}\mathbf{B}^*\mathbf{F}^* = \mathbf{F}\mathbf{D}_{\rm ZS}^{-1}\mathbf{D}_{\rm ZS}^{-1}\mathbf{F}^* \tag{29}$$

where, similarly to the CP case, we define $\mathbf{D}_{\rm ZS} = (\sqrt{\mathbf{B}\mathbf{B}^*})^{-1}$ which is given in (25). ■

It is well known, however, that the maximization problem in (22) is nonconvex [17], and a closed form solution in the presence of a total power constraint can be computed only for the high SNR limit.

IV. Secrecy Capacity in 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 $\sigma^2_{{\rm R},n} = E[|g_{\rm R}(n)|^2]$ and $\sigma^2_{{\rm E},n} = E[|g_{\rm E}(n)|^2]$; thus, the average SNRs at the legitimate receiver and the eavesdropper are $\Gamma_{\rm R} = 1/M\sum_{n=0}^{L_{\rm R}-1}\sigma^2_{{\rm R},n}$ and $\Gamma_{\rm E} = 1/M\sum_{n=0}^{L_{\rm E}-1}\sigma^2_{{\rm E},n}$, respectively. The ratio between the average SNR on the main channel and that on the eavesdropper channel is denoted by $\Gamma = \Gamma_{\rm R}/\Gamma_{\rm E}$.

A. *OFDM Transmission With Generic Eavesdropper*

In the following, we will apply to the OFDM case the approach described in [17] to calculate the high SNR secrecy capacity of a MIMO Gaussian wiretap channel and we will compute the solution of the maximization problem in (22) when $P \to \infty$.

Lemma 3 [20, Th. 2]: Let $\mathbf{H}_1 \in \mathbb{C}^{n_1\times m}$ and $\mathbf{H}_2 \in \mathbb{C}^{n_2\times m}$ with $n_1, n_2 \ge m$. Let $\mathbf{X} \in \mathbb{C}^{m\times m}$ be positive semi-definite. If $\operatorname{rank}(\mathbf{H}_2) = m$, the limiting solution for $P \to \infty$, of the maximization problem

$$f(P) = \max_{\operatorname{tr}(\mathbf{X})\le P}[\log|\mathbf{I}+\mathbf{H}_1\mathbf{X}\mathbf{H}_1^*| - \log|\mathbf{I}+\mathbf{H}_2\mathbf{X}\mathbf{H}_2^*|] \tag{30}$$

is given in terms of the singular values of $\mathbf{H}_1\mathbf{H}_2^\dagger$ by

$$\lim_{P\to\infty} f(P) = \sum_i [\log\sigma_i^2(\mathbf{H}_1\mathbf{H}_2^\dagger)]^+. \tag{31}$$

By assuming that $g_{\rm E}(n)$ are continuous random variables it follows that $\operatorname{rank}(\tilde{\mathbf{H}}_{\rm E}) = M$ almost surely. Then the null space of $\tilde{\mathbf{H}}_{\rm E}$ is $\{\mathbf{0}\}$ and from Lemma 3 the asymptotic secrecy capacity for high SNR is

$$\lim_{P\to\infty} C_{\rm s} = \sum_{i=1}^{M}[\log_2\sigma_i^2(\tilde{\mathbf{H}}_{\rm R}\tilde{\mathbf{H}}_{\rm E}^\dagger)]^+. \tag{32}$$

B. *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 (1).

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

Once we fix a channel model, with its bandwidth $F_0 = 1/T_0 = MF_{\rm u}$ and its lengths $L_{\rm R}$ and $L_{\rm E}$, 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 $C_{\rm s}$ as $N \to \infty$, 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 $\mathbf{C}_N = \mathbf{C}_{\rm R}\mathbf{C}_{\rm E}^{-1}$ so that the dependence on N is explicitly indicated and noting that

$$|\mathcal{G}_{\rm R}(f)|^2 = \sum_{n=-L_{\rm R}+1}^{L_{\rm R}-1} c_{\rm R}(n)e^{-j2\pi f n T_0} \tag{33}$$

(the same holds for the eavesdropper channel) we can use [21, Th. 5.3] to write

$$\lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}[\log\lambda_i(\mathbf{C}_N)]^+ = \frac{1}{F_0}\int_{\mathcal{B}}\left[\log\frac{|\mathcal{G}_{\rm R}(f)|^2}{|\mathcal{G}_{\rm E}(f)|^2}\right]^+ df \tag{34}$$

where $\mathcal{B} = (-F_0/2, F_0/2)$. Comparing the integral in (34) with the high SNR limit of the secrecy capacity (10) of parallel Gaussian channels, we observe that both the unconstrained and the OFDM eavesdropper scenarios converge to the same value of secrecy capacity. Moreover, one can see that also in the case of OFDM transmission with a generic eavesdropper the high SNR secrecy capacity converges to (34) when $N \to \infty$ and the quantity μ is fixed, as the matrices $\mathbf{A}$ and $\mathbf{B}$ 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 [20]. 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 $\operatorname{rank}(\mathbf{G}_{\rm R}) = \operatorname{rank}(\mathbf{G}_{\rm E}) = N$ almost surely, this scheme translates to a simple uniform power allocation, and the high SNR secrecy rate achieved by this method is given, as $N \to \infty$ by

$$R_\infty = \lim_{N\to\infty}\left[\frac{1}{N}\sum_{i=1}^{N}\log\lambda_i(\mathbf{C}_N)\right]^+ \tag{35}$$

$$= \frac{1}{F_0}\left[\int_{\mathcal{B}}\log\frac{|\mathcal{G}_{\rm R}(f)|^2}{|\mathcal{G}_{\rm E}(f)|^2}df\right]^+. \tag{36}$$

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

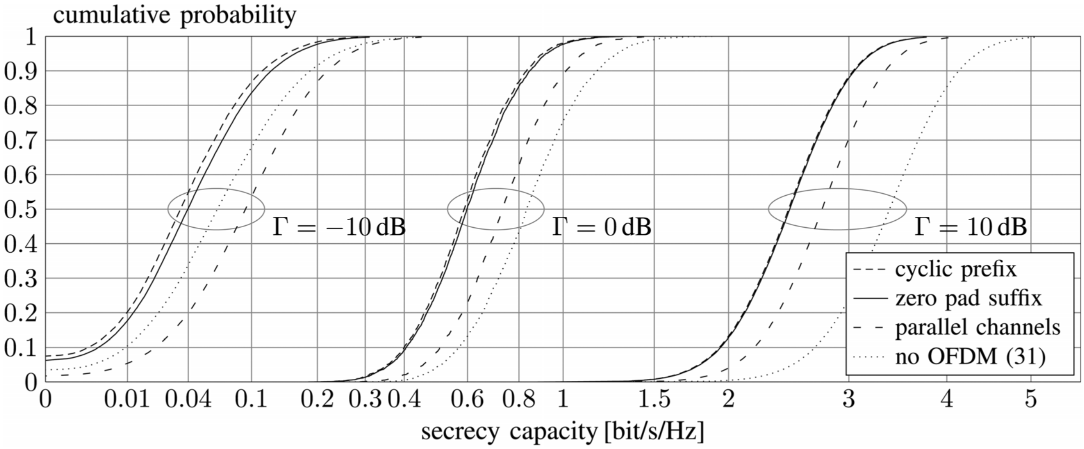

Fig. 3. Cumulative distribution functions of high SNR secrecy capacity for different ratios between the SNR at the legitimate receiver and that at the eavesdropper, $\Gamma = -10, 0, 10$ dB.

Hence, the asymptotic secrecy rate obtained can be easily computed in terms of the power cepstrum [12, Ch. 12] of the channel impulse responses

$$R_\infty = \left[\sqrt{\hat{g}_{\rm R}(0)} - \sqrt{\hat{g}_{\rm E}(0)}\right]^+ \tag{37}$$

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

$$\hat{g}(k) = \left|\int_{\mathcal{B}} \log|\mathcal{G}(f)|^2 e^{-j2\pi f k T_0} df\right|^2 \tag{38}$$

with

$$\mathcal{G}(f) = \sum_n T_0 g(nT_0) e^{-j2\pi f n T_0}. \tag{39}$$

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 $\tilde{g}_{\rm R}(n) = g_{\rm R}(n)/\sqrt{\Gamma_{\rm R}}$, $\tilde{g}_{\rm E}(n) = g_{\rm E}(n)/\sqrt{\Gamma_{\rm E}}$ the channel impulse responses normalized over the average SNR, and by $\tilde{\mathcal{G}}_{\rm R}(f)$ and $\tilde{\mathcal{G}}_{\rm E}(f)$ the corresponding normalized frequency responses, we can write

$$\mathrm{E}[R_\infty] = \mathrm{E}\left[\left[\log\Gamma + \frac{1}{F_0}\int_{\mathcal{B}} \log\frac{|\tilde{\mathcal{G}}_{\rm R}(f)|^2}{|\tilde{\mathcal{G}}_{\rm E}(f)|^2} df\right]^+\right]. \tag{40}$$

We observe that the average secrecy rate $\mathrm{E}[R_\infty]$ scales with $\log\Gamma$ when $\Gamma \to \infty$. In fact, a lower bound on the average secrecy rate is given by

$$\begin{aligned}\mathrm{E}[R_\infty] &\geq \log\Gamma + \mathrm{E}\left[\frac{1}{F_0}\int_{\mathcal{B}} \log\frac{|\tilde{\mathcal{G}}_{\rm R}(f)|^2}{|\tilde{\mathcal{G}}_{\rm E}(f)|^2} df\right] && (41)\\ &= \log\Gamma && (42)\end{aligned}$$

where the equality in (42) is due to the fact that $\tilde{\mathcal{G}}_{\rm R}(f), \tilde{\mathcal{G}}_{\rm E}(f)$ are independent and identically distributed (i.i.d.) random variables. On the other hand, the average secrecy rate is upper bounded by

$$\mathrm{E}[R_\infty] \leq [\log\Gamma]^+ + \mathrm{E}\left[\left[\frac{1}{F_0}\int_{\mathcal{B}} \log\frac{|\tilde{\mathcal{G}}_{\rm R}(f)|^2}{|\tilde{\mathcal{G}}_{\rm E}(f)|^2} df\right]^+\right] \tag{43}$$

and hence we can write

$$\mathrm{E}[R_\infty] \asymp \log\Gamma \tag{44}$$

as the second term in the right-hand side of (43) does not increase with Γ.

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

$$\mathrm{E}[C_{\rm s}] \asymp N \log\Gamma, \quad \text{as } \Gamma \to \infty \tag{45}$$

while for both the OFDM and the parallel channels case

$$\mathrm{E}[C_{\rm s}] \asymp M \log\Gamma, \quad \text{as } \Gamma \to \infty. \tag{46}$$

C. 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 exponential power delay profiles.

In Fig. 3 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 (or zero-padding suffix) $\mu = 16$ and channel delay spreads $L_{\rm R} = L_{\rm E} = \mu = 16$. 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 $\Gamma = 10$ dB), the highest secrecy capacity is achieved by the fading channel itself without constraints. On the other hand, the results obtained with $\Gamma = -10$ 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 conditions.

As regards the two types of OFDM systems, it is interesting to observe that ZS clearly exhibits a slight advantage over CP in terms of the high SNR secrecy capacity distribution. This is in contrast with what happens in a scenario without security constraints, where they provide identical performance [16].

We now focus our attention on how design parameters affect the secrecy capacity of OFDM systems. As explained in Section IV, 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 tradeoff between augmenting the legitimate receiver capacity and leaking of information towards the eavesdropper. As depicted in Fig. 4, 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 OFDM 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.

V. Secrecy Outage Probability

In this section, we characterize the probability that, according to the channel model introduced at the beginning of Section IV, the pair of fading channels $(g_{\rm R}, g_{\rm E})$ can support some positive secrecy rate. Given a slow fading channel model, the traditional definition of secrecy outage probability[2]

$$P_{\rm out}(R_{\rm s}) = P[C_{\rm s} < R_{\rm s}] \tag{47}$$

is the probability that the actual channel realization cannot support a secret communication scheme with transmission rate $R_{\rm s}$.

This quantity is not straightforward to compute even in the high SNR regime, for all the communication scenarios considered in the previous sections. For example, assuming the eavesdropper is using an OFDM receiver and for $P \longrightarrow \infty$, the secrecy outage probability is given by

$$P_{\rm out}(R_{\rm s}) = P\left[\sum_{i=1}^{M}\left[\log\frac{|\mathcal{G}_{\rm R}(f_i)|^2}{|\mathcal{G}_{\rm E}(f_i)|^2}\right]^+ < R_{\rm s}\right] \tag{48}$$

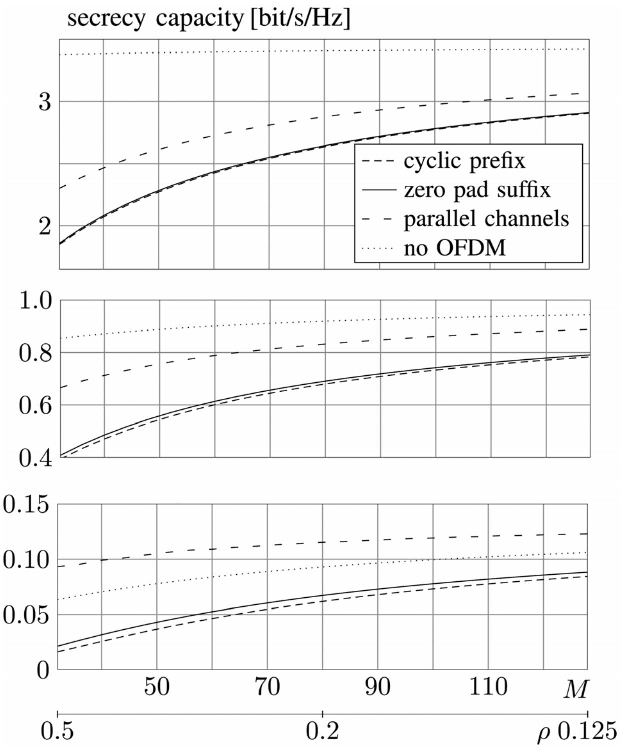

Fig. 4. High SNR secrecy capacity versus number of subcarriers for different values, $\Gamma = -10, 0, 10$ dB, of ratio between the SNR on legitimate and eavesdropper channel. The quantity $\rho = \mu/M$ represents the spectral redundancy of the system.

which cannot be easily expressed in terms of the probability density functions (pdfs) of the channel impulse responses. On the other hand, for both the cases of OFDM transmission with a generic eavesdropper and generic transmission, the secrecy outage probability becomes

$$P_{\rm out}(R_{\rm s}) = \left[P\sum_{i=1}^{M}\left[\log\sigma_i^2\right]^+ < R_{\rm s}\right] \tag{49}$$

with σ_i the generalized singular values of the matrices $\tilde{\mathbf{H}}_{\rm R}\tilde{\mathbf{H}}_{\rm E}^{\dagger}$ and $\mathbf{G}_{\rm R}\mathbf{G}_{\rm E}^{\dagger}$, respectively. Here, the difficulty in evaluating the secrecy outage probability is represented by the lack of a tractable statistical description of the σ_i's.

Nevertheless, it is possible to compute the probability of existence of nonzero secrecy, which is defined in terms of the secrecy outage probability as

$$P_{\rm ex} = P[C_{\rm s} > 0] = 1 - \lim_{R_{\rm s}\longrightarrow 0^+} P_{\rm out}(R_{\rm s}). \tag{50}$$

Thus, $P_{\rm ex}$ represents the probability that the channel realization is able to support a secret transmission scheme with nonzero data rate.

On recalling that for a MIMO Gaussian wiretap channel it holds that [20, Claim 1]

$$\lim_{P\longrightarrow\infty} C_{\rm s} > 0 \iff C_{\rm s} > 0, \ \forall P > 0 \tag{51}$$

we can claim that $P_{\rm ex}$ can be determined by limiting the analysis to the high SNR regime and its value does not change with P.

[2] In the following, we will adopt an outage formulation accounting for the probability of having transmission that are both reliable and secure. A discussion about this approach and an alternative formulation can be found in [23].

A. Parallel Channels

First, we consider the case in which legitimate users and eavesdropper deploy OFDM transceivers. Given the formulation of the secrecy capacity in (10), the probability of secure nonzero secrecy rate is the probability that the main channel has higher amplitude than the eavesdropper at some subcarrier frequency

$$P_{\text{ex}} = P\left[\bigcup_{i=1}^{M}\{|\mathcal{G}_{\text{R}}(f_i)| > |\mathcal{G}_{\text{E}}(f_i)|\}\right]. \tag{52}$$

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

$$\begin{aligned} P_{\text{ex}} &= 1 - P\left[\bigcap_{i=1}^{M}\{|\mathcal{G}_{\text{R}}(f_i)| \le |\mathcal{G}_{\text{E}}(f_i)|\}\right] & (53)\\ &\simeq 1 - \prod_{i=1}^{M} P[|\mathcal{G}_{\text{R}}(f_i)| \le |\mathcal{G}_{\text{E}}(f_i)|]. & (54)\end{aligned}$$

If we assume that both channels have independent taps with Rayleigh fading, then $|\mathcal{G}_{\text{R}}(f_i)|^2$ and $|\mathcal{G}_{\text{E}}(f_i)|^2$ are two independent random variables exponentially distributed with means $\Gamma_{\text{R}} = 1/M\sum_{n=0}^{L_{\text{R}}-1}\sigma_{\text{R},n}^2$ and $\Gamma_{\text{E}} = 1/M\sum_{n=0}^{L_{\text{E}}-1}\sigma_{\text{E},n}^2$, respectively, and the approximation is obtained from the outage probability in [24] as

$$P_{\text{ex}} \simeq 1 - \left(\frac{1}{1+\Gamma}\right)^{M} \tag{55}$$

in which we recall that $\Gamma = \Gamma_{\text{R}}/\Gamma_{\text{E}}$ is the ratio between the SNR at the legitimate receiver and that at the eavesdropper.

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

$$\begin{aligned} \lim_{N\longrightarrow\infty} P_{\text{ex}} &= \text{P}[\exists f \in \mathcal{B} : |\mathcal{G}_{\text{R}}(f)| \ge |\mathcal{G}_{\text{E}}(f)|] & (56)\\ &= 1 - \text{P}[|\mathcal{G}_{\text{E}}(f)|^2 - |\mathcal{G}_{\text{R}}(f)|^2 \ge 0,\ \forall f \in \mathcal{B}]. & (57)\end{aligned}$$

The last term in (57) suggests an effective criterion to link the probability of positive secrecy capacity with the time domain expression of the channel. Namely, from Bochner's theorem [25] we can state that the asymptotic probability of nonzero secrecy capacity is equal to the probability that the function $c_{\text{E}}(n) - c_{\text{R}}(n)$ is not positive semi-definite.

B. Generic Transmission and Generic Eavesdropper

In order to derive the probability P_{ex} for the scenarios with unconstrained modulation format, we can leverage again the results on the secrecy capacity for a MIMO Gaussian wiretap channel. In this case, P_{ex} depends on the largest eigenvalue of $\mathbf{C}_{\text{R}}\mathbf{C}_{\text{E}}^{-1}$, as

$$P_{\text{ex}} = \text{P}[\lambda_{\max}(\mathbf{C}_N) > 1]. \tag{58}$$

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 value of P_{ex} for $N \longrightarrow \infty$. Then, by applying [21, Corollary 4.2 and Th. 5.3], we can state that

$$\lim_{N\longrightarrow\infty} \lambda_{\max}(\mathbf{C}_N) = \max_{f\in(-F_0/2,F_0/2)} \frac{|\mathcal{G}_{\text{R}}(f)|^2}{|\mathcal{G}_{\text{E}}(f)|^2}. \tag{59}$$

Thus, for the unconstrained case, the asymptotic probability of existence of nonzero secrecy rate is given again by (57).

C. OFDM Transmission With Generic Eavesdropper

For this case we can repeat the same analysis as given previously. The high SNR regime analysis of the achievable rates for the OFDM system with a generic eavesdropper provides us with a physical interpretation of the probability of having nonzero secrecy rate in this scenario. For 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

$$\tilde{\mathbf{H}}_{\text{R}}(\tilde{\mathbf{H}}_{\text{E}}^{*}\tilde{\mathbf{H}}_{\text{E}})^{-1}\tilde{\mathbf{H}}_{\text{R}}^{*} = \mathbf{H}_{\text{R}}(\mathbf{H}_{\text{E}}^{*}\mathbf{H}_{\text{E}})^{-1}\mathbf{H}_{\text{R}}^{*}. \tag{60}$$

Thus, we can address the secrecy capacity starting from the definition of the channels $\mathbf{H}_{\text{R}}$ and $\mathbf{H}_{\text{E}}$. In particular, from the expression of the high SNR secrecy capacity in terms of the generalized singular values of the couple $(\mathbf{H}_{\text{R}}, \mathbf{H}_{\text{E}})$ 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 [20]

$$\sigma_{\max}^2(\mathbf{H}_{\text{R}}\mathbf{H}_{\text{E}}^{\dagger}) = \sup_{\mathbf{u}\in\mathbb{C}^M} \frac{||\mathbf{H}_{\text{R}}\mathbf{u}||^2}{||\mathbf{H}_{\text{E}}\mathbf{u}||^2} \le 1. \tag{61}$$

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

$$||\mathbf{H}_{\text{R}}\mathbf{u}||^2 = \sum_{i=1}^{M} |\mathcal{G}_{\text{R}}(f_i)|^2 |u_i|^2 \tag{62}$$

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

$$||\mathbf{H}_{\text{E}}\mathbf{u}||^2 = \int_{\mathcal{B}} \left|\sum_{i=1}^{M} u_i \Gamma_0(f - f_i)\mathcal{G}_{\text{E}}(f)\right|^2 df \tag{63}$$

where $\Gamma_0(f - f_i)$ is the frequency response of the ith subcarrier transmission filter. In particular, for the CP system it holds that

$$\Gamma_0(f) = \frac{1+\rho}{\sqrt{F_{\text{u}}}} \text{sinc}(Tf) e^{-j\pi(1-\rho)f/F_{\text{u}}} \tag{64}$$

whereas, for ZS we have

$$\Gamma_0(f) = \frac{1}{\sqrt{F_\mathrm{u}}}\mathrm{sinc}\left(\frac{f}{F_\mathrm{u}}\right)e^{-j\pi f/F_\mathrm{u}}. \tag{65}$$

The expression in (63) tells us that the probability P_ex is closely related to the probability that there exists at least one index i for which

$$|\mathcal{G}_\mathrm{R}(f_i)|^2 > \int_\mathcal{B} |\Gamma_0(f-f_i)|^2 |\mathcal{G}_\mathrm{E}(f)|^2 df. \tag{66}$$

From (66) 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 ith 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.

D. 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 $L_\mathrm{R} = L_\mathrm{E} = \mu$.

The probability of existence of positive secrecy rate for the SNR range favorable to the eavesdropper is reported in Fig. 5. The small gap between the channel curve and the OFDM 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 (55) represents a tight upper bound especially when the main channel has a much lower SNR than the eavesdropper, and the single events $\{|\mathcal{G}_\mathrm{R}(f_i)| > |\mathcal{G}_\mathrm{E}(f_i)|\}$ become less and less probable.

Nevertheless, it is interesting to note that, despite its widespread use in the literature [8], the independent carriers assumption turns out to be misleading in evaluating the asymptotic probability of nonzero secrecy rate for the parallel channels scenario even as $N \longrightarrow \infty$. The probabilities in Fig. 6 are computed for transmissions over Rayleigh fading channels of length $L_\mathrm{R} = L_\mathrm{E} = \mu = 8$ with $\Gamma = -10$ dB. The approximation in (55) always approaches 1 when $N \gg \max\{L_\mathrm{R}, L_\mathrm{E}\}$ regardless of the actual values of Γ and the channel impulse responses. On the other hand, the correlation among subcarriers is shown to limit the available diversity at the transmitter even when the number of subchannels increases. As a consequence of the argument in Section V-A, the asymptotic probability of nonzero secrecy rate over frequency selective channels is determined by the difference in the channel autocorrelations and may be bounded away from 1.

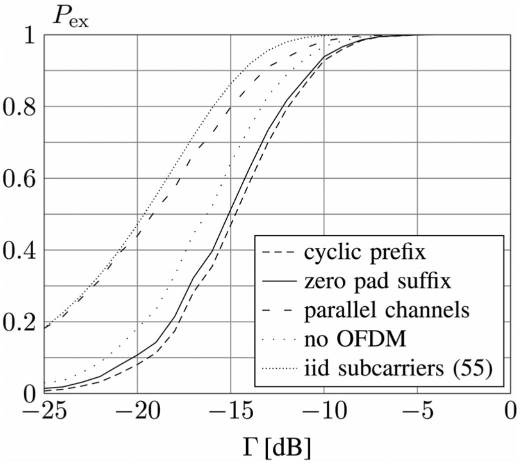

Fig. 5. Probability of existence of nonzero secrecy rate as a function of the ratio Γ between SNRs on the main and eavesdropper channels. Results are given for the different scenarios analyzed in this paper and also for the statistically independent subcarriers approximation.

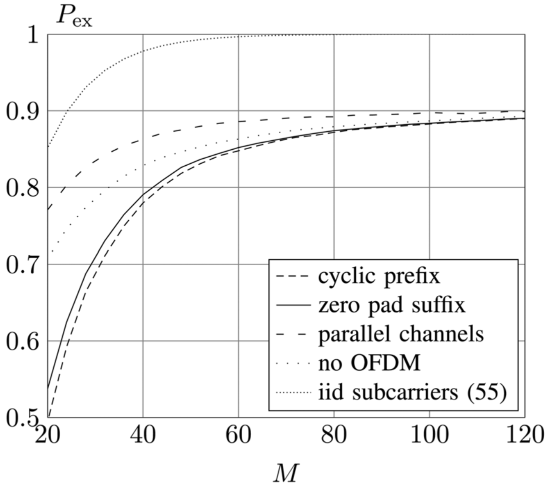

Fig. 6. Probability of existence of nonzero secrecy rate versus number of subcarriers M. Numerical results are given for the scenarios analyzed in this paper and also for the statistically independent subcarriers approximation. The ratio between SNRs on main and eavesdropper channels is $\Gamma = -10$ dB.

VI. Secrecy Capacity Derivative in 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 $\tilde{\mathbf{H}}_\mathrm{R}$ and $\tilde{\mathbf{H}}_\mathrm{E}$ for both the ZS and CP systems to gain insight into the behavior of the secrecy capacity in the low SNR regime, i.e., for $P \longrightarrow 0$. In particular, we can use the result in [26] and claim that the first derivative of the secrecy capacity for $P = 0$ is proportional to the maximal eigenvalue of the pencil $\mathbf{\Phi} = \tilde{\mathbf{H}}_\mathrm{R}^*\tilde{\mathbf{H}}_\mathrm{R} - \tilde{\mathbf{H}}_\mathrm{E}^*\tilde{\mathbf{H}}_\mathrm{E}$. Namely,[3]

$$\dot{C}_\mathrm{s}|_{P=0} = \frac{1}{(1+\rho)\ln 2}\left[\lambda_{\max}(\mathbf{\Phi})\right]^+. \tag{67}$$

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

[3] Note that the result in [26] is correct despite some flaws in its proof, as was discussed in [27].

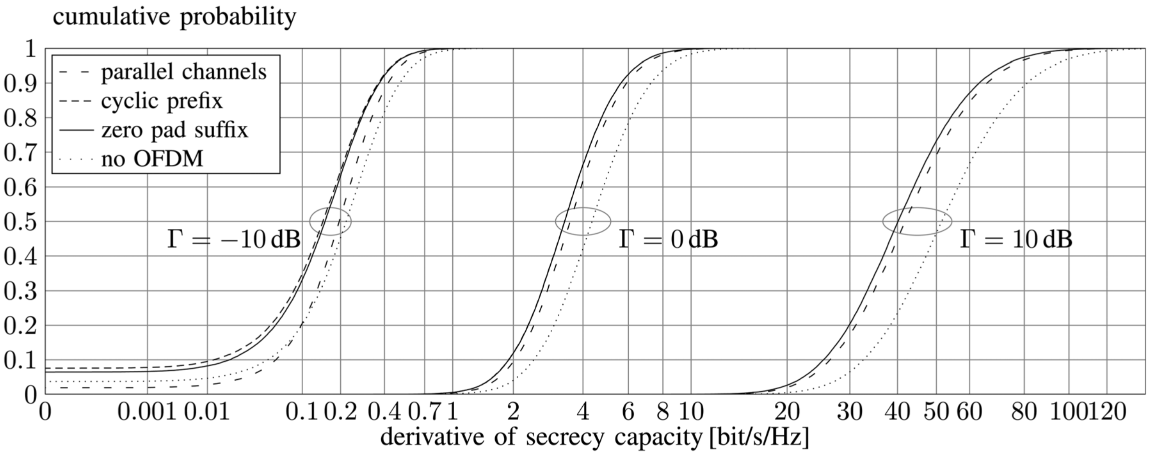

Fig. 7. Cumulative distribution function of the low SNR derivative of the secrecy capacity for different ratios between the SNRs on the legitimate receiver and eavesdropper channel, $\Gamma = -10, 0, 10$ dB. Curves for CP and ZS overlap, whereas slight differences can be observed among the two OFDM implementations and parallel channels assumption.

In Fig. 7 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.

VII. Evaluation of Some Achievable Secrecy Rates With Finite SNRs

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.

A. Optimal Input for High SNR

First we consider the performance obtained with the input that achieves the secrecy capacity at high SNR. Recall that the secrecy capacity was established in Section IV-A, starting from the generalized singular value decomposition (GSVD) of $(\tilde{\mathbf{H}}_{\rm R}, \tilde{\mathbf{H}}_{\rm E})$. In particular [20], the GSVD of $(\tilde{\mathbf{H}}_{\rm R}, \tilde{\mathbf{H}}_{\rm E})$ yields unitary $\mathbf{\Psi}_{\rm R}$ and $\mathbf{\Psi}_{\rm E}$, and a nonsingular $\mathbf{\Omega}$ such that

$$\mathbf{\Psi}_{\rm R}^* \tilde{\mathbf{H}}_{\rm R} \mathbf{\Omega} = \mathbf{D}_{\rm R}, \ \mathbf{\Psi}_{\rm E}^* \tilde{\mathbf{H}}_{\rm E} \mathbf{\Omega} = \begin{bmatrix} \mathbf{D}_{\rm E} \\ \mathbf{0} \end{bmatrix}. \tag{68}$$

In (68), the diagonal matrices $\mathbf{D}_{\rm R} = \operatorname{diag}(r_1, \ldots, r_M)$ and $\mathbf{D}_{\rm E} = \operatorname{diag}(e_1, \ldots, e_M)$ contain the values that give the singular values $\sigma_i = r_i/e_i$, $i = 1, \ldots, M$, which we assume to be sorted in increasing order. The corresponding maximizer for (22) is given by [17]

$$\mathbf{K}^\star = \alpha P \mathbf{\Omega}_\xi \mathbf{\Omega}_\xi^* \tag{69}$$

where $\mathbf{\Omega}_\xi$ gathers the last ξ columns of $\mathbf{\Omega}$ in the GSVD (68), and ξ is the number of generalized singular values that are greater than one. In (69), $\alpha = 1/\operatorname{tr}(\mathbf{\Omega}_\xi \mathbf{\Omega}_\xi^*)$ 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.

B. Water-Filling Solution

Next, we evaluate the results provided by the power allocation scheme of [9]. 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 on each channel is known to reach the secrecy capacity [8], and hence the optimal input covariance matrix $\mathbf{K_u}$ is diagonal. This fact turns out to be useful in handling the total power trace constraint for the CP system. In fact, since $\mathbf{K_u} = \operatorname{diag}(P_1, \ldots, P_M)$ is diagonal, the matrix $\mathbf{F}^* \mathbf{K_u} \mathbf{F}$ is circulant and its diagonal elements are equal to $\operatorname{tr}(\mathbf{K_u})/M$. Thus, the total power constraint can be easily expressed as

$$\begin{aligned} \operatorname{tr}(\mathbf{T}\mathbf{K_u}\mathbf{T}^*) &= \operatorname{tr}(\mathbf{A}\mathbf{F}^*\mathbf{K_u}\mathbf{F}\mathbf{A}^*) && (70) \\ &= (M+\mu)\frac{\operatorname{tr}(\mathbf{K_u})}{M} && (71) \\ &= (1+\rho)\operatorname{tr}(\mathbf{K_u}). && (72) \end{aligned}$$

For the sake of a compact notation, we define $\alpha_m = 1/|\mathcal{G}_{\rm E}(f_m)|^2 - 1/|\mathcal{G}_{\rm R}(f_m)|^2$ and $\beta_m = 1/|\mathcal{G}_{\rm E}(f_m)|^2 + 1/|\mathcal{G}_{\rm R}(f_m)|^2$. Thus, the optimal power allocation for parallel Gaussian channels is a water-filling type solution [9] for which $P_m^* = 0$ when $|\mathcal{G}_{\rm R}(f_m)| \leq |\mathcal{G}_{\rm E}(f_m)|$, otherwise

$$P_m^* = \left[\sqrt{\frac{\alpha_m^2}{4} + \frac{\alpha_m}{\eta}} - \frac{\beta_m}{2}\right]^+ \tag{73}$$

with $\eta > 0$ such that

$$\sum_{m=1}^{M} P_m^* = P'. \tag{74}$$

We observe that, in order to fulfill 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.

C. 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 (27) to diagonal input covariance matrices $\mathbf{K}_{\mathbf{u}}$, and hence obtain lower complexity, close to that of the algorithm in [9]. 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, $I(\mathbf{u},\mathbf{v}) - I(\mathbf{u},\mathbf{z})$, under the constraint that $\mathrm{tr}(\mathbf{K}_{\mathbf{x}}) \leq P$. Then, if we denote the set of diagonal covariance matrices that satisfy the trace constraint as

$$\mathcal{K}'_P = \left\{ \mathbf{K} = \mathrm{diag}(P_1,\ldots,P_M) : P_i \geq 0, \sum_{i=1}^{M} P_i \leq P \right\} \tag{75}$$

from (72), we can write the optimal power allocation for the CP system as

$$R_{\mathrm{s}}^{\mathrm{cp}} = \max_{\mathbf{K}_{\mathbf{u}} \in \mathcal{K}'_{P'}} \left[\log|\mathbf{I} + \mathbf{H}_{\mathrm{R}}\mathbf{K}_{\mathbf{u}}\mathbf{H}_{\mathrm{R}}^*| - \log|\mathbf{I} + \mathbf{H}_{\mathrm{E}}\mathbf{K}_{\mathbf{u}}\mathbf{H}_{\mathrm{E}}^*|\right]. \tag{76}$$

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

$$R_{\mathrm{s}}^{\mathrm{zp}} = \max_{\mathbf{K}_{\mathbf{u}} \in \mathcal{K}'_{P}} \left[\log|\mathbf{I} + \tilde{\mathbf{H}}_{\mathrm{R}}\mathbf{K}_{\mathbf{u}}\tilde{\mathbf{H}}_{\mathrm{R}}^*| - \log|\mathbf{I} + \mathbf{H}_{\mathrm{E}}\mathbf{K}_{\mathbf{u}}\mathbf{H}_{\mathrm{E}}^*|\right]. \tag{77}$$

D. Achievable Secrecy Rates With Equiprobable QAM Inputs

Consider now the secrecy rates that can be achieved when the M subcarriers are loaded with independent symbols belonging to finite quadrature amplitude modulation (QAM) constellations [28], [29]. We denote by $R(\mathbf{n},\mathbf{P})$ the secrecy rate achieved by an OFDM system in the presence of a generic eavesdropper, when the M subcarriers are loaded with $\mathbf{n} = [n_1,\ldots,n_M]$ bits and power is allocated according to the vector $\mathbf{P} = [P_1,\ldots,P_M]$. We show that in the high SNR limit, if the numbers n_i of bits loaded on the M subcarriers are sufficiently high, it is possible to achieve the same secrecy rates achieved by Gaussian inputs. As in Section V-C, when considering the zero-padding system, we neglect the effects of the noise correlation at the receiver output, and we model the legitimate channel as the parallel of M Gaussian channels.

For $n_i \longrightarrow \infty$, the QAM input to the ith subcarrier converges in distribution to a uniform input over the interval

$$\left[-\sqrt{\frac{3P_i}{2}}, \sqrt{\frac{3P_i}{2}}\right] \times \left[-\sqrt{\frac{3P_i}{2}}, \sqrt{\frac{3P_i}{2}}\right].$$

Then, by denoting with $R_{\mathrm{U}}(\mathbf{P})$ the secrecy rate achieved when all M subcarriers have a uniform input, we state the following lemma.[4]

Lemma 4: $\lim_{\mathbf{n}\longrightarrow\infty} R(\mathbf{n},\mathbf{P}) = R_{\mathrm{U}}(\mathbf{P})$.

Proof: This can be proved by considering the corresponding convergence of the differential entropies $h(\mathbf{v})$ and $h(\mathbf{z})$, which in turn is justified on the grounds of dominated convergence [30]. ■

Lemma 5: $\lim_{\mathbf{P}\longrightarrow\infty} R_{\mathrm{U}}(\mathbf{P}) = \lim_{\mathbf{P}\longrightarrow\infty} R_{\mathrm{G}}(\mathbf{P})$.

Proof: Without loss of generality, assume $P_i > 0$ for $i = 1,\ldots,M$, that is power is transmitted over all the subcarriers.[5] Then, consider the SVD of matrix $\mathbf{H}_{\mathrm{E}}$

$$\mathbf{H}_{\mathrm{E}} = \mathbf{U}_{\mathrm{E}} \begin{bmatrix} \mathbf{\Sigma}_{\mathrm{E}} \\ \mathbf{0} \end{bmatrix} \mathbf{V}_{\mathrm{E}}^* \tag{78}$$

in which the diagonal matrix $\mathbf{\Sigma}_{\mathrm{E}} = \mathrm{diag}(\sigma_{\mathrm{E},1},\ldots,\sigma_{\mathrm{E},M})$ contains the nonzero singular values of $\mathbf{H}_{\mathrm{E}}$ and $\mathbf{U}_{\mathrm{E}}, \mathbf{V}_{\mathrm{E}}^*$ are unitary. Then, the mutual information of the eavesdropper channel is equal to the mutual information of the channel having input/output relationship

$$\mathbf{z}' = \tilde{\mathbf{\Sigma}}_{\mathrm{E}}\mathbf{u} + \mathbf{w}'_{\mathrm{E}} \tag{79}$$

where $\tilde{\mathbf{\Sigma}}_{\mathrm{E}} = \mathbf{\Sigma}_{\mathrm{E}}\mathbf{V}_{\mathrm{E}}^*$ and $\mathbf{w}'_{\mathrm{E}}$ contains the first M entries of the vector $\mathbf{U}_{\mathrm{E}}^*\mathbf{w}_{\mathrm{E}}$. Then, the achievable secrecy rate with independent Gaussian inputs over the M subcarriers is

$$R_{\mathrm{G}}(\mathbf{P}) = [I_{\mathrm{G}}(\mathbf{u};\mathbf{v}) - I_{\mathrm{G}}(\mathbf{u};\mathbf{z}')]^+ \tag{80}$$

$$= \left[\sum_{i=1}^{M} \log|\mathcal{G}_{\mathrm{R}}(f_i)|^2 P_i - \log|\mathbf{I} + \tilde{\mathbf{\Sigma}}_{\mathrm{E}}\mathrm{diag}(\mathbf{P})\tilde{\mathbf{\Sigma}}_{\mathrm{E}}^*|\right]^+. \tag{81}$$

In the limit for $\mathbf{P} \longrightarrow \infty$, (81) becomes

$$\lim_{\mathbf{P}\longrightarrow\infty} R_{\mathrm{G}}(\mathbf{P}) = \left[\sum_{i=1}^{M} \log|\mathcal{G}_{\mathrm{R}}(f_i)|^2 - \log|\mathbf{\Sigma}_{\mathrm{E}}\mathbf{\Sigma}_{\mathrm{E}}^*|\right]^+ \tag{82}$$

$$= \left[\sum_{i=1}^{M} \log|\mathcal{G}_{\mathrm{R}}(f_i)|^2 - \sum_{i=1}^{M} \log\sigma_{\mathrm{E},i}^2\right]^+. \tag{83}$$

On the other hand, the secrecy rate with uniform inputs can be written as

$$R_{\mathrm{U}}(\mathbf{P}) = [I_{\mathrm{U}}(\mathbf{u};\mathbf{v}) - I_{\mathrm{U}}(\mathbf{u};\mathbf{z}')]^+ \tag{84}$$

$$= [I_{\mathrm{U}}(\mathbf{u};\mathbf{v}) - h_{\mathrm{U}}(\mathbf{z}') + h_{\mathrm{U}}(\mathbf{z}'|\mathbf{u})]^+. \tag{85}$$

In the high SNR regime, as shown in [31], the mutual information gap between Gaussian signaling and uniform signaling over each subchannel of the legitimate receiver is $\log(\pi e/6)$, and hence $I_{\mathrm{U}}(\mathbf{u};\mathbf{v}) = I_{\mathrm{G}}(\mathbf{u};\mathbf{v}) - M\log(\pi e/6)$. Moreover, when the input power is sufficiently high, $h_{\mathrm{U}}(\mathbf{z}') = h_{\mathrm{U}}(\tilde{\mathbf{\Sigma}}_{\mathrm{E}}\mathbf{u})$ and by using [32]

$$h_{\mathrm{U}}(\mathbf{\Sigma}_{\mathrm{E}}\mathbf{u}) = h_{\mathrm{U}}(\mathbf{u}) + 2\log|\tilde{\mathbf{\Sigma}}_{\mathrm{E}}| \tag{86}$$

[4] We use the notation $\mathbf{x} \longrightarrow \infty$ to indicate that all the entries in the vector $\mathbf{x}$ tend to ∞.

[5] If there exists some index i for which $P_i = 0$, then the mutual information terms in the secrecy rate can be evaluated from the equivalent channels with reduced dimensions obtained by eliminating the ith column from the channel matrices.

we obtain

$$\lim_{\mathbf{P}\longrightarrow\infty} R_{\mathrm{U}}(\mathbf{P}) = \left[\sum_{i=1}^{M}\log\frac{|\mathcal{G}_{\mathrm{R}}(f_i)|^2}{6} - M\log\left(\frac{\pi e}{6}\right) - 2\log|\tilde{\mathbf{\Sigma}}_{\mathrm{E}}| + M\log(\pi e)\right]^{+} \tag{87}$$

$$= \left[\sum_{i=1}^{M}\log|\mathcal{G}_{\mathrm{R}}(f_i)|^2 - \sum_{i=1}^{M}\log\sigma^2_{\mathrm{E},i}\right]^{+} \tag{88}$$

where in (87) we have used the fact that the differential entropy of a zero mean uniform complex random variable with power P_i is equal to $\log 6P_i$. ■

By combining Lemmas 4 and 5 we can immediately state the following.

Proposition 6:

$$\lim_{\mathbf{P}\longrightarrow\infty}\lim_{\mathbf{n}\longrightarrow\infty} R(\mathbf{n},\mathbf{P}) = \lim_{\mathbf{P}\longrightarrow\infty} R_{\mathrm{G}}(\mathbf{P})$$

.

Thus, the result in Proposition 6 reveals that the achievable rates obtained with Gaussian inputs and a power allocation $\mathbf{P}$, such as those in Section VII-B and Section VII-C, can be achieved also by more practical QAM signaling schemes, provided that the power is suitably increased and QAM constellations with sufficiently large cardinalities are chosen.

E. 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 $L_{\mathrm{R}} = L_{\mathrm{E}} = \mu = 16$ with exponentially decaying power delay profiles. The legitimate and eavesdropper channel are given 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 (76) and (77).

In Fig. 8, 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 (73) is degraded with respect to the corresponding result in [9] for the OFDM eavesdropper. In particular, as shown in Fig. 9, the loss is about 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.

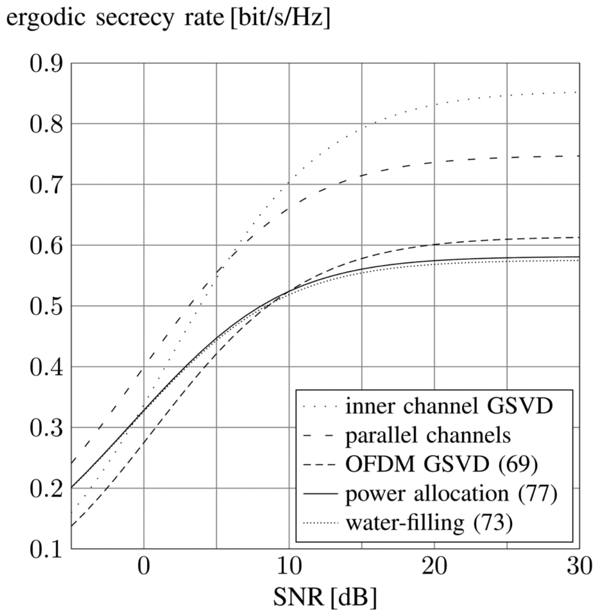

Fig. 8. Ergodic secrecy rates achieved by three different strategies in Section VII for ZS system and performance of inner channel and parallel channels assumption.

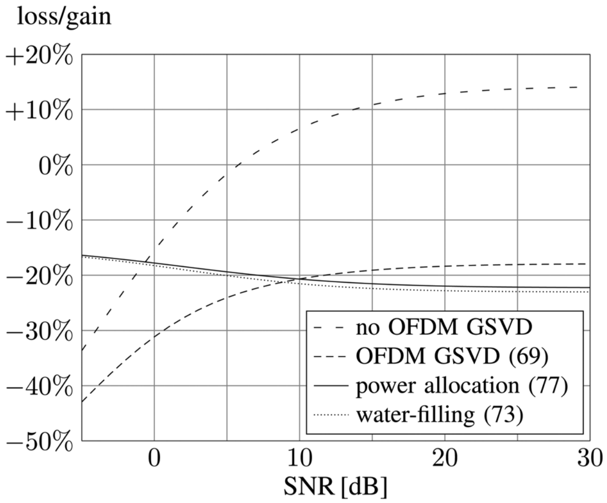

Fig. 9. Percentage loss of ergodic secrecy rates achieved by three different strategies in Section VII with respect to parallel channel scenario.

Although the optimal power allocations (76) and (77) show only a very slight improvement with respect to (73) when the average secrecy rate is taken as the performance metric, the proposed method can guarantee appreciable improvement.

VIII. Conclusion

We have considered how the information theoretic limits on secure 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 the eavesdropper is also forced to implement OFDM demodulation and we have quantified the losses caused by the use at the eavesdropper of a more sophisticated receiver.

In particular, we have computed the secrecy capacity reduction due to an unconstrained eavesdropper in the high SNR regime and we have evaluated the impact of different channels conditions between the legitimate parties and the eavesdropper. In this way, we have pointed out that the predictions obtained when assuming an OFDM demodulator at the eavesdropper can be extremely misleading when the eavesdropper enjoys better channel conditions than the legitimate receiver. We note that the ZS system exhibits slightly higher values of the secrecy capacity with respect to CP. Similarly, we have evaluated the secrecy capacity behavior for low SNRs, showing that the effects of an OFDM eavesdropper are less crucial than for high SNR values.

We have also considered the probability of existence of a nonzero secrecy rate in the system and compared new accurate results with the predictions offered by models that previously appeared in the literature.

All results on the OFDM secrecy capacity have been compared with the secrecy capacity of the wiretap fading channel itself. The latter case, in which no constraints are imposed on the type of modulation adopted or the complexity of the transceiver implementation, clearly represents an upper bound for the former. Such performance bounds have been expressed in terms of the channel impulse and frequency responses. Hence, they can also be used in the future in evaluating the benefits of transmission systems other than OFDM from the point of view of information-theoretic security.

For positive and finite SNR values, given the impossibility of deriving the secrecy capacity, we have evaluated the achievable secrecy rates obtained for different inputs. In particular, we have shown that the secrecy rates obtained by independent Gaussian inputs on each subcarrier can also be achieved with more practical equiprobable QAM inputs, providing the power in each subcarrier is suitably increased and the corresponding QAM cardinality is sufficiently large.

References

[1] R. S. Owor, K. Dajani, Z. Okonkwo, and J. Hamilton, “An elliptical cryptographic algorithm for RF wireless devices,” in *Proc. Winter Simulation Conf.*, Washington, DC, 2007.

[2] D. Reilly and G. Kanter, “Noise-enhanced encryption for physical layer security in an OFDM radio,” in *Proc. IEEE Radio Wireless Symp.*, San Diego, CA, Jan. 2009.

[3] W.-J Lin and J.-C Yen, “An integrating channel coding and cryptography design for OFDM based WLANs,” in *Proc. IEEE Int. Symp. Consumer Electronics*, Kyoto, Japan, May 2009.

[4] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.*, vol. 29, pp. 656–715, 1949.

[5] A. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

[6] I. Csiszár and J. Körner, “Broadcast channels with confidential messages,” *IEEE Trans. Inform. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[7] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*. Hanover, MA: Now Publishers, 2009.

[8] Z. Li, R. Yates, and W. Trappe, “Secrecy capacity of independent parallel channels,” in *Proc. 44th Annu. Allerton Conf. Commun., Contr., Computing*, Monticello, IL, 2006.

[9] E. Jorswieck and A. Wolf, “Resource allocation for the wire-tap multi-carrier broadcast channel,” in *Proc. Int. Workshop Multiple Access Communications (MACOM)*, St. Petersburg, Russia, Jun. 2008.

[10] E. Jorswieck and S. Gerbracht, “Secrecy rate region of downlink OFDM systems: Efficient resource allocation,” in *Proc. 14th Int. OFDM-Workshop (InOWo)*, Hamburg, Germany, Sep. 2009.

[11] 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, LA, Dec. 2008.

[12] G. R. Tsouri and D. Wulich, “Securing OFDM over wireless time-varying channels using subcarrier overloading with joint signal constellations,” *EURASIP J. Wireless Commun. Netw.*, vol. 2009, p. 18, Article ID 437824.

[13] M. Kobayashi, M. Debbah, and S. Shamai, “Secured communication over frequency-selective fading channels: A practical Vandermonde precoding,” *EURASIP J. Wireless Commun. Netw.*, vol. 2009, p. 19, 2009, Article ID 386547.

[14] R. Liu, T. Liu, H. V. Poor, and S. Shamai, “Multiple-input multiple-output Gaussian broadcast channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4215–4227, Sep. 2010.

[15] R. Bustin, R. Liu, H. V. Poor, and S. Shamai, “An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel,” *EURASIP J. Wireless Commun. Netw.*, vol. 2009, Article 370970.

[16] 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.

[17] A. Khisti, G. W. Wornell, A. Wiesel, and Y. Eldar, “On the Gaussian MIMO wiretap channnel,” in *Proc. IEEE Int. Symp. Inform. Theory*, Nice, France, Jun. 2007.

[18] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[19] T. Liu and S. Shamai, “A note on the secrecy capacity of the multiple-antenna wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[20] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas-II: The MIMOME wiretap channel,” *IEEE Trans. Inform. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[21] R. M. Gray, *Toeplitz and Circulant Matrices: A Review*. Dordrecht, The Netherlands: Now Publishers, 2006.

[22] A. V. Oppenheim and R. W. Schafer, *Discrete-Time Signal Processing*. Englewood Cliffs, NJ: Prentice Hall, 1989.

[23] X. Zhou, M. McKay, B. Maham, and A. Hjørungnes, “Rethinking the secrecy outage formulation: A secure transmission design perspective,” *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–304, Mar. 2011.

[24] J. Barros and M. R. D. Rodrigues, “Secrecy capacity of wireless channels,” in *Proc. IEEE Int. Symp. Inform. Theory*, Seattle, WA, Jul. 2006.

[25] S. Bochner, *Lectures on Fourier Integrals*. Princeton, NJ: Princeton Univ. Press, 1959.

[26] M. C. Gursoy, “Secure communication in the low-SNR regime: A characterization of the energy-secrecy tradeoff,” in *Proc. IEEE Int. Symp. Inform. Theory*, Seoul, Korea, Jun. 2009.

[27] F. Renna, M. Bloch, and N. Laurenti, “Semi-blind key agreement over MIMO quasi-static channels,” in *Proc. Joint Newcom++/COST 2100 Workshop on Wireless Communications (JNCW)*, Paris, France, Mar. 2011.

[28] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, “On Gaussian wiretap channels with M-PAM inputs,” in *Proc. Eur. Wireless Conf.*, Lucca, Italy, Apr. 2010.

[29] S. Bashar, Z. Ding, and C. Xiao, “On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input,” *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 527–529, May 2011.

[30] F. J. Piera and P. Parada, “On convergence properties of Shannon entropy,” *Probl. Inf. Transm.*, vol. 45, pp. 75–94, Jun. 2009.

[31] G. D. Forney, Jr and G. Ungerboeck, “Modulation and coding for linear Gaussian channels,” *IEEE Trans. Inform. Theory*, vol. 44, no. 6, pp. 2384–2415, Oct. 1998.

[32] F. Neeser and J. Massey, “Proper complex random processes with applications to information theory,” *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1293–1302, Jul. 1993.

Francesco Renna (S’09–M’11) received the Laurea Specialistica degree in telecommunication engineering and Ph.D. degree in information engineering, both from University of Padova, Padova, Italy, in 2006 and 2011, respectively.

In 2007, he was an Intern at Infineon Technology AG, in Villach, Austria. In 2009, he was a Visiting Student Research Collaborator at the Department of Electrical Engineering, Princeton University, Princeton, NJ. During 2010, he was a Visiting Scholar at the School of Electrical Engineering of Georgia Tech Loarraine, Metz, France, and later at Supelec, Gif-sur-Yvette, France. In 2011, he was with the Department of Information Engineering, University of Padova, as a Research Fellow. Since 2012, he has been at the Instituto de Telecomunicações, University of Porto, as a Research Fellow. His research interests focus mainly on physical-layer security methods for multicarrier and multiantenna systems, optimal receiver design for multicarrier transmissions and quantum key distribution.

Nicola Laurenti was born in 1970, in Adria, Italy, and graduated from University of Padova, Padova, Italy, with a Laurea degree in electrical engineering in 1995. In 1992 and 1993, he was an exchange student at the University of California, Berkeley. He received the Ph.D. degree in electrical and telecommunications engineering from University of Padova, in 1999.

Since 2001, he has been an Assistant Professor in the Department of Information Engineering, University of Padova, where he was a Research Fellow from 1999 to 2001. In 2008 and 2009, he was a Visiting Scholar at Coordinated Science Laboratory, University of Illinois, Urbana-Champaign. His research interests mainly focus on network security at lower layers (physical, data link and network), information theoretic security and quantum key distribution, but also include other aspects of digital communications, especially multicarrier modulation and ultra-wideband transmission.

H. Vincent Poor (S'72–M'77–SM'82–F'87) received the Ph.D. degree in electrical engineering and computer science from Princeton University, Princeton, NJ, in 1977.

From 1977 until 1990, he was on the faculty of the University of Illinois, Urbana-Champaign. Since 1990, he has been on the faculty at Princeton University, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. His research interests are in the areas of stochastic analysis, statistical signal processing, and information theory, and their applications in wireless networks and related fields such as social networks and smart grid. Among his publications in these areas are the recent books *Classical, Semi-classical and Quantum Noise* (Springer, 2012) and *Smart Grid Communications and Networking* (Cambridge University Press, 2012).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, a Fellow of the American Academy of Arts and Sciences, and an International Fellow of the Royal Academy of Engineering (U.K.). He is also a Fellow of the Institute of Mathematical Statistics, the Acoustical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, and from 2004 to 2007 he served as the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY. He received a Guggenheim Fellowship in 2002 and the IEEE Education Medal in 2005. Recent recognition of his work includes the 2010 IET Ambrose Fleming Medal, the 2011 IEEE Eric E. Sumner Award, the 2011 Society Award of the IEEE Signal Processing Society, and honorary doctorates from the University of Edinburgh and Aalborg University, conferred in 2011 and 2012, respectively.