Secrecy Capacity of FBMC-OQAM Modulation over Frequency Selective Channel

François Rottenberg, Philippe De Doncker, François Horlin and Jérôme Louveaux

Abstract—This paper studies the information-theoretic secrecy capacity of an Offset-QAM-based filterbank multicarrier (FBMC-OQAM) communication over a wiretap frequency selective channel. The secrecy capacity is formulated as an optimization problem which has a closed-form solution in the high signal-to-noise ratio (SNR) regime. Two of the most common equalization strategies in FBMC-OQAM are considered, namely, single-tap and multi-tap equalization. For the sake of comparison, we also consider the secrecy capacity of a generic modulation and a cyclic prefix-orthogonal frequency division multiplexing (CP-OFDM) modulation. As a result, we find that FBMC-OQAM is particularly competitive for medium-to-long burst transmissions.

Keywords—FBMC-OQAM, secrecy capacity, multipath channel.

I. INTRODUCTION

The information-theoretic secrecy-capacity is defined as the number of bits per channel use that can be reliably transmitted from a legitimate transmitter (Alice) to a legitimate receiver (Bob) while guaranteeing a negligible information leakage to the eavesdropper (Eve). The seminal work of Wyner [1] and its extension to more general channels [2], have shown that a "physical advantage" at Bob with respect to Eve is required to guarantee a larger-than-zero secrecy capacity. Multipath channels lead to channel frequency selectivity. If Alice knows the channel of Bob and Eve, she can modulate her signal to take benefit of frequency bins where Bob's channel has an advantage over Eve's channel. This scenario has been studied in details in the case of multicarrier modulations, including CP-OFDM [3]–[5].

However, to the best of the authors knowledge, we are the first to analyze the secrecy capacity of the FBMC-OQAM modulation, which has received increasing attention in the last decades as an attractive alternative to CP-OFDM modulation [6]. In this paper, we consider that Alice and Bob communicate over a frequency selective channel using FBMC-OQAM modulation/demodulation while Eve tries to eavesdrop on the conversation. Based on this model, we formulate the secrecy capacity as an optimization problem that can be solved in closed-form at high SNR. At Bob side, two of the most common equalization strategies in FBMC-OQAM are considered, namely, multi-tap and single-tap equalization [7]. We demonstrate that both equalization schemes lead to equivalent performance for mildly frequency selective channels. At Eve side, we additionally consider the loss in secrecy occuring if she is not constrained to apply conventional FBMC-OQAM demodulation. For the sake of comparison, we also consider the secrecy capacity of a generic modulation and a CP-OFDM modulation. In the
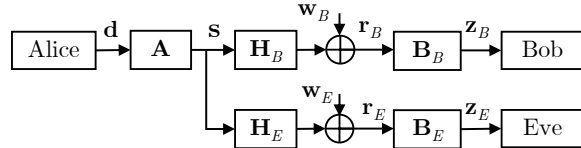
Fig. 1: Transmission model over multipath channel equivalent to a special case of MIMO wiretap channel.

end, we show that FBMC-OQAM is particularly competitive for medium-to-long burst transmissions.

Notations: Vectors and matrices are denoted by bold lowercase and uppercase letters $\mathbf{a}$ and $\mathbf{A}$, respectively (resp.). Superscripts $*$, T, H and $\dagger$ stand for conjugate, transpose, Hermitian transpose and Moore-Penrose pseudo-inverse. The symbols $\text{tr}[.]$, $\mathbb{E}(.)$, $\Im(.)$ and $\Re(.)$ denote the trace, expectation, imaginary and real parts, respectively. $\jmath$ is the imaginary unit. $\|\mathbf{A}\|$ and $|\mathbf{A}|$ are the Frobenius norm and determinant respectively. $\mathbf{I}_N$ denotes the identity matrix of order N. $\mathbf{0}_{N \times M}$ is a zero matrix of size $N \times M$. Subscripts of matrices are dropped whenever matrix dimensions are clear from the context. $\text{diag}(\mathbf{a})$ returns a diagonal matrix with $\mathbf{a}$ on its diagonal. The positive part of a real quantity is denoted by $[a]^+ = \max(a, 0)$. $\sigma_n(\mathbf{A})$ (or $\lambda_n(\mathbf{A})$) is the n-th largest singular (or eigenvalue) of $\mathbf{A}$. $\otimes$ stands for the Kronecker product.

II. SYSTEM MODEL

As depicted in Fig. 1, we consider a conventional wiretap channel where Alice wants to communicate secretly with Bob while Eve tries to eavesdrop on the communication. Alice transmits a group of symbols $\mathbf{d}$, modulated with matrix $\mathbf{A}$ as $\mathbf{s} = \mathbf{A}\mathbf{d}$ where $\mathbf{s} \in \mathbb{C}^{N \times 1}$. We consider a constraint on the power of the transmitted signal so that $\text{tr}[\mathbf{R}_s] \leq P$ with $\mathbf{R}_s = \mathbb{E}(\mathbf{s}\mathbf{s}^H) \in \mathbb{C}^{N \times N}$. The channel is modeled as a multipath channel that is considered quasi-static, *i.e.*, it remains constant over the duration of the N symbols. The channel impulse responses from Alice to Bob and Eve are denoted by $h_B[n]$ and $h_E[n]$ respectively, of length L_B and L_E, and are assumed to be known by Alice, which is a common assumption [8]. The knowledge of Bob's channel can be acquired in practice through pilots and feedback, or based on channel reciprocity in time division duplexing mode. On the other hand, the knowledge of Eve's channel is a stronger assumption as she might remain passive. However, if she is an active network node, Alice may also have knowledge of her channel in the same way as Bob. The vector of received samples at Bob and Eve are denoted by $\mathbf{r}_B \in \mathbb{C}^{N + L_B - 1 \times 1}$ and $\mathbf{r}_E \in \mathbb{C}^{N + L_E - 1 \times 1}$. The multipath channel can be modeled as a special case of the multiple-input-multiple-output (MIMO) wiretap channel [9]

$$\mathbf{r}_B = \mathbf{H}_B \mathbf{s} + \mathbf{w}_B, \ \mathbf{r}_E = \mathbf{H}_E \mathbf{s} + \mathbf{w}_E, \quad (1)$$

where the "MIMO" channel matrix $\mathbf{H}_B \in \mathbb{C}^{N + L_B - 1 \times N}$ has a Toeplitz structure with vector $(h_B[0], \dots, h_B[L_B -$

$1], \mathbf{0}_{1 \times N-1})^T$ as its first column and analogously for $\mathbf{H}_E \in \mathbb{C}^{N+L_E-1 \times N}$. Note that $\mathbf{H}_B$ and $\mathbf{H}_E$ are both full rank by construction. The noise vectors $\mathbf{w}_B \in \mathbb{C}^{N+L_B-1 \times 1}$ and $\mathbf{w}_E \in \mathbb{C}^{N+L_E-1 \times 1}$ are modeled as zero mean circularly-symmetric complex Gaussian (ZMCSCG) vector with covariance $\mathbf{I}_{N+L_B-1}$ and $\mathbf{I}_{N+L_E-1}$ respectively. The normalization choice of a unit noise variance simplifies exposition and is not a loss of generality since a difference in SNR can be captured through a scaled channel gain. Bob (resp. Eve) applies matrix $\mathbf{B}_B$ (resp. $\mathbf{B}_E$) to demodulate and equalize the received samples, obtaining $\mathbf{z}_B$ (resp. $\mathbf{z}_E$).

III. GENERIC SECRECY CAPACITY

In this section, we are interested in the secrecy capacity without imposing any constraint on the transmitter and the receiver implying that $\mathbf{A}$, $\mathbf{B}_B$ and $\mathbf{B}_E$ are identity matrices. Using the general result of [2], the secrecy capacity of the MIMO wiretap model of (1), under the power constraint $\mathrm{tr}\left[\mathbf{R}_s\right] \leq P$, can be written as

$$C_s = \max_{p(\mathbf{s},v),\mathrm{tr}[\mathbf{R}_s]\leq P} I(v;\mathbf{r}_B) - I(v;\mathbf{r}_E), \qquad (2)$$

where $I(.;.)$ is the mutual information, v is an auxiliary random variable defined such that $p(\mathbf{r}_B,\mathbf{r}_E|\mathbf{s},v) = p(\mathbf{r}_B,\mathbf{r}_E|\mathbf{s})$ with $p(.)$ being the probability density function. The result of [10] states that the secrecy capacity of the general Gaussian MIMO wiretap channel (1) is attained without channel prefixing ($v = \mathbf{s}$) and $\mathbf{s}$ has to follow a ZMCSCG with covariance matrix $\mathbf{R}_s$. Using this result, (2) can be further detailed so that the secrecy capacity and the covariance matrix $\mathbf{R}_s$ can be obtained by maximizing

$$C_s = \max_{\mathbf{R}_s,\mathrm{tr}[\mathbf{R}_s]\leq P} \log \frac{\left|\mathbf{I} + \mathbf{H}_B \mathbf{R}_s \mathbf{H}_B^H\right|}{\left|\mathbf{I} + \mathbf{H}_E \mathbf{R}_s \mathbf{H}_E^H\right|}. \qquad (3)$$

This maximization problem is well known to be non convex and no general closed-form solution exists [11]. Still, in the high SNR regime, a closed-form solution of C_s exists. The generalized singular value decomposition of the matrix pair $(\mathbf{H}_B, \mathbf{H}_E)$ allows us to decompose the MIMO wiretap channel into a set of parallel independent Gaussian wiretap channels. This is analogous to the case with no eavesdropper, where classical singular value decomposition allows to convert the MIMO channel in a set of independent parallel channels. Using the result of [11, Th. 2] in the case of $\mathrm{Ker}(\mathbf{H}_E) \cap \mathrm{Ker}(\mathbf{H}_B)^{\perp} = \varnothing$ (since $\mathbf{H}_B$ and $\mathbf{H}_E$ are of full rank), we find

$$\lim_{P\to+\infty} C_s = \sum_{n=1}^{N} \left[\log \sigma_n^2\left(\mathbf{H}_B \mathbf{H}_E^{\dagger}\right)\right]^+ = \sum_{n=1}^{N} \left[\log \lambda_n\left(\mathbf{C}_N\right)\right],$$

where $\mathbf{C}_N = \mathbf{H}_B^H \mathbf{H}_B (\mathbf{H}_E^H \mathbf{H}_E)^{-1}$. The fact that $\mathrm{Ker}(\mathbf{H}_E) \cap \mathrm{Ker}(\mathbf{H}_B)^{\perp} = \varnothing$ directly implies that Alice cannot communicate secretly with Bob by modulating her signal such that it lies in the null space of Eve. Still, Alice can transmit in channel modes where the gain at Bob is higher than Eve but the secrecy capacity remains bounded as the SNR grows large. This in contrast with the multi-antenna case where Alice can use spatial beamforming to transmit in the null space of Eve so that the capacity can be unbounded as the SNR grows large [11].

Using the asymptotic properties of Toeplitz matrices, the authors in [5] have further characterized the limiting behavior of the latest expression as the number of symbols N in $\mathbf{s}$ grows large

$$\lim_{N\to+\infty} \frac{1}{N} \sum_{n=1}^{N} \left[\log \lambda_n\left(\mathbf{C}_N\right)\right]^+ = \int_0^1 \left[\log \frac{|H_B(f)|^2}{|H_E(f)|^2}\right]^+ df,$$

with $H_B(f) = \sum_{n=0}^{L_B-1} h_B[n]e^{-j2\pi fn}$ and $H_E(f) = \sum_{n=0}^{L_E-1} h_E[n]e^{-j2\pi fn}$.

IV. SECRECY CAPACITY OF CP-OFDM

This section details the CP-OFDM secrecy capacity, as was done in [5]. We assume that the cyclic prefix (CP) length L_{CP} is larger than $L_B - 1$ and $L_E - 1$. Under that condition, successive OFDM blocks do not interfere and it is sufficient to consider a single OFDM symbol that we denote by $\mathbf{d} \in \mathbb{C}^{M \times 1}$ where $M = N - L_{CP}$ is the number of subcarriers. The CP-OFDM modulation imposes the following structure on the transmitted symbols

$$\mathbf{s} = \mathbf{A}\mathbf{d}, \quad \mathbf{A} = \begin{pmatrix} \mathbf{0} & \mathbf{I}_{L_{CP}} \\ \mathbf{I}_M \end{pmatrix} \mathbf{F}^H,$$

where $\mathbf{F} \in \mathbb{C}^{M \times M}$ is the unitary FFT matrix. Note that the total power is not equal before/after CP insertion so that the transmit power constraint becomes $\mathrm{tr}\left[\mathbf{R}_s\right] = \mathrm{tr}[\mathbf{A}\mathbf{R}_d\mathbf{A}^H] \leq P$. At the receiver, Bob uses conventional OFDM demodulation, *i.e.*, CP removal and FFT

$$\mathbf{z}_B = \mathbf{B}_B \mathbf{r}_B = \mathbf{D}_B \mathbf{d} + \tilde{\mathbf{w}}_B,$$

with

$$\mathbf{B}_B = \mathbf{F}\left(\mathbf{0}_{M\times L_{CP}} \; \mathbf{I}_M \; \mathbf{0}_{M\times L_B-1}\right)$$
$$\mathbf{D}_B = \mathbf{B}_B \mathbf{H}_B \mathbf{A} = \mathrm{diag}\left(H_B(f_0),...,H_B(f_{M-1})\right)$$
$$\tilde{\mathbf{w}}_B = \mathbf{B}_B \mathbf{w}_B,$$

and $f_m = m/M$. At Eve side, two cases can be distinguished for its receiver structure $\mathbf{B}_E$: 1) Eve uses a generic (ideal) receiver in which case $\mathbf{B}_E = \mathbf{I}$ or 2) Eve uses conventional (sub-optimal) OFDM demodulation as Bob implying that $\mathbf{B}_E = \mathbf{B}_B$. It was shown in [5] that the secrecy capacity is attained if symbols $\mathbf{d}$ are ZMCSCG. Then, the secrecy capacity can be written as

$$C_s^{\mathrm{OFDM}} = \max_{\mathbf{R},\mathrm{tr}[\mathbf{R}]\leq P} \log \frac{\left|\mathbf{I} + \mathbf{T}_B \mathbf{R} \mathbf{T}_B^H\right|}{\left|\mathbf{I} + \mathbf{T}_E \mathbf{R} \mathbf{T}_E^H\right|},$$

where $\mathbf{T}_B = \mathbf{D}_B \mathbf{C}^{-1/2}$ and $\mathbf{T}_E = \mathbf{B}_E \mathbf{H}_E \mathbf{A} \mathbf{C}^{-1/2}$ with $\mathbf{C} = \mathbf{A}^H \mathbf{A}$. The optimal input covariance matrix $\mathbf{R}_d = \mathbb{E}(\mathbf{d}\mathbf{d}^H)$ is related to matrix $\mathbf{R}$ as $\mathbf{R}_d = \mathbf{C}^{-1/2}\mathbf{R}\mathbf{C}^{-1/2}$. Using again the result of [11, Th. 2], the secrecy capacity at high SNR becomes

$$\lim_{P\to+\infty} C_s^{\mathrm{OFDM}} = \sum_{m=1}^{M} \left[\log \sigma_m^2\left(\mathbf{T}_B \mathbf{T}_E^{\dagger}\right)\right]^+.$$

If Eve uses a conventional CP-OFDM receiver ($\mathbf{B}_E = \mathbf{B}_B$), we have $\mathbf{T}_E = \mathbf{D}_E \mathbf{C}^{-1/2}$ with $\mathbf{D}_E$ defined analogously as $\mathbf{D}_B$, implying that

$$\lim_{P\to+\infty} C_s^{\mathrm{OFDM}} = \sum_{m=1}^{M} \left[\log \frac{|H_B(f_m)|^2}{|H_E(f_m)|^2}\right]^+,$$

which is equivalent to the secrecy capacity of M parallel independent wiretap channels. For a fixed L_{CP}, as M grows large (and thus N), the sum converges to an integral and the OFDM secrecy capacity will converge to the generic one.

V. Secrecy Capacity of FBMC-OQAM

We consider an FBMC-OQAM system with M subcarriers and N_s multicarrier symbols. The real-valued multicarrier symbols, denoted by $d_{m,l}$ with $m = 0, ..., M - 1$ and $l = 0, ..., N_s - 1$, are modulated using a prototype pulse $g[n]$ of length $M\kappa$, where κ is the so-called overlapping factor, i.e., $g[n] = 0$ if $n \notin [0, M\kappa - 1]$. The FBMC-OQAM modulated signal can be expressed as [7, Section 2.1]

$$s[n] = \sum_{m=0}^{M-1} \sum_{l=0}^{N_s-1} d_{m,l} j^{m+l} g[n - lM/2] e^{j\frac{2\pi}{M}m(n - \frac{M\kappa-1}{2})},$$

for $n = 0, ...N - 1$ with $N = (N_s + 2\kappa - 1)M/2$. Note that real-valued multicarrier symbols are spaced only $M/2$ samples apart in time instead of $M + L_{CP}$ for complex symbols in CP-OFDM so that the spectral efficiency is similar for both modulations. To be exact, the CP-OFDM spectral efficiency is penalized by the CP insertion. On the other hand, the FBMC-OQAM spectral efficiency is impacted by tails of length $(2\kappa - 1)M/2$ due to the spread of $g[n]$ over multiple multicarrier symbols, which induces an overhead particularly detrimental for small bursts but negligible for long burst (as N_s grows large). Similarly as the capacity analysis in [12], we reformulate the transmit signal using a matrix formalism giving

$$\mathbf{s} = \mathbf{A}\tilde{\mathbf{d}},$$

where

$$\tilde{\mathbf{d}} = \begin{pmatrix} \mathbf{d}_0 \\ \vdots \\ \mathbf{d}_{N_s-1} \end{pmatrix} \in \mathbb{R}^{MN_s \times 1}, \ \mathbf{d}_l = \begin{pmatrix} d_{0,l} \\ \vdots \\ d_{M-1,l} \end{pmatrix} \in \mathbb{R}^{M \times 1},$$

and matrix $\mathbf{A} \in \mathbb{C}^{N \times MN_s}$ is defined as follows: the element located at the n-th row and $m + lM$-th column is given by $j^{m+l} g[n - lM/2] e^{j\frac{2\pi}{M}m(n - \frac{M\kappa-1}{2})}$. At the receiver side, the legitimate receiver, Bob, discards the last $L_B - 1$ symbols, using matrix $\mathbf{S}_B = (\mathbf{I}_N, \ \mathbf{0}_{N \times L_B - 1})$ and demodulates the signal by applying matrix $\mathbf{A}^H$. If the filter $g[n]$ has perfect reconstruction properties, this leads to the identity $\Re(\mathbf{A}^H \mathbf{A}) = \mathbf{I}_{MN_s}$, so that, under ideal propagation condition and synchronization ($\mathbf{H}_B = \mathbf{I}$, $\mathbf{S}_B = \mathbf{I}$ and $\mathbf{w}_B = \mathbf{0}$), the transmit symbols are recovered after demodulation and real conversion.

In practice however, the multipath channel must be equalized before real conversion to avoid inter-symbol and inter-carrier interference. The obtained samples at Bob and Eve can generally be written as

$$\mathbf{z}_B = \mathbf{B}_B \mathbf{H}_B \mathbf{A}\tilde{\mathbf{d}} + \mathbf{B}_B \mathbf{w}_B, \ \mathbf{z}_E = \mathbf{B}_E \mathbf{H}_E \mathbf{A}\tilde{\mathbf{d}} + \mathbf{B}_E \mathbf{w}_E.$$

The equalizer can be designed in many different ways, see [7, Section 2.1.5] for a review. The most conventional way consists in single-tap per-subcarrier equalization as in CP-OFDM. However, as the channel becomes more selective in frequency, the system will be impacted by inter-symbol and inter-carrier interference. Improved equalizer designs rely on a multi-tap structure to estimate the current symbol $d_{m,l}$

based on demodulated symbols at neighboring multicarrier symbols and subcarriers. In the following, we will first derive the FBMC-OQAM secrecy capacity for general matrices $\mathbf{B}_B$ and $\mathbf{B}_E$. We will then consider different types of equalizers at Bob and Eve.

Before going further, one should note that vector $\tilde{\mathbf{d}}$ is real-valued and hence $\mathbb{E}(\tilde{\mathbf{d}}\tilde{\mathbf{d}}^T) \neq \mathbf{0}$ so that vectors $\mathbf{z}_B$ and $\mathbf{z}_E$ are improper, i.e., $\mathbb{E}(\mathbf{z}_B \mathbf{z}_B^T) \neq \mathbf{0}$ and $\mathbb{E}(\mathbf{z}_E \mathbf{z}_E^T) \neq \mathbf{0}$. Hence, conventional results for the complex circularly symmetric Gaussian case do not hold. Therefore, we introduce the following real-valued notations for matrices and vectors: for arbitrary vector $\mathbf{v}$ and matrix $\mathbf{V}$, vector $\mathbf{v}_r$ and matrix $\mathbf{V}_r$ are defined as

$$\mathbf{v}_r = \begin{pmatrix} \Re(\mathbf{v}) \\ \Im(\mathbf{v}) \end{pmatrix}, \ \mathbf{V}_r = \begin{pmatrix} \Re(\mathbf{V}) & -\Im(\mathbf{V}) \\ \Im(\mathbf{V}) & \Re(\mathbf{V}) \end{pmatrix}.$$

Subscript "r" stands for real-valued. We also define $\tilde{\mathbf{I}} = (\mathbf{I}_{MN_s} \ \mathbf{0}_{MN_s \times MN_s})^T$. Using these definitions, the perfect reconstruction property becomes $\tilde{\mathbf{I}}^T \mathbf{A}_r^T \mathbf{A}_r \tilde{\mathbf{I}} = \mathbf{I}_{MN_s}$ and the power constraint on transmitted symbols $\mathbf{s} = \mathbf{A}_r \tilde{\mathbf{I}} \tilde{\mathbf{d}}$ directly translates into a constraint on symbols $\tilde{\mathbf{d}}$

$$\text{tr}[\mathbf{R}_s] = \text{tr}\left[\mathbf{A}_r \tilde{\mathbf{I}} \mathbf{R}_{\tilde{d}} \tilde{\mathbf{I}}^T \mathbf{A}_r^T\right] = \text{tr}\left[\mathbf{R}_{\tilde{d}}\right] \leq P.$$

Using this real-valued formalism, the demodulated signal at Bob and Eve can be rewritten as

$$\mathbf{z}_{B,r} = \mathbf{B}_{B,r} \mathbf{H}_{B,r} \mathbf{A}_r \tilde{\mathbf{I}} \tilde{\mathbf{d}} + \mathbf{B}_{B,r} \mathbf{w}_{B,r}$$
$$\mathbf{z}_{E,r} = \mathbf{B}_{E,r} \mathbf{H}_{E,r} \mathbf{A}_r \tilde{\mathbf{I}} \tilde{\mathbf{d}} + \mathbf{B}_{E,r} \mathbf{w}_{E,r}. \quad (4)$$

We are now ready to state our main result.

Theorem 1. The FBMC-OQAM secrecy capacity C_s^{FBMC}, under a transmit power constraint, can be written as

$$C_s^{\text{FBMC}} = \max_{\mathbf{R}_{\tilde{d}}, \text{tr}[\mathbf{R}_{\tilde{d}}] \leq P} \frac{1}{2} \log \frac{\left|\mathbf{I} + \mathbf{T}_{B,r} \mathbf{R}_{\tilde{d}} \mathbf{T}_{B,r}^T\right|}{\left|\mathbf{I} + \mathbf{T}_{E,r} \mathbf{R}_{\tilde{d}} \mathbf{T}_{E,r}^T\right|}, \quad (5)$$

where $\mathbf{T}_{B,r} = \mathbf{R}_{w,B}^{-1/2} \mathbf{B}_{B,r} \mathbf{H}_{B,r} \mathbf{A}_r \tilde{\mathbf{I}}$ and $\mathbf{T}_{E,r} = \mathbf{R}_{w,E}^{-1/2} \mathbf{B}_{E,r} \mathbf{H}_{E,r} \mathbf{A}_r \tilde{\mathbf{I}}$. Matrices $\mathbf{R}_{w,B} = 1/2\mathbf{B}_{B,r} \mathbf{B}_{B,r}^T$ and $\mathbf{R}_{w,E} = 1/2\mathbf{B}_{E,r} \mathbf{B}_{E,r}^T$ are the noise covariance matrix at Bob and Eve.

Proof: See Appendix. ∎

As in the generic case, this optimization problem is non convex and high dimensional, which makes it hard to solve, even numerically. The factor $1/2$ comes from the fact that multicarrier symbols composed of real symbols are transmitted instead of complex ones. The following result gives a closed-form expression of the secrecy capacity at high SNR. Using again the result of [11, Th. 2] as in the generic and OFDM cases, the FBMC-OQAM secrecy capacity at high SNR is

$$\lim_{P \to +\infty} C_s^{\text{FBMC}} = \frac{1}{2} \sum_{k=1}^{MN_s} \left[\log \sigma_k^2 \left(\mathbf{T}_{B,r} \mathbf{T}_{E,r}^\dagger\right)\right]^+. \quad (6)$$

We now study different equalization structures at Bob and Eve. We distinguish between two extreme cases for Bob receiver structure: 1) multi-tap equalization, 2) single-tap equalization. We consider that Eve also has the choice to use these two receivers plus the generic (ideal) receiver given by $\mathbf{B}_E = \mathbf{I}$, which does not discard any received samples and does not apply FBMC-OQAM demodulation.

1) Multi-tap Equalization: In this case, we set $\mathbf{B}_{B,r} = \mathbf{A}_r^T \mathbf{S}_{B,r}$ and we look at the secrecy capacity before real conversion. This can be seen as a multi-tap equalizer making use of the information contained in all of the complex-valued neighboring symbols. Similarly, Eve can also use a multi-tap equalizer $\mathbf{B}_{E,r} = \mathbf{A}_r^T \mathbf{S}_{E,r}$. The FBMC-OQAM secrecy capacity and high SNR secrecy capacity with multi-tap equalization are respectively given by (5) and (6), using the new definition of $\mathbf{B}_{B,r}$.

2) Single-Tap Equalization: In contrast with the previous section, we now study the performance of the most simple equalization scheme, which consists in i) single-tap equalization by multiplying each subcarrier output by the conjugate of the channel frequency response and ii) real conversion. This gives

$$\mathbf{B}_{B,r} = \tilde{\mathbf{I}}^T \tilde{\mathbf{D}}_{B,r}^T \mathbf{A}_r^T \mathbf{S}_{B,r}, \tag{7}$$

where $\tilde{\mathbf{D}}_{B,r}$ is the real-valued representation of $\tilde{\mathbf{D}}_B = (\mathbf{I}_{N_s} \otimes \mathbf{D}_B)$. Note that Eve can also use a single-tap equalizer as given in (7) but matched to her own channel. The FBMC-OQAM secrecy capacity and high SNR secrecy capacity with single-tap equalization are respectively given by (5) and (6), using the new definition of $\mathbf{B}_{B,r}$ in (7).

The following theorem shows that, for mildly frequency selective channels, single-tap equalization at Bob incurs no loss as compared to multi-tap equalization and even ideal equalization.

Theorem 2. As $\frac{L_B}{M} \to 0$ and for well time-frequency localized prototype filters [13, (As2)], FBMC-OQAM demodulation with single-tap and multi-tap equalization achieves the same capacity as ideal equalization. Hence, the secrecy capacity C_s^{FBMC} is identical for single-tap, multi-tap and generic equalization at Bob and Eve, for any P. Moreover, the high SNR secrecy capacity then becomes

$$\lim_{P \to +\infty} C_s^{\text{FBMC}} = \frac{N_s}{2} \sum_{m=1}^{M} \left[\log \frac{|H_B(f_m)|^2}{|H_E(f_m)|^2} \right]^+.$$

Proof: See Appendix. ∎

This result is optimistic in that single-tap equalization has a much lower complexity than multi-tap and generic equalization structures. Moreover, the high SNR secrecy capacity is again equivalent to the secrecy capacity of M parallel independent wiretap channels as in CP-OFDM.

VI. SIMULATION RESULTS

We now evaluate numerically the high SNR secrecy capacity of the different transceivers previously studied. Simulations are performed relying on the Matlab-based Wave-ComBox toolbox [14]. For a fair comparison, the secrecy capacity is normalized in terms of bits per sample, *i.e.*, dividing obtained expressions of C_s by N. The generic secrecy capacity is computed in the large N case. The number of subcarriers and the subcarrier spacing are fixed to $M = 64$ and 15 kHz respectively for both CP-OFDM and FBMC-OQAM modulations. For CP-OFDM, as explained earlier, given that successive multicarrier symbols do not overlap, it is sufficient to consider a single multicarrier symbol, *i.e.*, $N_s = 1$. For FBMC-OQAM, the prototype filter is the conventional PHYDYAS pulse [15] with overlapping factor $\kappa = 2$. To take into account the capacity penalty due
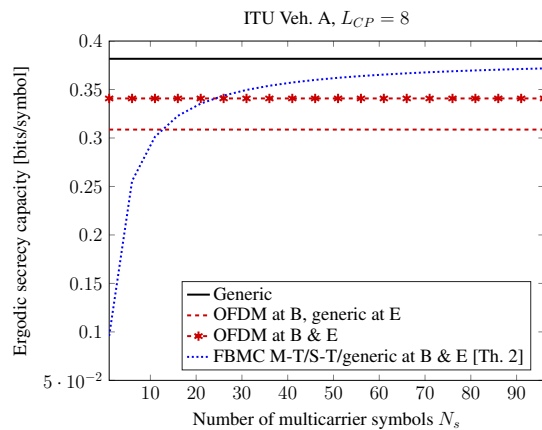

Fig. 2: High SNR ergodic secrecy capacity for mildly frequency selective channel.
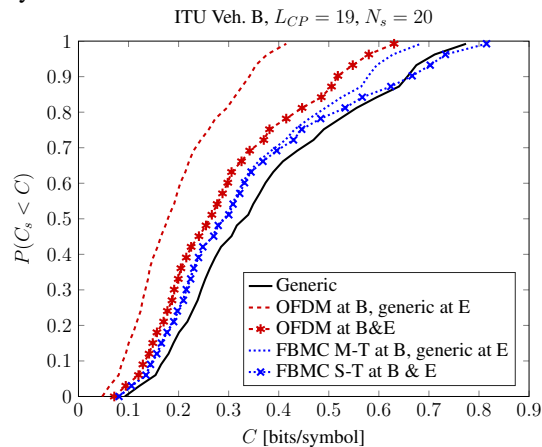

Fig. 3: Cumulative density function of the high SNR secrecy capacity for highly frequency selective channel.

to tail effects, the number of multicarrier symbols N_s is varied to evaluate differences between short and long burst transmissions. Bob and Eve channels, $h_B[n]$ and $h_E[n]$, are generated according to either the ITU Veh. A model or the the ITU Veh. B model, *i.e.*, a mildly and a highly frequency selective channel respectively. The averaged power of both channels is normalized to one.

Fig. 2 shows the high SNR ergodic secrecy capacity, *i.e.*, the secrecy capacity averaged over channel statistics, of generic, CP-OFDM and FBMC-OQAM modulations as a function of N_s, for an ITU Veh. A channel. The gap between the OFDM and the generic secrecy capacity is due to the CP insertion, of length $L_{CP} = M/8 = 8$ here. Moreover, if Eve is not constrained to use a conventional CP-OFDM receiver, an additional loss is induced. On the FBMC-OQAM side, we see that all transceiver configurations at Bob and Eve, namely, single-tap (S-T), multi-tap (M-T) and generic equalization, reach a similar performance, as foreseen by Th. 2 given the mildly frequency selective nature of the ITU Veh. A channel. Moreover, as explained earlier, FBMC-OQAM suffers from a capacity penalty due to tail effects. As N_s grows large, this overhead becomes negligible and it outperforms OFDM.

Fig. 3 plots the cumulative density function of the high SNR secrecy capacity for the highly frequency selective ITU Veh. B channel. The OFDM gap from the generic secrecy capacity is increased because the CP length has to be increased to $L_{CP} = 19$ to compensate for the longer channel impulse response. For a fixed number of multicarrier symbols

$N_s = 20$, the FBMC curves outperform OFDM ones. We also see that the secrecy capacity is improved if Eve uses FBMC-OQAM demodulation and single-tap equalization. In some cases, the secrecy capacity becomes even higher than the generic secrecy capacity. Note that this is only possible because Eve uses a suboptimal receiver.

VII. CONCLUSION

In this paper, we have characterized the FBMC-OQAM secrecy capacity over a frequency selective channel. The secrecy capacity is formulated as an optimization problem that has a closed-form in the high SNR regime. Single-tap and multi-tap equalizers were compared and were shown to be equivalent for mildly frequency selective channels. We have also shown that FBMC-OQAM is particularly competitive for medium-to-long burst transmission as compared to the OFDM and generic secrecy capacity. A promising research direction includes the extension of this study to multiple-antenna systems taking different FBMC-OQAM beamforming and equalization techniques into account.

VIII. APPENDIX

Proof of Theorem 1: We need to derive the secrecy capacity of the real MIMO wiretap channel given in (4), under the transmit power constraint $\operatorname{tr}[\mathbf{R}_s] = \operatorname{tr}[\mathbf{R}_{\tilde{d}}] \leq P$. The noise samples can be colored after demodulation and equalization, depending on the structure of $\mathbf{B}_{B,r}$ and $\mathbf{B}_{E,r}$. To whiten the noise samples, one can multiply $\mathbf{z}_{B,r}$ and $\mathbf{z}_{E,r}$ by $\mathbf{R}_{w,B}^{-1/2}$ and $\mathbf{R}_{w,E}^{-1/2}$ respectively, where $\mathbf{R}_{w,B}$ and $\mathbf{R}_{w,E}$ are defined in Th. 1. Note that this operation is invertible and does not affect the information contained at Bob and Eve. Using the definitions introduced in Th. 1, we obtain

$$\tilde{\mathbf{z}}_{B,r} = \mathbf{T}_{B,r}\tilde{\mathbf{d}} + \tilde{\mathbf{w}}_{B,r}, \ \tilde{\mathbf{z}}_{E,r} = \mathbf{T}_{E,r}\tilde{\mathbf{d}} + \tilde{\mathbf{w}}_{E,r}.$$

We can then apply the result of [16, Th. 3] and we find the result of Th. 1. Secrecy capacity is achieved without channel prefixing and by choosing $\tilde{\mathbf{d}}$ as a zero mean real Gaussian vector with covariance $\mathbf{R}_{\tilde{d}}$.

Proof of Theorem 2: We need to show that the capacity with single-tap, multi-tap and ideal equalization is equivalent for mildly frequency selective channels. For clarity we omit subscripts "B" and "E" in this section as the result needs to be proven at Bob and Eve and the proof is completely symmetrical. Given the identity $|\mathbf{I} + \mathbf{AB}| = |\mathbf{I} + \mathbf{BA}|$, the FBMC-OQAM capacity with single-tap, multi-tap and ideal equalization become equivalent if the product $(\mathbf{T}_r)^T\mathbf{T}_r = \mathbf{K}$ for some fixed $\mathbf{K}$ and for $\mathbf{T}_r \in \{\mathbf{T}_r^{\text{Single}}, \mathbf{T}_r^{\text{Multi}}, \mathbf{T}_r^{\text{Gen}}\}$. To show this, we will use the three following results. Under general assumptions on the prototype filter $g[n]$, the methodology used in [13], relying on a Taylor approximation of the channel variations in frequency, can be used to show that

$$\mathbf{A}_r^T\mathbf{S}_r\mathbf{H}_r\mathbf{A}_r = \mathbf{A}_r^T\mathbf{A}_r\tilde{\mathbf{D}}_r + \boldsymbol{\epsilon}_1 \qquad (8)$$

$$\tilde{\mathbf{I}}^T\tilde{\mathbf{D}}_r^T\mathbf{A}_r^T\mathbf{A}_r\tilde{\mathbf{D}}_r\tilde{\mathbf{I}} = \left(\mathbf{I}_{N_s} \otimes \mathbf{D}^H\mathbf{D}\right) + \boldsymbol{\epsilon}_2 \qquad (9)$$

$$\tilde{\mathbf{I}}^T\mathbf{A}_r^T\mathbf{H}_r^T\mathbf{H}_r\mathbf{A}_r\tilde{\mathbf{I}} = \left(\mathbf{I}_{N_s} \otimes \mathbf{D}^H\mathbf{D}\right) + \boldsymbol{\epsilon}_3, \qquad (10)$$

and the approximation errors $\|\boldsymbol{\epsilon}_1\|$, $\|\boldsymbol{\epsilon}_2\|$ and $\|\boldsymbol{\epsilon}_3\|$ go to zero at rate $\frac{L}{M}$ as $\frac{L}{M} \to 0$. For the multi-tap case, we have $\mathbf{B}_r = \mathbf{A}_r^T\mathbf{S}_r$ and

$$\lim_{L/M\to 0} \mathbf{T}_r^{\text{Multi}} \stackrel{(8)}{=} \mathbf{R}_{w,B}^{-1/2}\mathbf{A}_r^T\mathbf{A}_r\mathbf{D}_r\tilde{\mathbf{I}}$$

$$\lim_{L/M\to 0} \left(\mathbf{T}_r^{\text{Multi}}\right)^T\mathbf{T}_r^{\text{Multi}} \stackrel{(9)}{=} 2\left(\mathbf{I}_{N_s} \otimes \mathbf{D}^H\mathbf{D}\right).$$

For the single-tap case, we have $\mathbf{B}_r = \tilde{\mathbf{I}}^T\tilde{\mathbf{D}}_r^T\mathbf{A}_r^T\mathbf{S}_r$ and

$$\lim_{L/M\to 0} \mathbf{T}_r^{\text{Single}} \stackrel{(8,9)}{=} \mathbf{R}_{w,B}^{-1/2}\left(\mathbf{I}_{N_s} \otimes \mathbf{D}^H\mathbf{D}\right)$$

$$\lim_{L/M\to 0} (\mathbf{T}_r^{\text{Single}})^T\mathbf{T}_r^{\text{Single}} \stackrel{(9)}{=} 2\left(\mathbf{I}_{N_s} \otimes \mathbf{D}^H\mathbf{D}\right).$$

For the generic (ideal) case, we have $\mathbf{B}_r = \mathbf{I}$ and

$$\mathbf{T}_r^{\text{Gen}} = \sqrt{2}\mathbf{H}_r\mathbf{A}_r\tilde{\mathbf{I}}$$

$$\lim_{L/M\to 0} (\mathbf{T}_r^{\text{Gen}})^T\mathbf{T}_r^{\text{Gen}} \stackrel{(10)}{=} 2\left(\mathbf{I}_{N_s} \otimes \mathbf{D}^H\mathbf{D}\right),$$

which shows that $(\mathbf{T}_r)^T\mathbf{T}_r$ is well identical for each type of equalization structure. Inserting these last results in (6) gives the final result of Th. 2.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] E. A. Jorswieck and A. Wolf, "Resource allocation for the wire-tap multi-carrier broadcast channel," in *2008 International Conference on Telecommunications*, June 2008, pp. 1–6.

[4] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of independent parallel channels," in *Securing Wireless Communications at the Physical Layer*. Springer, 2009, pp. 1–18.

[5] F. Renna, N. Laurenti, and H. V. Poor, "Physical-Layer Secrecy for OFDM Transmissions Over Fading Channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 4, pp. 1354–1367, Aug 2012.

[6] B. Farhang-Boroujeny, "OFDM Versus Filter Bank Multicarrier," *IEEE Signal Process. Mag.*, vol. 28, no. 3, pp. 92–112, May 2011.

[7] F. Rottenberg, "FBMC-OQAM transceivers for wireless and optical fiber communications," Ph.D. dissertation, Université Catholique de Louvain & Université Libre de Bruxelles, 2018. [Online]. Available: https://dial.uclouvain.be

[8] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering.* Cambridge University Press, 2011.

[9] M. Kobayashi, M. Debbah, and S. Shamai, "Secured communication over frequency-selective fading channels: A practical Vandermonde precoding," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 386547, 2009.

[10] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug 2011.

[11] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO Wiretap Channel," in *2007 IEEE International Symposium on Information Theory*, June 2007, pp. 2471–2475.

[12] A. RezazadehReyhani and B. Farhang-Boroujeny, "Capacity Analysis of FBMC-OQAM Systems," *IEEE Communications Letters*, vol. 21, no. 5, pp. 999–1002, May 2017.

[13] F. Rottenberg, X. Mestre, D. Petrov, F. Horlin, and J. Louveaux, "Parallel Equalization Structure for MIMO FBMC-OQAM Systems Under Strong Time and Frequency Selectivity," *IEEE Transactions on Signal Processing*, vol. 65, no. 17, pp. 4454–4467, Sep. 2017.

[14] F. Rottenberg, M. Van Eeckhaute, F. Horlin, and J. Louveaux, "WaveComBox: a Matlab Toolbox for Communications using New Waveforms," *ArXiv e-prints*, Jun. 2018.

[15] M. Bellanger, "Specification and Design of a Prototype Filter for Filter Bank Based Multicarrier Transmission," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing*, vol. 4, 2001, pp. 2417 – 2420.

[16] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2547–2553, June 2009.