Filter Hopping: Physical Layer Secrecy Based on FBMC

Volker Lücken*, Taniya Singh*, Özge Cepheli†, Güneş Karabulut Kurt†, Gerd Ascheid*, Guido Dartmann*
*Institute for Communication Technologies and Embedded Systems, RWTH Aachen University, Germany
{luecken, singht, ascheid, dartmann}@ice.rwth-aachen.de
†Wireless Communications Research Laboratory, Istanbul Technical University, Turkey
{irmakoz, gkurt}@itu.edu.tr

***Abstract*—This paper presents a novel physical layer secrecy enhancement technique for multicarrier communications based on dynamic filter hopping. Using the Filter Bank Multicarrier (FBMC) waveform, an efficient eavesdropping mitigation technique is developed using time- and frequency-varying prototype filters. Without knowledge of the filter assignment pattern, an eavesdropper will experience a high level of inter-carrier (ICI) and inter-symbol interference (ISI). With this severe receive signal-to-interference-plus-noise ratio (SINR) degradation for an illegitimate receiver, the secrecy capacity of the communication system is increased. At the same time, the interference at the legitimate receiver is designed to be negligible in comparison to the channel noise.**

***Index Terms*—Filter bank multicarrier, FBMC, filter hopping, secrecy, eavesdropping.**

I. Introduction

Wireless communication always faces the downside of using a non-exclusive channel as communication medium when compared to wired systems. This leads to the risk of an illegitimate receiver accessing the channel and thus facilitates wiretapping of the communication without being noticed. Classical secrecy approaches are mainly located on the higher-level OSI layers, providing a theoretical protection against attacks such as eavesdropping. However, recent incidents have shown that such countermeasures often represent a single point of failure, e.g. on the application layer if attack vectors (like software bugs or vulnerabilities of the methods employed) exist. Therefore, the paradigms of system design constantly change to a multi-layer approach already optimizing the communication link itself against eavesdropping. In most cases, these approaches cannot fully replace higher-layer security measures. Nevertheless, they can particularly complement these methods for already blocking interceptions on the wireless link. In this paper, the focus lies on the field of eavesdropping mitigation by increasing the secrecy capacity of the link based on the interference at the eavesdropper's side.

A. Related Work

Wyner [1] initiated the research in the field of physical layer secrecy by investigating the secrecy capacity for discrete memoryless channels (DMC). Based on his work, it was shown that the secrecy capacity between a legitimate user and an eavesdropper is given by the difference of each channel's capacity, which can be a DMC [2] or a Gaussian wiretap channel [3]. The majority of publications following the seminal work of Wyner requires at least partial knowledge about the eavesdropper's channel and they are therefore location based techniques. An often-used location based technique is beamforming, for which two cases are distinguished in literature: The first only considers beamforming to increase the received signal power at the legitimate users and jointly decrease the received signal power at the eavesdropper [4]. The second approach additionally use artificial interference/noise to reduce the SINR at the eavesdropper [5], [6], [7]. Unfortunately, the eavesdropper is usually passive. Hence, no information of the eavesdropper's channel will be available in practical scenarios.

An alternative technique for improving the physical layer secrecy without exploiting the spatial dimension is based on an optimization of the transmission filter in a single-carrier system [8]. The quality-of-service based filter design can be used to create a set of consecutive filters optimized subject to signal-to-interference ratio (SIR) constraints at the legitimate receiver and the eavesdropper. With this design, the eavesdropper's SINR is limited even with a high channel SNR. However, the technique is based on the assumption of online eavesdropping. If the eavesdropper uses a different receive filter selection strategy than anticipated by the transmitter, the secrecy enhancement might be compromised. Furthermore, an offline processing of the transmission or an intelligent adaption to the optimizer from the eavesdropper side is also a vulnerability of this method.

B. Contribution

In our paper, we present a novel physical layer secrecy improvement technique based on the filter bank multicarrier (FBMC) waveform [9]. By using the flexibility of this multicarrier modulation, it is possible to obtain a high number of degrees of freedom. This can then be exploited for improving the secrecy level of the communication link independently of the eavesdropper position or the channel. Our work is based on a continuous variation of the filter mapping in the time-frequency-lattice (TFL), which leads to a high level of interference for any receiver without knowledge of the correct filter sequence. In comparison to the optimization-based single carrier techniques presented in [8], two dimensions of interference (ISI and ICI) are exploited for improving the secrecy capacity. Despite the similar naming, the technique should not be confused with classical frequency hopping techniques, which only offer a limited robustness against eavesdropping and just represent a basic reassignment of the frequency slots without generating intrinsic interference. In addition, it is also fundamentally different from the eavesdropping mitigation principles using scrambling codes (like in CDMA), even though every multicarrier system can be theoretically described as a special case of such systems. The main advantages of the proposed technique are:

1) Due to the variation of prototype filter mappings over both time and frequency symbol positions and missing knowledge of this mapping for an eavesdropper, offline processing attacks can be fully mitigated.
2) Compared to jamming techniques using artificial noise/interference, the presented approach does not require additional transmission energy and only relies on the intrinsic interference at the receiver side due to missing filter sequence knowledge of the eavesdropper.

The paper is organized as follows. Section II proposes an approach to the variable filter mapping from the perspective of Gabor frame theory and then gives the signal and channel model for the transmission. Section III introduces the concept of filter hopping with the underlying signal model and fundamental approaches for exploiting this technique in practical transmissions. In Section IV, a proof of concept is shown with the corresponding filter sets and mappings, also including an analysis of the secrecy capacity gain and the simulative evaluation in a transceiver chain. Section V discusses possible attack vectors by the eavesdropper. Finally, Section VI presents our conclusions and Section VII sketches possible future work.

II. Signal Model

A. Channel Model

The transmission of a legitimate transmitter Alice to a legitimate receiver Bob is considered. Alice transmits to Bob with unit variance $\sigma_s^2 = 1$ over an additive white Gaussian noise (AWGN) channel with a noise variance of $\sigma^2_{n_{Bob}}$, yielding a signal-to-noise ration (SNR) of $\mathrm{SNR_{Bob}}$. At the same time, an eavesdropper, Eve, is also receiving the signal over a distinct AWGN channel with a noise variance of $\sigma^2_{n_{Eve}}$, resulting in $\mathrm{SNR_{Eve}}$. The full transmission model is shown in Fig. 1, also including the modulation and demodulation, which is introduced in the following section.

B. FBMC Transmission with Time-Varying Filters

Filter bank multicarrier is used as the waveform and modulation for the transmission. It is based on an OQAM lattice [9] with a per-subcarrier pulse shaping. Considered a prospective candidate for 5G mobile communication standards, FBMC is under investigation in several EU projects such as METIS [10]. Solely based on the flexibility gained by pulse shaping, especially in contrast to OFDM, it is possible to realize the filter hopping techniques presented in this paper.

At the transmitter, a continuous-time OQAM signal is represented by the following equation (based on [11], [12]):

$$s(t) = \sum_{m=0}^{M-1} \sum_{n\in\mathbb{Z}} a_{m,n} g_{m,n}(t - nT_0) e^{j2\pi m F_0 t} e^{j\phi_{m,n}}, \quad (1)$$

with M subcarriers, $a_{m,n}$ being the real-valued transmitted symbol, the premodulation $\phi_{m,n} = [\pi/2(n+m)] \bmod \pi$, and $T_0 F_0 = \frac{1}{2}$ for the TFL scaling. This equation describes a basic FBMC/OQAM transmitter, as also shown in Fig. 1, with the extension of a time-frequency position dependent filter $g_{m,n}(t)$ instead of a fixed and static prototype filter.

Similarly at the receiver side, the received symbol is formulated in continuous-time as follows (based on [13]):

$$\hat{a}_{m,n} = \mathbb{R}\Big\{ \int_{-\infty}^{\infty} g_{m,n}(t - n\frac{T_0}{2}) e^{-j2\pi m F_0 t} e^{-j\phi_{m,n}} s(t) dt \Big\}, \quad (2)$$

where $\mathbb{R}(\cdot)$ returns the real-valued part of the input.

C. FBMC/OQAM: Special Case of Multi-Pulse Gabor Theory

Gabor frame theory [14] is used for the efficient analysis of non-stationary signals in two dimensions, i.e. time and frequency. Each function $\tilde{s}(t)$ can be expanded to a weighted series of elementary functions given by

$$\tilde{s}(t) = \sum_{k,l\in\mathbb{Z}} d_{k,l} f_{k,l}(t), \quad (3)$$

where $d_{k,l}$ represent the transmitted symbols and $f_{k,l}(t)$ are the elementary functions occupying a certain area around the symbol at position (k,l) in the TFL given by

$$f_{k,l}(t) = h(t - la) e^{2\pi j k b t}, \quad (4)$$

where a, b are time-frequency shift parameters such that $a, b > 0$. The work of Bölcskei [15] shows that the design of time-frequency well-localized OFDM/OQAM pulse shaping filters is equivalent to design of an orthogonal symmetric function $f_{k,l}(t)$. The dual of this function is a tight gabor frame with oversampling factor 2. Based on Gabor theory, a large number of publications followed having a single base atom/transmit pulse $f(t)$ for the elementary signal $f_{k,l}(t)$.

In an alternate approach [16], multiple pulse multi carrier (MPMC) systems have been proposed. Multiple transmit and receive pulses can be used in the modulator and demodulator to increase spectral efficiency and to have more degrees of freedom. The MPMC transmit signal can be written as (based on [16]):

$$\tilde{s}(t) = \sum_{\tilde{n}\in\mathbb{Z}} \sum_{\tilde{m}=0}^{\tilde{M}-1} \tilde{\boldsymbol{a}}^T_{\tilde{\boldsymbol{m}},\tilde{\boldsymbol{n}}} \boldsymbol{h}_{\tilde{\boldsymbol{m}},\tilde{\boldsymbol{n}}}(t - \tilde{n}T) e^{2\pi j \tilde{m} F t}, \quad (5)$$

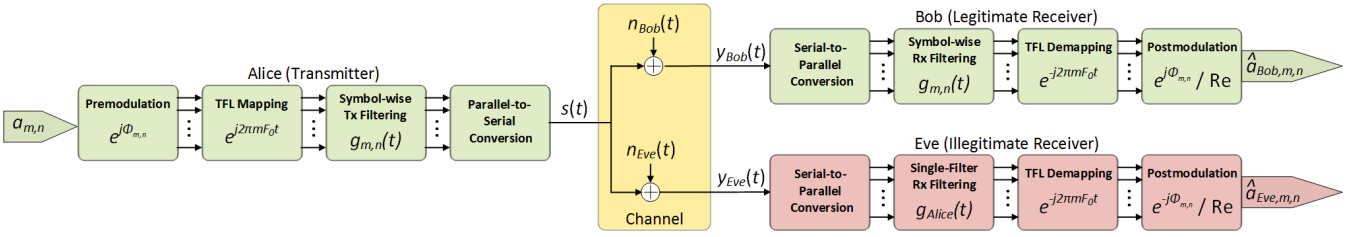


Fig. 1: Transmission model with modulation for Alice, and channel & demodulation for Bob and Eve

with the transmit multipulse composed of U transmit pulses denoted by $\boldsymbol{h}_{\tilde{m},\tilde{n}}(t) = [h^{(1)}_{\tilde{m},\tilde{n}}(t) \dots h^{(U)}_{\tilde{m},\tilde{n}}(t)]^T$ and $\tilde{M}$ representing the number of MPMC subcarriers. Then, at symbol time $\tilde{n}$ and subcarrier $\tilde{m}$, U symbols are transmitted in parallel given by $\tilde{\boldsymbol{a}}_{\tilde{\boldsymbol{m}},\tilde{\boldsymbol{n}}} = [\tilde{a}^{(1)}_{\tilde{m},\tilde{n}} \dots \tilde{a}^{(U)}_{\tilde{m},\tilde{n}}]^T$. The symbol duration T and the subcarrier spacing F constitute the MPMC TFL parameters. In contrast to classical MPMC theory, the transmit multipulse $\boldsymbol{h}_{\tilde{m},\tilde{n}}(t)$ is extended by a dependency on the TFL position in comparison to a previously fixed $\boldsymbol{h}_{\tilde{m},\tilde{n}}(t) = \boldsymbol{h}(t)$. This is done for realizing the filter mapping.

FBMC/OQAM is considered as a special case of MPMC systems. It has been shown as a MPMC gabor system with four linearly independent prototype transmit pulses. This multipulse consists of four prototype filters, given by the vector $\boldsymbol{p}_{\tilde{m},\tilde{n}}(t) = [p^{(1)}_{\tilde{m},\tilde{n}}(t) \dots p^{(U)}_{\tilde{m},\tilde{n}}(t)]^T$, which are time- and frequency-shifted by $\boldsymbol{h}_{\tilde{m},\tilde{n}}(t)$ for realizing the specific excerpt of the OQAM lattice. Based on the description of [16], the OQAM transmit multipulse (5) can be written as $\boldsymbol{h}_{\tilde{m},\tilde{n}}(t) = [h^{(1)}_{\tilde{m},\tilde{n}}(t) \dots h^{(U)}_{\tilde{m},\tilde{n}}(t)]^T =$

$$\left[p^{(1)}_{\tilde{m},\tilde{n}}(t),\, jp^{(2)}_{\tilde{m},\tilde{n}}(t)e^{j\frac{2\pi t}{T}},\, jp^{(3)}_{\tilde{m},\tilde{n}}\left(t-\tfrac{T}{2}\right),\, p^{(4)}_{\tilde{m},\tilde{n}}\left(t-\tfrac{T}{2}\right)e^{j\frac{2\pi t}{T}}\right]^T, \tag{6}$$

where OQAM uses $TF/U = 1/2$. As mentioned before, the multipulse for OQAM is modified to be TFL-position dependent. Multipulse Gabor Riesz bases are the fundamental concept for MPMC systems and can employ Zak-Fourier domain implementations for the efficient MPMC modulation and demodulation [16].

Proposition 1: Comparing the classical continuous-time OQAM (1) with the MPMC system formulation (5), (6), we see that the additional phase premodulation ($e^{j\phi_{m,n}}$) and the time and frequency modulation in classical OQAM systems is replaced by multiple transmit pulses denoted by the modulated transmit multipulse vector $\boldsymbol{h}_{\tilde{m},\tilde{n}}(t)$ in MPMC systems.

We want to show the equality of (1) and (5). Rewrite (1) as:

$$s(t) = \sum_{m=0}^{M-1} \sum_{n\in\mathbb{Z}} a_{m,n} b_{m,n}(t). \tag{7}$$

Comparing the time and frequency shift due to $\tilde{m}, \tilde{n}, m, n$ in (5) and (1) with the OQAM multipulse (6), we can state that

$$\tilde{m} = \left\lfloor \frac{m}{2} \right\rfloor, \quad \tilde{n} = \left\lfloor \frac{n}{2} \right\rfloor, \quad \tilde{M} = M/2, \quad \text{and} \quad U = 4. \tag{8}$$

The multipulse with index $(\tilde{m}, \tilde{n})$ is then composed of four modulated symbols $\tilde{a}_{m,n}(t)$ from the signal model. With a coefficient comparison of the summation terms in (1) and (5), the remaining parameters can be derived. Due to their different frequency shifts and complex phases, they can be related.

$$m = 0, n = 1 \Rightarrow \tilde{m} = 0, \tilde{n} = 0, u = 3:$$
$$a_{0,1} g_{0,1}(t - T_0) j \overset{!}{=} \tilde{a}^{(3)}_{0,0} \underbrace{h^{(3)}_{0,0}(t)}_{jp^{(3)}_{0,0}(t-T/2)} \Rightarrow T = 2T_0$$
$$m = 1, n = 0 \Rightarrow \tilde{m} = 0, \tilde{n} = 0, u = 2:$$
$$a_{1,0} g_{1,0}(t) e^{j2\pi F_0 t} j \overset{!}{=} \tilde{a}^{(2)}_{0,0} \underbrace{h^{(2)}_{0,0}(t)}_{jp^{(2)}_{0,0}(t)e^{j2\pi t/T}} \Rightarrow F_0 = 1/T$$

Then, symbols and prototype filters are mapped accordingly:

$$\tilde{\boldsymbol{a}}_{\tilde{\boldsymbol{m}},\tilde{\boldsymbol{n}}} = [a_{2\tilde{m},2\tilde{n}},\, a_{2\tilde{m},2\tilde{n}+1},\, a_{2\tilde{m}+1,2\tilde{n}},\, a_{2\tilde{m}+1,2\tilde{n}+1}]^T, \tag{9}$$
$$\boldsymbol{p}_{\tilde{m},\tilde{n}}(t) = [g_{2\tilde{m},2\tilde{n}}(t),\, g_{2\tilde{m},2\tilde{n}+1}(t),\, g_{2\tilde{m}+1,2\tilde{n}}(t),\, g_{2\tilde{m}+1,2\tilde{n}+1}(t)]^T. \tag{10}$$

With $F = 2F_0$, insert (10) into (6) and then (6) and (9) into (5). This yields equality with the transmit signal (1).

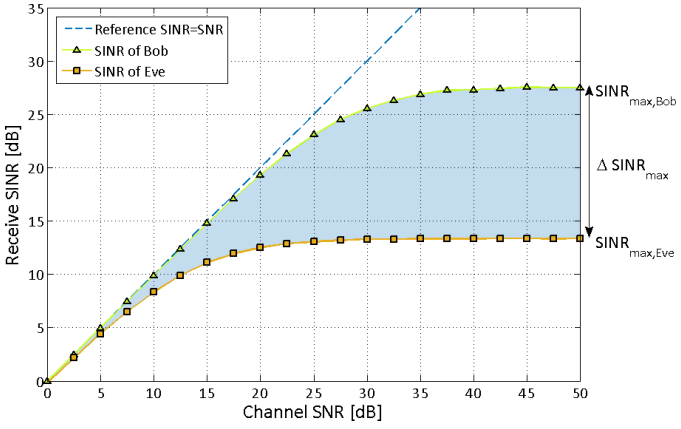


Fig. 2: Degradation of Eve and Bob due to filter hopping-induced intrinsic interference (see Section IV-C for parameters)

III. Filter Hopping

In this section, the concept of filter hopping is introduced. For this paper, the availability of a pre-shared sequence between Alice and Bob is assumed, as the key exchange techniques, which can be used for the generation of such sequence, constitute a special problem and are already employed for current cryptographic techniques. Firstly, an interference model is derived based on the ambiguity function of two different filters. Then, the degradation of the eavesdropper's signal is further analyzed. Based on this degradation, operation regions in different communication scenarios are then introduced.

A. Interference Model

The interference terms between different TFL symbols can be described using the cross-ambiguity function [11]

$$A_{g_1,g_2}(\tau,\nu) = \int_{\mathbb{R}} g_1\left(t+\frac{\tau}{2}\right) g_2^*\left(t-\frac{\tau}{2}\right) e^{-j2\pi\nu t}\,\mathrm{d}t, \tag{11}$$

which yields the level of the signal ($A_{g_1,g_2}(0,0)$) or interference for a time- (τ) and frequency-shifted (ν) filter reception. This is e.g. case with a TFL mapping of the prototype filters. Using this function, we can obtain the interference levels due to filter hopping or mismatching filters at the eavesdropper side, or also the non-perfect reconstruction (NPR) effects. With an average complex-valued symbol energy ${\sigma_s}^2 = 1$ in the OQAM lattice (when combining two real-valued symbols) and assuming statistically independent symbols, the mean SINR over the TFL can be calculated based on a summation of all interference energies at the sampling points (T_0, F_0). Especially for Eve with mismatching receive filters, the interference energy at these points is significant.

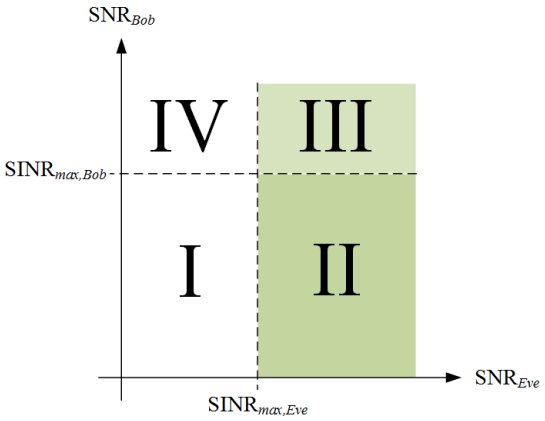


Fig. 3: Filter hopping operation regions

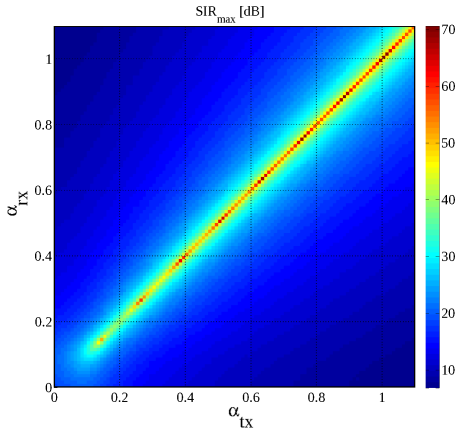


Fig. 4: Maximum SIR with RRC Filter α mismatch in OQAM

B. Operation Regions

Without knowledge of the correct filter mapping, Eve cannot follow the hopping and therefore experiences interference on the received symbols $\hat{a}_{m,n}$. Here, we assume that Eve chooses a static receive filter $g_{Eve}(t)$. The interference level for Eve determines her maximum achievable mean SINR of SINR_{Eve}, denoted as $\mathrm{SINR}_{max,Eve}$. When interference is dominant compared to channel noise, even with further increasing SNR_{Eve} of her channel, no additional SINR_{Eve} gain is possible. Therefore, SINR_{Eve} is in saturation. For Bob, the undesired limitation of SINR_{Bob} to a maximum of $\mathrm{SINR}_{max,Bob}$ is due to a partial non-orthogonality because of the hopping. Figure 2 shows an example for degradation effects of Eve and Bob. The maximum achievable $\mathrm{SINR}_{max,Bob}$ and $\mathrm{SINR}_{max,Eve}$ are marked, with a maximum gain $\Delta\mathrm{SINR}_{\max} = \mathrm{SINR}_{max,Bob} - \mathrm{SINR}_{max,Eve}$ with both receivers in saturation (interference-limited). The interference domination can be expressed as $\mathrm{SIR} \ll \mathrm{SNR}$, when separating SIR due to filter mismatch and SNR of the channels. Still, even at lower $\mathrm{SNR}_{\mathrm{Eve}}$, Eve already incurs a degradation.

For the practical operation of the communication system, different channel conditions of Eve and Bob have to be considered in terms of SNR. Figure 3 shows four operation regions differentiated by each Eve or Bob being in the noise- or interference-limited region. As Eve does not know the correct filter mapping, it can be assumed in general that

$$\mathrm{SINR}_{max,Bob} > \mathrm{SINR}_{max,Eve}. \tag{12}$$

The normal operation regions for the filter hopping technique are located in Regions II and III. There, Eve is in the interference-saturated region and thus, the secrecy capacity is increased linearly with SINR_{Bob} in Region II and is constant in Region III. In Region I, both receivers operate normally, with the channel noise determining the capacity of each channel. Here, the filter hopping technique has no effect and other measures have to be considered, e.g. by changing the transmission mode or energy. Region IV is less relevant with the filter hopping, as with (12), Eve's channel conditions are worse than Bob's, again yielding (12).

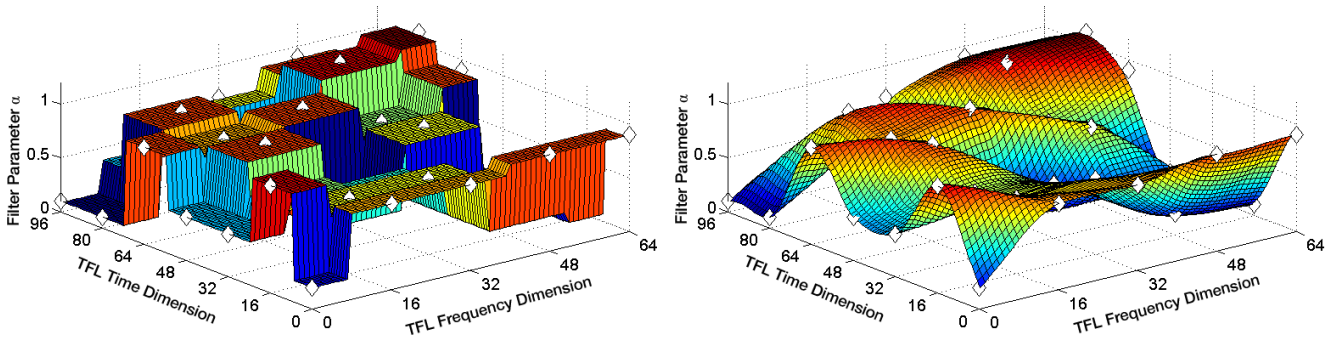
IV. Proof of Concept

In this section, a proof of concept is presented for the filter hopping techniques. The choice of initial prototype filters and their mapping concepts are highlighted along with their application in different scenarios and channel conditions. Finally, achievable secrecy gains are presented and also shown in a communication link performance simulation.

A. Choice of Filter Set

For an initial investigation of the filter hopping technique, parametric filters are favored over designs based on optimizations of the filters. The former allow a simple generation and smooth transition between different filters, even though maximum performance might not be achieved. Therefore, for this proof of concept, a root raised cosine (RRC) filter is chosen as a prototype $g_{m,n}(t)$ in the following, as defined in [17], with a given roll-off factor α. The variation of this single parameter allows a modification of the time-frequency-properties of the symbol pulse shape. The roll-off factor α is changed without modifying the effective filter bandwidth itself. For a suitability analysis of the RRC filter in this context, the maximum achievable SIR is calculated for different fixed prototype filter choices at the transmitter and receiver, meaning that the filter is not depending on the TFL position of the symbol. The different choice of the parameter α for the transmitter (α_{tx}) and the receiver (α_{rx}) creates a filter mismatch and loss of orthogonality at the receiver side, leading to ISI and ICI. Therefore, the maximum achievable SIR is strongly decreased in comparison to a matched filter reception.

Figure 4 visualizes the degradation of the signal with a RRC filter roll-off parameter mismatch for an FBMC/OQAM filter bank. The analysis was performed using an FBMC system with $M = 64$ subcarriers and an overlapping factor of $K = 16$, leading to a filter length of $L = M \cdot K = 1024$ samples. With a time domain truncation of the filter, which is necessary for real systems, the filter bank chain now also exhibits NPR. Therefore, the achievable filter SIR saturates even with matched filter reception, which is shown on the diagonal $\alpha_{tx} = \alpha_{rx}$ of the diagram. The achievable transmission SINR levels in this case are still sufficiently high, as for real transceiver systems, Bob's receiver is noise-dominated. Therefore, Regions III and IV in Fig. 3 are rarely reached. The strong decline in the plot when moving away from the diagonal is desired and beneficial. Only with a slight mismatch of the filter roll-off α, an eavesdropper then already experiences a strong degradation.



(a) Blockwise mapping of filter roll-off α

(b) Cubic spline interpolation of filter roll-off α

Fig. 5: Filter $\alpha(t_0, f_0)$ interpolation example with $\Delta_t = \Delta_f = 16$ (interpolation node points are marked by white diamonds)

B. Mapping Concepts

The distribution of the different filters over the TFL determines the undesired remaining interference at Bob with his correct receive filter mapping. With this given RRC filter set, a fixed $\alpha(t_0, f_0)$ is chosen for specific uniformly distributed points on the TFL, with a distance of Δ_t in time and Δ_f in frequency domain. For these interpolation node points, the value of $\alpha(t_0, f_0)$ is randomly chosen between $[0.1 \ldots 1.1]$, being a reasonable range due to the maximum achievable filter SIR ($\alpha_{tx} = \alpha_{rx}$, see Fig. 4). After this step, a calculation of the $\alpha(t_0, f_0)$ values is performed for all symbols in the TFL, using either a nearest-neighbor approach for a blockwise mapping (as can be seen in Fig. 5a) or a 2-dimensional cubic spline interpolation for a continuous mapping (as shown in Fig. 5b).

With the block-type mapping, all filters $g_{m,n}(t)$ in each block are the same. The interference due to the violated orthogonality conditions of adjacent symbols with different filters, as modeled in Section III-A, is located in the border region of the block. In the middle of the block, however, orthogonality is almost completely preserved. This can also be understood based on the ambiguity function of the filter III-A. Still, the local interference levels in the border region of the blocks are stronger compared to an interpolation, due to the steeper α-value transitions. With cubic spline interpolation, interference is more evenly distributed over the whole TFL, leading to lower local deviations from the mean SINR.

A comparison of both method's gains is shown in Section IV-C. The gain difference between both methods in a final transmission chain also depends on the error-correcting code (ECC) employed in the transmission. Especially in case of the block-type mapping, the error probability due to interference is unevenly distributed, and strongly varies over the symbols in TFL because of interference localization. This is different in case of a smooth interpolation, yielding an even distribution of the interference over the TFL.

C. Secrecy Capacity Gain Analysis

With the presented filter designs and hopping concepts, an analysis of the SINR vs. SNR relations for Bob and Eve and their resulting $\mathrm{SINR}_{\max}$ can be performed. Figure 2 shows this relation for a cubic interpolation with a node spacing of $\Delta_f = \Delta_t = 32$ and a filter choice of $\alpha_{Eve} = 1$ (see Section IV-D). With this, $\mathrm{SINR}_{max,Bob} = 27.66\,\mathrm{dB}$ and $\mathrm{SINR}_{max,Eve} = 13.21\,\mathrm{dB}$ can be achieved, leading to a gain of $\Delta\mathrm{SINR}_{\max} = 14.45\,\mathrm{dB}$. The interference approximately appears as an additional uncorrelated and Gaussian noise if the symbols are uncorrelated and the interference is spread over a large area in the TFL. Because of the interpolation, it can be also assumed to be evenly distributed over the TFL. Then, $\Delta\mathrm{SINR}_{\max}$ is also the maximum achievable secrecy capacity gain, as no knowledge of the filter set is available for Eve and therefore, she cannot perform any interference cancellation.

In case of a block type mapping of the filters, the results are $\mathrm{SINR}_{max,Bob} = 22.55\,\mathrm{dB}$, $\mathrm{SINR}_{max,Eve} = 12.66\,\mathrm{dB}$ and $\Delta\mathrm{SINR}_{\max} = 9.89\,\mathrm{dB}$. For this mapping, the overall maximum gain is significantly smaller due to a stronger degradation at Bob's receiver, but also, the threshold for operation, $\mathrm{SINR}_{max,Eve}$, is reduced. Considering the implementation, block-type mappings are advantageous, as they can still be realized using polyphase filter bank segments, which come along with a low computational complexity.

D. Transceiver Chain Analysis

For an analysis of the filter hopping method in a realistic transceiver chain setup, a simulation in an FBMC testbed was performed. In addition to the transmission model shown in Fig. 1, a soft-symbol detection with different symbol constellations (16QAM, 64QAM, 256QAM) is performed after the receiver. The legitimate receiver Bob uses the correct receive filter mapping $g_{m,n}(t)$, while Eve uses a static filter out of the RRC group with $\alpha_{rx,Eve} = 1$. Further, an error-correcting code is used to alleviate the effects of localized errors and closely reproduce the conditions in a real transceiver system. As a code, a half-rate (32400,64800) LDPC taken from the DVB-S.2 standard [18] is chosen.

The results for the coded BER of Bob and Eve are shown in Fig. 6 for different symbol constellations. It can be seen that for higher-order constellations, the degradation for Eve is significant even for high SNR. This is due to the dominant interference and incapacitates Eve from achieving an acceptable Qos, as SINR_{Eve} is not crossing the waterfall region of the BER curve in contrast to SINR_{Bob}. For 16QAM, the degradation of Eve in comparison to Bob is $1.86\,\mathrm{dB}$ in terms of the required SNR for achieving a BER of 10^{-3}. With 64QAM modulation,

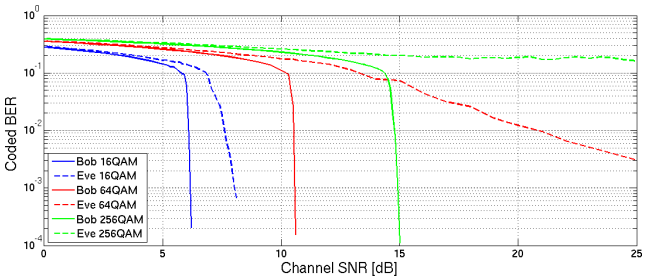


Fig. 6: Coded BER results with Filter Hopping

this degradation already exceeds 15 dB and for 256QAM, Eve cannot reach a BER lower than 10^{-1}. These results show that the modulation should always be chosen as high as possible based on Bob's SNR for maximizing the spectral efficiency. Then, with the much lower capacity of the effective transmission to Eve, she cannot recover from the degradation.

V. Countermeasures by Eve

In the following, possible countermeasures by the eavesdropper against the filter hopping technique are discussed. The gain of this method is based on the eavesdropper's missing knowledge of the filter mapping, otherwise, the secrecy capacity gain might be reduced or not be achieved. Possible attacks can be based on analyses of the signal yielding additional previous knowledge, such as unprotected pilot or reference symbols, allowing an estimation or approximation of the filters. Furthermore, finite symbol constellations can be used to gather information about the filter, especially with offline processing techniques With a coarse hopping of the filters in time and frequency dimension (high Δ_f and Δ_t), the filter sequence estimation might be easier for Eve. In addition, with strongly localized prototype filters, which are a goal of some FBMC filter optimizations, the gain of this method is limited due to a small interference neighborhood and distribution. This may finally improve the possibility for the eavesdropper for an estimation of the filter. The gain of the filter mapping method is better in general when the prototype filters involve a high time and frequency dispersion.

VI. Summary

In this paper, we introduced a novel physical layer secrecy technique named filter hopping. Contrary to existing physical layer secrecy solutions, we do not use any a priori information about the eavesdropper making our approach practically more relevant. The filter hopping technique does not require any knowledge about the eavesdropper's channel. Only the knowledge of the legitimate receiver's noise variance is required to ensure the choice of a modulation with a sufficiently high spectral efficiency for preventing the detection of the symbols by Eve. Eve does not have any knowledge about the filter mapping and can only employ an arbitrary filter set. Hence, it can be ensured that Eve has worse SINR conditions than Bob. Moreover, our approach does not require additional transmit power as opposed to artificial noise/interference solutions.

By using a dynamic filter assignment with the FBMC waveform, which is highly relevant for upcoming 5G communication systems, high gains in terms of secrecy capacity between Bob and Eve are achieved. With a transceiver chain simulation, we showed the practical gains with clear QoS deterioration for Eve for several constellations, while preserving the QoS for Bob. Assuming the correct choice of modulation spectral efficiency, the desired degradation of Eve due to $\Delta SINR$ is achieved. Only in case of low-SNR channel conditions and corresponding modulation choices, none of the receivers is in saturation (Region I, Fig. 3), which is known by the transmitter with the given knowledge of $\mathrm{SNR}_{\mathrm{Bob}}$ for his channel.

VII. Future Work

In our concept, we used a simple parametric filter mapping without joint optimization of the filter mismatch-related interference patterns and TFL filter assignments. Further analyses should include additional optimizations of these two aspects. Also, a complete per-symbol filter optimization will be investigated for achieving maximum secrecy gain and minimum signal degradation for Bob. This should also cover filter designs with a low saturation SIR in case of filter mismatch.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.
[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, May 1978.
[3] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451–456, Jul 1978.
[4] S. Gerbracht *et al.*, "Beamforming for secrecy rate maximization under outage constraints and partial CSI," in *45th Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, 2011, pp. 193–197.
[5] J. Huang and A. Swindlehurst, "QoS-constrained robust beamforming in MISO wiretap channels with a helper," in *45th Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, 2011, pp. 188–192.
[6] W.-C. Liao *et al.*, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, 2011.
[7] N. Romero-Zurita *et al.*, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, 2012.
[8] G. Dartmann *et al.*, "Filter optimization aided interference management with improved secrecy," in *80th IEEE Vehicular Technology Conference*, 2014.
[9] B. Farhang-Boroujeny, "OFDM versus filter bank multicarrier," *Signal Processing Magazine, IEEE*, vol. 28, no. 3, pp. 92–112, May 2011.
[10] A. Osseiran *et al.*, "The foundation of the mobile and wireless communications system for 2020 and beyond: Challenges, enablers and technology solutions," in *77th IEEE Vehicular Technology Conference*, June 2013, pp. 1–5.
[11] J. Du, "Pulse shape adaptation and channel estimation in generalised frequency division multiplexing systems," 2008.
[12] H. Lin *et al.*, "Equalization with interference cancellation for Hermitian symmetric OFDM/OQAM systems," in *IEEE ISPLC*, April 2008, pp. 363–368.
[13] P. Siohan *et al.*, "Analysis and design of OFDM/OQAM systems based on filterbank theory," *IEEE Trans. Signal Process.*, vol. 50, no. 5, pp. 1170–1183, 2002.
[14] D. Gabor, "Theory of Communication," *IEEE Elect. Eng. J.*, vol. 93, no. 26, pp. 429–457, Nov. 1946.
[15] H. Bölcskei, "Orthogonal frequency division multiplexing based on offset QAM," in *"Advances in Gabor Analysis"*, H. G. Feichtinger and T. Strohmer, Eds., 2003, pp. 321–352.
[16] M. M. Hartmann *et al.*, "Wireless multicarrier communications via multipulse Gabor Riesz bases," *EURASIP J. Appl. Signal Process.*, vol. 2006, pp. 96–96, Jan. 2006.
[17] S. Chennakeshu and G. Saulnier, "Differential detection of pi/4-shifted-DQPSK for digital cellular radio," in *41st IEEE Vehicular Technology Conference*, May 1991, pp. 186–191.
[18] ETSI EN 302 307, DVB-S2 standard V1.2.1 (2009-08). [Online]. Available: http://www.etsi.org/deliver/etsi_en/302300_302399/302307/01.02.01_60/en_302307v010201p.pdf