Achievable secrecy rates for wiretap OFDM with QAM constellations

Francesco Renna
Department of Information Engineering
University of Padua
frarenna@dei.unipd.it

Nicola Laurenti
Department of Information Engineering
University of Padua
nil@dei.unipd.it

H. Vincent Poor
Department of Electrical Engineering
Princeton University
poor@princeton.edu

ABSTRACT

Orthogonal frequency division multiplexing (OFDM) systems have enjoyed widespread adoption as the physical layer standard for high data rate wired and wireless networks, due to their ability to efficiently cope with slowly varying dispersive channels. Therefore in searching for feasible implementations of physical layer security techniques, it is appropriate to analyze how existing information theoretic results can be applied to the OFDM structure This paper considers the information theoretic secrecy rates that are achievable in a wiretap OFDM channel when transmitting quadrature amplitude modulation (QAM) constellation symbols. The loss with respect to the secrecy rates obtained with Gaussian distributed inputs is evaluated for both finite constellation cardinalities and in the asymptotic approximation of arbitrarily high cardinality. Moving from the insight gained with this analysis, we propose bit-loading strategies to efficiently allocate the appropriate number of bits in each subchannel, by considering the twofold objective of minimizing the loss with respect to the Gaussian input secrecy capacity and minimizing the total bit load.

Categories and Subject Descriptors

C.2.0 [**Computer-communication networks**]: General—*Security and protection*; C.2.1 [**Computer-communication networks**]: Network architecture and design—*Wireless communication*

General Terms

Security

Keywords

OFDM, wiretap channel, secrecy capacity

1. INTRODUCTION

Emerging and future wireless will allow data to be exchanged with increasing capillarity, mobility and flexibility. However, the pervasive nature of those data transmissions is clearly in contrast with another important requirement in communications, that is confidentiality of sensitive contents. For this reason, considerable attention has been paid to the problem of securing communications across all transmission layers.

Although there is already a rich literature regarding methods to provide secure communication from the end-to-end perspective of higher layers, there is still room to investigate secure transmission strategies at the physical layer. In fact, the randomness characterizing the wireless medium can be effectively harnessed to secure transmissions from unauthorized eavesdroppers. This concept was first presented in the seminal works of Wyner [1] and Csiszár and Körner [2], in which the information theoretic bounds on secret transmission over discrete memoryless channels were assessed. Secrecy rates (and the secrecy capacity) were introduced as information rates at which a message can be exchanged between a transmitter and a legitimate receiver while keeping the information rate between the message and an eavesdropper arbitrarily low.

The secrecy rates achievable over several channel models have been characterized over the years, starting from the scalar Gaussian wiretap channel model [3], and moving to parallel Gaussian channels and fading channels [4, 5], both with full and partial channel state information (CSI) at the transmitter [6]. Also the performance of multiantenna systems has been assessed in terms of the corresponding secrecy capacity [7, 8, 9]. For a comprehensive review of the various channel models and network scenarios for which achievable secrecy rates have been computed the reader might refer, for example, to [10].

More recently, several studies have sought to bridge the gap from assessing the fundamental information theoretic bounds on secure communications to practical physical layer security protocols [11, 12]. A step in this direction is represented by the investigation on the effects of the modulation format on the security performance of the system. In particular, orthogonal frequency division multiplexing (OFDM) techniques have become widespread in recent years as the physical layer solution for the majority of high data-rate wireless standards. The reason of their success is found in the capability to exploit the frequency diversity offered by dispersive channels with computationally efficient transceivers, based on the fast Fourier transform (FFT) algorithm. In the information theoretic security literature, the OFDM wiretap channel has usually been modeled as a collection of parallel

SECURENETS 2011, May 16, Paris, France

DOI 10.4108/icst.valuetools.2011.245791

Gaussian wiretap channels [4, 13], thus implicitly assuming that also the eavesdropper adopts an OFDM demodulator. The assumption of an OFDM receiver at the eavesdropper is relaxed in [14], although the eavesdropper is still supposed to drop the first fraction of each received symbol. On the other hand, our previous works [15, 16, 17] evaluate the loss in the secrecy performance incurred when the eavesdropper is free to adopt more sophisticated receivers and estimate the efficiency of OFDM modulation with the performance provided by the fading channels without modulation constraints. Nonetheless, the achievable secrecy rates for OFDM transmissions were computed on assuming Gaussian distributed inputs. In this paper, instead, we go back to the OFDM eavesdropper hypothesis and evaluate the secrecy performance of multicarrier systems when data symbols belong to finite quadrature amplitude modulation (QAM) constellations. Starting from the results presented in [18] and [19], we focus on analyzing the role of efficient bit-loading strategies that allocate the available total number of bits to the different subchannels of the system.

The remainder of this paper is organized as follows. In Section 2 the system model of OFDM transmission in the presence of an eavesdropper is described. Section 3 reviews some results on the achievable secrecy rates of Gaussian channels with finite constellation inputs and provides the evaluation of the asymptotic performance for arbitrarily high constellation cardinality. Then, different bit-loading strategies for OFDM transmissions are presented and compared in Section 4. Finally, we draw some conclusions in Section 5.

Throughout the paper, vectors are indicated with lower-case boldface symbols, whereas upper-case boldface letters are used for matrices. 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 closest integer greater than or equal to x as $\lceil x \rceil$, and the signal convolution between g and h as $g * h$. We also denote with $\mathbb{E}\{\cdot\}$ the expectation operator and with the symbol $\bar{x}$ the complex conjugate of x. The probability mass function (pmf) of a discrete random variable x is denoted with $p_x(a)$, whereas for the probability density function (pdf) of a continuos random variable y we use the notation $f_y(b)$.

2. SYSTEM MODEL

We consider OFDM transmissions, in the presence of an eavesdropper attempting to discern a secret message transmitted. Let M be the number of used subcarriers, T the OFDM symbol period and F the subcarrier spacing, so that each subcarrier frequency is $f_i = m_i F$, $i = 1, \ldots, M$ with m_i a suitable integer. Then, the (baseband equivalent of the) transmitted signal for a packet of K symbols can be written as the combination of the transmit waveforms

$$x(t) = \sum_{k=1}^{K} \sum_{i=1}^{M} u_i(k) \gamma_i(t - kT). \tag{1}$$

The data symbol $u_i(k)$ in the ith subchannel and kth symbol is taken from a finite constellation, while $\gamma_i(t) = \gamma_0(t) e^{j2\pi f_i t}$ is the frequency shifted version of a common waveform $\gamma_0(t)$. Similarly, the demodulator produces the symbols $y_i(k)$ by taking the inner product between the received signal $y(t)$ and the receiver waveforms

$$y_i(k) = \int \bar{\varphi}_i(t - kT) y(t)\, dt \quad , \quad \begin{matrix} i = 1, \ldots, M \\ k = 1, \ldots, K \end{matrix} \tag{2}$$

where $\varphi_i(t) = \varphi_0(t) e^{j2\pi f_i t}$. By considering different expressions for γ_0 and φ_0 we can model different types of OFDM systems as shown in Table 1. Note that the structure of the transmit and receive waveforms allows for efficient implementation of both the modulator and demodulator via the FFT.

system	transmit and receive filters
DMT/CP	$\gamma_0(t) = \sqrt{F}\mathbb{U}_{1/F-T}^{1/F}(t),\ \varphi_0(t) = \sqrt{F}\mathbb{U}_0^{1/F}(t)$
DMT/ZS	$\gamma_0(t) = \sqrt{F}\mathbb{U}_0^{1/F}(t),\ \varphi_0(t) = \sqrt{F}\mathbb{U}_0^{T}(t)$
FMT/NS	$\Gamma_0(f) = \Phi_0(f) = \sqrt{T\,\mathrm{rcos}(\rho, Tf)}$

Table 1: Filter expressions for common OFDM systems in the general model. The discrete multitone with cyclic prefix (DMT/CP) and zero-padding suffix (DMT/ZS), and the filtered multitone system non-critically sampled (FMT/NS). 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 $\rho = FT - 1$.

The dispersive channels towards both the legitimate receiver and the eavesdropper are linear and time invariant; hence they act onto the transmitted signal as filters with impulse responses $g_{\mathrm{R}}(t)$ and $g_{\mathrm{E}}(t)$, respectively.

In this paper, for the ease of tractability, we assume that the eavesdropper uses an OFDM receiver too, thus implying an M parallel Gaussian wiretap channel. However, it should be noted that, even if this assumption is customary [4, 5, 13], a more conservative scenario would allow the eavesdropper to use a more sophisticated receiver to retrieve more information from the transmitted signal and hence reduce the secrecy rate [15]. We also assume that, hence, intersymbol interference (ISI) and interchannel interference (ICI) are avoided at both the legitimate receiver and the eavesdropper, either because the cyclic prefix (or zero-padding suffix) is longer than the delay spread of both channels or because the channel coherence bandwidth is larger than the subcarrier spacing.

Then, on gathering into the vector $\mathbf{u}(k) \in \mathbb{C}^{M\times 1}$ the data transmitted within the kth OFDM symbol, and on denoting with $\mathbf{y}(k), \mathbf{z}(k) \in \mathbb{C}^{M\times 1}$ the corresponding outputs at the legitimate receiver and at the eavesdropper demodulators, the input-output relation of the system can be written as

$$\begin{aligned} \mathbf{y}(k) &= \mathbf{G}_{\mathrm{R}}\mathbf{u}(k) + \mathbf{w}_{\mathrm{R}}(k) \\ \text{and} \quad \mathbf{z}(k) &= \mathbf{G}_{\mathrm{E}}\mathbf{u}(k) + \mathbf{w}_{\mathrm{E}}(k). \end{aligned} \tag{3}$$

Here, $\mathbf{G}_{\mathrm{R}} = \mathrm{diag}\{G_{\mathrm{R}}(f_i)\}$ and $\mathbf{G}_{\mathrm{E}} = \mathrm{diag}\{G_{\mathrm{E}}(f_i)\}$ are diagonal matrices containing the frequency response values of the two channels at the M subcarriers' central frequencies. The vectors $\mathbf{w}_{\mathrm{R}}(k)$ and $\mathbf{w}_{\mathrm{E}}(k)$ contain independent and identically distributed (iid), zero-mean, circularly symmetric, complex Gaussian random variables with unit variances,

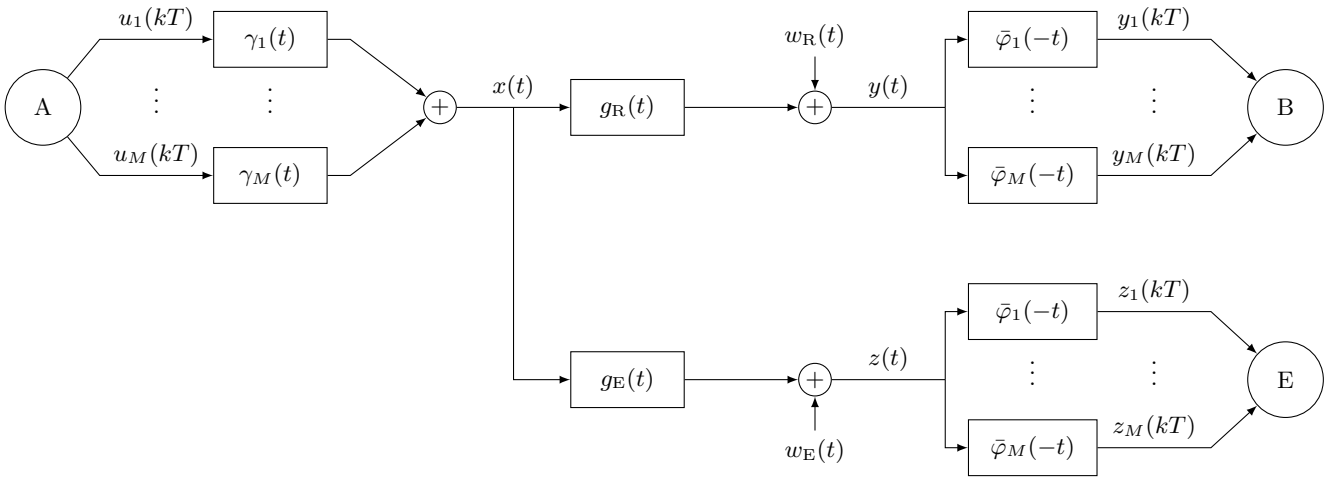

Figure 1: Block diagram of the filter bank description of an OFDM system with dispersive channel and an OFDM eavesdropper E. The OFDM symbol duration is denoted by T.

and they represent the effect of thermal noise at the legitimate receiver and the eavesdropper. The channel inputs are subject to the average power constraint

$$\frac{1}{K}\sum_{k=1}^{K}\mathbb{E}\left\{\|\mathbf{u}(k)\|^2\right\} \leq P_{\mathrm{tot}} \tag{4}$$

in which K is the number of channel uses (or, in this case, the number of OFDM symbols transmitted).

Then, the entire system under analysis can be modeled as M parallel Gaussian wiretap channels [4, 5], in which we assume all terminals have complete CSI about the legitimate and the eavesdropper channels. The input distribution that achieves the secrecy capacity for this kind of channels was shown to be Gaussian [3]. Nevertheless, we focus on the case in which the data symbols $u_i(k)$ are drawn uniformly from symmetric QAM constellations with finite cardinality $\mathcal{C}_i$.

3. SECRECY RATES OF A SCALAR GAUSSIAN CHANNEL WITH QAM INPUTS

We address the problem of evaluating the achievable secrecy rates of the system when the input data belong to a QAM constellation with cardinality $\mathcal{C}$. In order to do that, we consider first the case of transmissions over a scalar Gaussian wiretap channel

$$\begin{aligned} y(k) &= G_{\mathrm{R}}u(k) + w_{\mathrm{R}}(k) \\ \text{and}\quad z(k) &= G_{\mathrm{E}}u(k) + w_{\mathrm{E}}(k). \end{aligned} \tag{5}$$

and we evaluate the corresponding achievable secrecy rates. A similar framework was already studied in [18], in which the authors consider transmission of pulse amplitude modulation (PAM) symbols over Gaussian wiretap channels. The optimal transmission power for this scenario is found via an iterative algorithm that leverages the well known relationship between mutual information and the minimum mean squared error (MMSE) [20]. In this work, similarly to what has been presented in [19], we consider $\mathcal{C}$-QAM constellations in which all the symbols from the alphabet

$$\begin{aligned} \mathcal{A}_{\mathcal{C}} = \{&\alpha_n = A(2n - \sqrt{\mathcal{C}} + 1) + jA(2m - \sqrt{\mathcal{C}} + 1), \\ &n, m = 0, \ldots, \sqrt{\mathcal{C}} - 1\}, \end{aligned} \tag{6}$$

have the same probability $p_{u(k)}(\alpha_n) = 1/\mathcal{C}$, and where the amplitude A is uniquely determined by the transmission power P, as

$$P = \frac{2A^2(\mathcal{C}-1)}{3}.$$

The secrecy rate achieved by such an input over a Gaussian wiretap channel is given by

$$S = [I(u;y) - I(u;z)]^+, \tag{7}$$

in which the symbol $I(\cdot;\cdot)$ denotes the mutual information between its two arguments. In particular, we refer to the explicit definition of the mutual information in order to compute (7) as the difference of two terms as in (9) at the top of the next page.

In Figure 2 we show the secrecy rates achieved with different constellation cardinalities and the corresponding secrecy capacity, obtained with a Gaussian input. As was already highlighted in [18], when a fixed finite constellation is adopted with equally likely symbols, the optimal transmission power may not be given by the available power, since both the mutual information terms in (7) converge to $\log_2 \mathcal{C}$ when $P \to \infty$. Moreover, it is possible to notice how the transmitter must increase the cardinality of the input constellation as the values of the channel SNRs increase, in order to reduce the gap from the secrecy capacity.

In the asymptotic limit of $\mathcal{C} \to \infty$, the channel input approaches a uniform random variable taking values in a square portion of the complex plane

$$\mathcal{S}_P = \left\{ z \in \mathbb{C} : |\Re\, z|, |\Im\, z| \leq \sqrt{3P/2} \right\}. \tag{10}$$

Hence, it is possible to determine the residual loss from the secrecy capacity when the constellation cardinality is arbi-

$$I(u;y) = \mathbb{E}\left\{\log_2 \frac{f_{y|u}(y|u)}{f_y(y)}\right\} = \int_{\mathbb{C}} \sum_{n=0}^{\mathcal{C}-1} p_u(\alpha_n) f_{w_{\mathrm{R}}}(b - G_{\mathrm{R}}\alpha_n) \log_2 \frac{f_{w_{\mathrm{R}}}(b - G_{\mathrm{R}}\alpha_n)}{\sum_{m=0}^{\mathcal{C}-1} p_u(\alpha_m) f_{w_{\mathrm{R}}}(b - G_{\mathrm{R}}\alpha_m)} db \tag{8}$$

$$= \log_2 \mathcal{C} - \log_2 e + \frac{1}{\mathcal{C}\pi} \int_{\mathbb{C}} \sum_{n=0}^{\mathcal{C}-1} e^{-|b - G_{\mathrm{R}}\alpha_n|^2} \log_2 \sum_{n=0}^{\mathcal{C}-1} e^{-|b - G_{\mathrm{R}}\alpha_n|^2} db \tag{9}$$

$$I_{\mathrm{U}}(u;y) = \mathbb{E}\left\{\log_2 \frac{f_{y|u}(y|u)}{f_y(y)}\right\} = \int_{\mathbb{C}} \int_{\mathcal{S}_P} f_u(a) f_{w_{\mathrm{R}}}(b - G_{\mathrm{R}}a) \log_2 \frac{f_{w_{\mathrm{R}}}(b - G_{\mathrm{R}}a)}{\int_{\mathcal{S}_P} f_u(a') f_{w_{\mathrm{R}}}(b - G_{\mathrm{R}}a') da'} da db \tag{11}$$

$$= \log_2 \frac{1}{2\pi e} - 2 \int_{-\infty}^{\infty} \frac{1}{2|G_{\mathrm{R}}|\sqrt{3P/2}} \left[Q(b - |G_{\mathrm{R}}|\sqrt{3P/2}) - Q(b + |G_{\mathrm{R}}|\sqrt{3P/2})\right]$$

$$\cdot \log_2 \frac{1}{2|G_{\mathrm{R}}|\sqrt{3P/2}} \left[Q(b - |G_{\mathrm{R}}|\sqrt{3P/2}) - Q(b + |G_{\mathrm{R}}|\sqrt{3P/2})\right] db \tag{12}$$

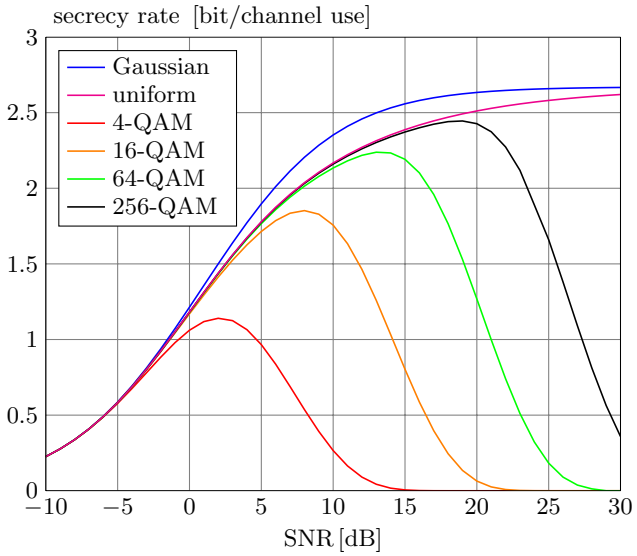

Figure 2: Typical curves of achievable secrecy rates as a function of the main channel SNR for a scalar Gaussian wiretap channel. The eavesdropper SNR is 8 dB below the main channel. The secrecy capacity (achieved with Gaussian input) is compared with the achievable rates provided by transmitting finite QAM constellation input. A QAM constellation with arbitrarily high cardinality is well approximated by a uniformly distributed input.

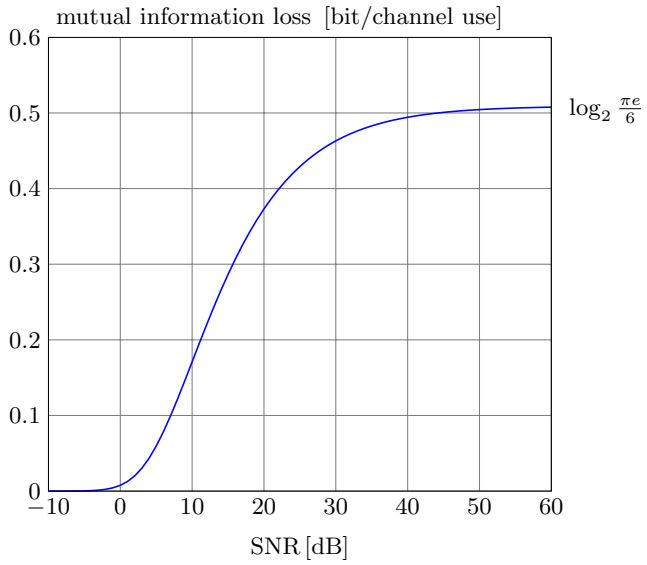

Figure 3: Difference (in bits per channel use) in the mutual information provided by a Gaussian channel with a Gaussian input and a uniformly distributed input with the same power. The difference is a function of only the SNR of the channel and it converges to the value $\log_2 \frac{\pi e}{6} \approx 0.5$ bits, when $\mathrm{SNR} \to \infty$.

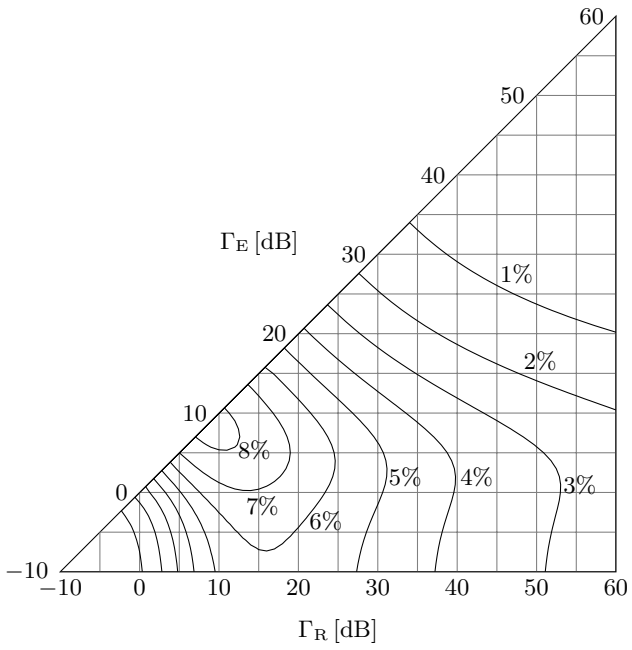

Figure 4: Contour lines of the relative loss (percentage) in the secrecy rates achieved with a uniformly distributed input with respect to the secrecy capacity yielded by the optimal Gaussian input.

trarily high, by evaluation of the mutual information between a uniform input and the corresponding output of a Gaussian channel (12), in which $Q(b) = \frac{1}{\sqrt{2\pi}} \int_b^{+\infty} e^{-a^2/2} da$ is the complementary cumulative distribution function (CDF) of the normal distribution.

The achievable information rates obtained with equiprobable symbols belonging to finite PAM constellations were reported, for example, in [21]. Through the analysis of multidimensional constellations, it was shown that the loss incurred by using a uniform distribution with respect to a Gaussian input (the *shape factor*), translates into an SNR loss of $\pi e/6 \approx 1.53\,\text{dB}$ in the high SNR regime.

For a uniform input over the complex square $\mathcal{S}_P$ the loss in mutual information from the circularly symmetric zero-mean Gaussian input, i.e.

$$\Delta = I_{\rm G}(u;y) - I_{\rm U}(u;y), \tag{13}$$

can be determined by numerical evaluation of the integral in (12) and is reported in Figure 3 as a function of the SNR. Consistently with the result in [21], Δ is a non-decreasing function of the SNR and it asymptotically achieves the value $\log_2 \frac{\pi e}{6} \approx 0.51$ bit. The difference between the values of the function Δ at the main and the eavesdropper channel SNRs, $\Gamma_{\rm R}$ and $\Gamma_{\rm E}$ respectively, yields the loss incurred in the achievable secrecy rates of the system by using a uniform input. In Figure 4 we illustrate the relative loss in the secrecy rates with respect to the Gaussian input secrecy capacity. The maximum relative loss is approximately 8% when $\Gamma_{\rm R} \approx 10$ dB, $\Gamma_{\rm E} \approx 7$ dB.

4. QAM BIT-ALLOCATION FOR SECRECY RATES OVER OFDM

The results presented in Section 3 illustrate the importance of choosing the appropriate QAM transmission constellations when using secrecy coding. Then, when multicarrier transmissions are implemented, the problem of bit-loading over the different subcarriers turns out to be fundamental, and efficient algorithms available in the literature for throughput maximization without secrecy constraints do not prove effective also in the secrecy scenario. In this section, we will present different bit allocation policies and we will compare their effectiveness in terms of achievable secrecy rates and number of used bits.

To find the optimal bit-allocation under a total bit number constraint represents a non-convex optimization problem with hard solutions. Hence, we present methods that move from the insights given by the analysis carried out so far, but that are not optimal in general.

Specifically, we assume that the transmitter has complete CSI about the legitimate and eavesdropper channel gains. Hence, the transmitter computes the optimal power allocation when assuming Gaussian input [4] and the corresponding secrecy rates achieved over the M subchannels. Namely, on denoting

$$a_i = \frac{1}{|G_{\rm E}(f_i)|^2} - \frac{1}{|G_{\rm R}(f_i)|^2} \quad \text{and} \quad b_i = \frac{1}{|G_{\rm E}(f_i)|^2} + \frac{1}{|G_{\rm R}(f_i)|^2}$$

the optimal power allocation for Gaussian inputs becomes

$$P_i^* = \begin{cases} 0 & , \quad |G_{\rm R}(f_i)| \le |G_{\rm E}(f_i)| \\ \left[\sqrt{\frac{a_i^2}{4} + \frac{a_i}{\lambda}} - \frac{b_i}{2}\right]^+ & , \quad |G_{\rm R}(f_i)| > |G_{\rm E}(f_i)| \end{cases} \tag{14}$$

with $\lambda > 0$ such that

$$\sum_{i=1}^{M} P_i^* \le P_{\rm tot}\ . \tag{15}$$

4.1 Secrecy capacity bit-allocation

The first method we present determines the number of bits to allocate to each subcarrier, based on the corresponding secrecy rate provided by each subchannel. Then, given the secrecy rate that is achievable in each subchannel with Gaussian input

$$S_{\rm G}(i) = [\log_2(1 + |G_{\rm R}(f_i)|^2 P_i^*) - \log_2(1 + |G_{\rm E}(f_i)|^2 P_i^*)]^+, \tag{16}$$

the number of bits to allocate to the ith channel is chosen as

$$\ell_{\rm SC}(i) = 2\lceil R_{\rm G}(i)/2 \rceil. \tag{17}$$

This approach grounds its motivation on the attempt to use approximately as few bits as the secure bits per channel use provided by the different subchannels, in order to reduce the constellation size.

4.2 Main channel rate bit-allocation

A more bit-consuming policy for the bit-allocation problem is suggested by the coding scheme that is adopted to provide secure communication over a degraded Gaussian chan-

nel; that is, random binning [3]. This scheme is based on the transmission of randomized information, with a rate equal to the main channel information rate. Then, moving from this observation, we consider again the optimal power allocation for the Gaussian input and the corresponding mutual information over the main channel

$$R_{\mathrm{G}}(i) = \log_2(1 + |G_{\mathrm{R}}(f_i)|^2 P_i^*). \tag{18}$$

Then, the number of bit composing the symbols transmitted over the ith channel is given by

$$\ell_{\mathrm{MC}}(i) = 2\lceil R_{\mathrm{G}}^{\mathrm{R}}(i)/2 \rceil. \tag{19}$$

It is evident that, for any channel realization, $\ell_{\mathrm{MC}}(i) \geq \ell_{\mathrm{SC}}(i)$, $\forall i$. Therefore, this scheme will provide higher secrecy rates then those provided by the method in Section 4.1 at the expense of a higher decoding complexity. Our aim is to determine which solution can be considered more suitable for different tradeoff targets.

4.3 MMSE bit-allocation

A third possible bit-allocation strategy is based on the behavior reported in Figure 2 and the analysis carried in [18] for the scalar Gaussian wiretap channel. In particular, it appears clear that the most critical losses in using finite QAM constellations for secret transmissions are experienced whenever the transmission power exceeds the optimal power allocation reported in [18] and the corresponding secrecy rate starts to decrease. The optimal transmission power for this case, $\tilde{P}$, was shown to satisfy the following relationship[1]

$$|G_{\mathrm{R}}|^2 \mathrm{mmse}(\ell, |G_{\mathrm{R}}|^2 \tilde{P}) = |G_{\mathrm{E}}|^2 \mathrm{mmse}(\ell, |G_{\mathrm{E}}|^2 \tilde{P}), \tag{20}$$

in which we have denoted by $\mathrm{mmse}(\ell, |G|^2 P)$ the MMSE estimation error encountered when estimating the 2^ℓ-QAM input u from the output of a Gaussian scalar channel with SNR equal to $|G|^2 P$.

As we have done for the algorithms in Sections 4.1 and 4.2, we decide to transmit adopting the optimal power allocation for Gaussian input (14) and we choose the corresponding constellation cardinality in order to guarantee that the secrecy rate of each subchannel is still in its interval of increase. Namely,

$$\begin{aligned} \ell_{\mathrm{MMSE}}(i) &= \min\{\ell : \tilde{P}_i \geq P_i^*\} \\ &= \min\{\ell : |G_{\mathrm{R}}(f_i)|^2 \mathrm{mmse}(\ell, |G_{\mathrm{R}}(f_i)|^2 P_i^*) \\ &\quad \geq |G_{\mathrm{E}}(f_i)|^2 \mathrm{mmse}(\ell, |G_{\mathrm{E}}(f_i)|^2 P_i^*)\}. \end{aligned} \tag{21}$$

This method turns out to be computationally more complex than the previous ones, as it requires the numerical solution of M equations of the type of (20). Nevertheless, the search for these roots can be performed with efficient iterative algorithms, such as bisection, secant, or Newton, since each equation has a unique solution $\tilde{P}$ and the difference $|G_{\mathrm{R}}|^2 \mathrm{mmse}(\ell, |G_{\mathrm{R}}|^2 P) - |G_{\mathrm{E}}|^2 \mathrm{mmse}(\ell, |G_{\mathrm{E}}|^2 P)$ is monotonically decreasing in the interval $0 < P < \tilde{P}$ [18]. On the other hand, this algorithm guarantees, for each subchannel, a limited loss.

[1]Eq. (20) was proved in [18] for the case of PAM transmission, but its generalization to the QAM constellation case is straightforward.

4.4 Numerical results

In the following, we compare the effectiveness of the bit-loading policies presented in the previous sections with two other, more naïve, approaches that do not need complete CSI about the eavesdropper channel to allocate power and bits among the available subcarriers. In particular, we consider a blind method in which the transmission power is distributed according to the waterfilling principle [22] with respect to the main channel,

$$P_i^{\mathrm{W}} = \left[\mu - \frac{1}{|G_{\mathrm{R}}(f_i)|^2}\right]^+,$$

with $\mu \geq 0$ such that $\sum_{i=1}^M P_i^{\mathrm{W}} \leq P_{\mathrm{tot}}$. Then, the number of bits constituting the ith QAM constellation is

$$\ell_{\mathrm{W}}(i) = 2\lceil \log_2(1 + |G_{\mathrm{R}}(f_i)|^2 P_i^{\mathrm{W}})/2 \rceil. \tag{22}$$

Finally, for the sake of comparison, we also evaluate the secrecy rate obtained by simply allocating power and bits uniformly over all the available subcarriers:

$$P_i^{\mathrm{U}} = P_{\mathrm{tot}}/M \quad \text{and} \quad \ell_{\mathrm{U}}(i) = 2\left\lceil \frac{1}{2M} \sum_{i=1}^M \ell_{\mathrm{MC}}(i) \right\rceil.$$

The effectiveness of the different algorithms under analysis is assessed by considering jointly the following two efficiency metrics. First, for each bit-allocation strategy we define the *secrecy rate efficiency* η_{S} as the ratio between the achievable secrecy rate provided by QAM inputs and the corresponding secrecy capacity of the same parallel Gaussian channel realization, that is

$$\eta_{\mathrm{S}} = \frac{\sum_{i=1}^M S(i)}{\sum_{i=1}^M S_{\mathrm{G}}(i)}.$$

On the other hand we take into account the number of bits introduced to reduce the loss from the optimal Gaussian perfomance by measuring the ratio between the achievable secrecy rate and the total number of bits used over the M subcarriers, which we call *bit allocation efficiency*:

$$\eta_{\mathrm{B}} = \frac{\sum_{i=1}^M S(i)}{\sum_{i=1}^M \ell(i)}.$$

In Figures 5 and 6 we show the CDF curves of the rate efficiency and the bit efficiency yielded by the bit-loading methods described in the previous sections. We have considered an OFDM system with $M = 16$ subcarriers. Both the legitimate receiver and the eavesdropper channels experienced independent Rayleigh fading over each subchannel. The average SNR for both channels was set to $\Gamma_{\mathrm{R}} = \Gamma_{\mathrm{E}} = 10$ dB.

When observing Figure 5, it is immediately clear that the bit-allocation strategy based on the secrecy capacity values of the subchannels (SC-ba) cannot provide secrecy rates close to the optimal secrecy capacity of the system, and higher cardinality constellations are needed in order to allow an effective coding of the secret message to transmit. Even a blind power and bit-allocation protocol seems to outperform this approach in terms of rate efficiency, though at the expense of a higher number of bits used. On the other hand, loading the subcarriers according to the information rate of

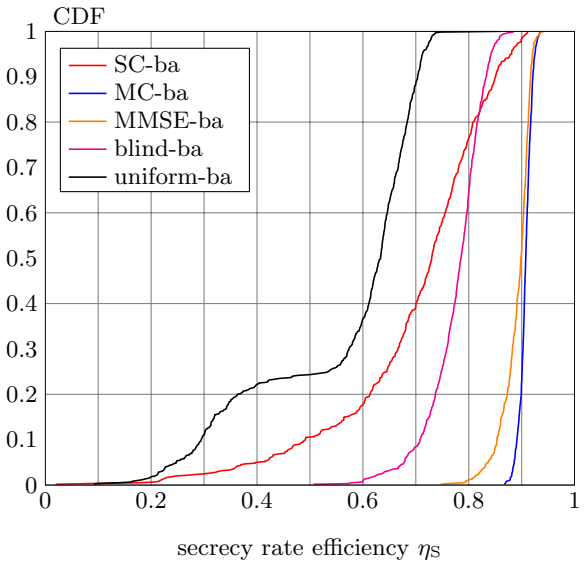

Figure 5: CDF of the secrecy rate efficiency η_S for the different bit-allocation algorithms. $M = 16$ subcarriers and the average SNR for both main and eavesdropper channel is $\Gamma_R = \Gamma_E = 10$ dB.

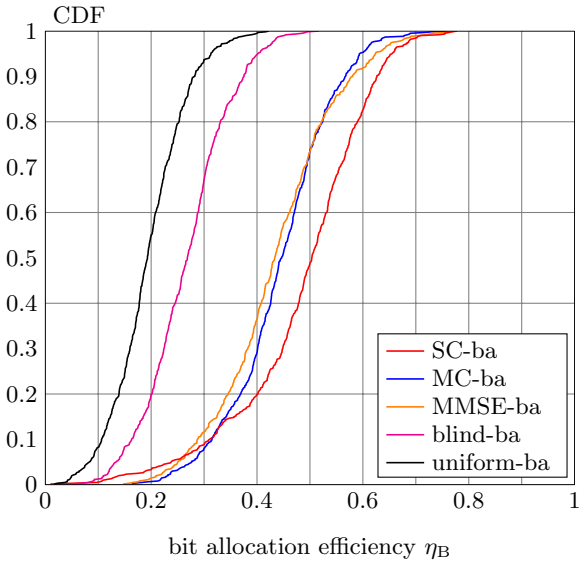

Figure 6: CDF of the bit allocation efficiency η_B for the different bit-allocation algorithms. $M = 16$ subcarriers and the average SNR for both main and eavesdropper channel is $\Gamma_R = \Gamma_E = 10$ dB.

the main channel with secrecy capacity achieving power allocation (MC-ba) guarantees losses around 10% with respect to the secrecy capacity of the system. Hence, this is quite close to the uniform distribution limit discussed in Section 3.

On the other hand, this method has a bit efficiency that is similar to that obtained with the MMSE-based bit-allocation of Section 4.3, as reported in Figure 6. Therefore, the evaluation of the mutual information rate on the main channel seems to be the most effective guideline in determining the suitable bit-loading for secure transmissions.

5. CONCLUSIONS

In this work we have considered the problem of evaluating achievable secrecy rates for OFDM systems with QAM input constellations. We have assumed that also the eavesdropper implements an OFDM receiver, thus modeling the entire systems as a parallel Gaussian wiretap channel, with complete CSI available to all the terminals. The loss introduced by using uniformly distributed QAM symbols can be reduced by augmenting the constellation cardinality, but it cannot be completely eliminated. The uniform distribution *shape factor* affects the secrecy performance of the system. The residual loss experienced when $\mathcal{C} \to \infty$ has been determined by assuming inputs uniform distributed over a square portion of the complex plane and it has been expressed as a function of the legitimate receiver and eavesdropper channel SNRs.

Aiming to target the bounds set by this asymptotic analysis, we have compared different bit-allocation policies for OFDM systems. Their performance has been evaluated in terms of achievable secrecy rates and the total number of bits used. To adjust the subchannel constellation cardinalities according to the corresponding secrecy capacities implies serious losses in the achievable secrecy rates. On the other hand, by leveraging the well known relationship between mutual information and the MMSE, these losses can be avoided. Namely, it is possible to adapt each constellation cardinality in order to always set the transmission power into the region when the secrecy rate is increasing. Nonetheless, an even simpler bit-loading algorithm based on the information rate of the main channel has been shown to provide performance that is closer to the asymptotic uniform distribution limit, without requiring an increase in the number of bits used among the subcarriers.

As possible future work, we aim to propose computationally efficient bit and power-loading protocols that jointly optimize the bit and power allocation among subchannels while satisfying given constraints on the total number of bits used. Moreover, we wish to extend our analysis (and the design of suitable bit-loading algorithms) to the case in which the eavesdropper is allowed to adopt a more sophisticated receiver then the standard OFDM receiver.

6. REFERENCES

[1] A. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1367, Oct. 1975.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*. Dordrecht, The Netherlands: Now Publishers, 2009.

[11] 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.

[12] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[13] 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. Petersburg, Russia, Jun. 2008.

[14] 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.

[15] F. Renna, N. Laurenti, and H. V. Poor, "Physical layer secrecy for OFDM systems," in *Proc. European Wireless Conference*, Lucca, Italy, Apr. 2010.

[16] ——, "High SNR secrecy rates with OFDM signaling over fading channels," in *Proc. IEEE PIMRC '10*, Istanbul, Turkey, Sep. 2010.

[17] ——, "Physical layer secrecy for OFDM transmissions over fading channels," submitted to *IEEE Trans. on Information Forensics and Security*, special issue on physical layer security.

[18] M. R. D. Rodrigues, A. Somekh-Baruch, and M. Bloch, "On Gaussian wiretap channels with M-PAM inputs," in *Proc. European Wireless Conference*, Lucca Italy, Apr. 2010.

[19] G. D. Raghava and B. Sundar Rajan, "Secrecy capacity of the Gaussian wire-tap channel with finite complex constellation input," [Online]. Available: http://arxiv.org/abs/1010.1163v1.

[20] D. Guo, S. Shamai (Shitz), and S. Verdú, "Mutual information and minimum mean-square error in Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1261–1282, Apr. 2005.

[21] G. D. Forney, Jr. and G. Ungerboeck, "Modulation and coding for linear Gaussian chennels," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2384–2415, Oct. 1998.

[22] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York, NY, USA: Wiley-Interscience, 2006.