Filter Optimization Aided Interference Management with Improved Secrecy

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

***Abstract*—This paper proposes a novel matched filter optimization based approach to improve secrecy in a communication among two legitimate users. The presented optimization scheme, named as QoS-based filter design, minimizes the stop-band attenuation and uses quality-of-service constraints on the legitimate receiver and an eavesdropper. The resulting problem is relaxed to a convex problem. The filter coefficients are optimal regarding the legitimate receiver's matched filter auto-correlation function, however, it results in a sub-optimal filter for the eavesdropper secrecy constraints. Therefore, an additional post-processing is developed to match the secrecy constraints.**

***Index Terms*—Filter design, convex optimization, secrecy, matched filter.**

I. Introduction

Traditional security techniques are applied at higher layers of the communication model. Following the seminal work of [1], researchers started investigating Layer 1 (physical layer) based techniques. These techniques mainly target to improve the secrecy of the system, working in a complementary fashion with Layer 2 and Layer 3 approaches. In this paper, we propose a novel Layer 1 approach that increases the secrecy of the communication system via optimizing the filter coefficients of the legitimate nodes.

A. Related Work

A secure communication link among two legitimate users (Alice and Bob) with the existence of an eavesdropper (Eve) can be achieved by sharing a secret key among the legitimate users secretly from the eavesdropper [2]. In these approaches, using secret keys, the eavesdropper receives cipher-text containing all information about the encrypted message.

Another approach is the maximization of the secrecy capacity [1], by increasing the interference to Eve or minimizing the eavesdropper's signal-to-interference-plus-noise ratio (SINR). This can be achieved by location-based techniques such as optimization of the precoding or beamforming vectors to increase the received signal power at the legitimate user, while jointly reducing the received signal power at the eavesdropper [3]–[5]. Other approaches are based on the generation of artificial interference (AI) to increase the interference at the eavesdropper [6]–[9] and our previous works [10], [11]. The authors of [12] propose a joint design of precoding and receive filters for a MIMO system. However, all these approaches need the knowledge of the eavesdropper channel. Unfortunately, the eavesdropper will usually be a passive user. Hence, in most of the applications, the channel of the eavesdropper will be unknown. In this paper, we target such cases and show that by optimizing the filter, the secrecy level of the communication can be improved.

In order to increase the secrecy capacity, the authors of [13], [14] propose coding schemes for the transmit filter. In [13], the legitimate users share a key in form of a filter which is unknown by Eve. Compared to the conventional symmetric encryption, where the eavesdropper receives the cipher-text containing all information about the encrypted message, the approaches of [13], [14] avoid a reception of an encrypted signal at the eavesdropper side. The design of the secret filter is based on a scrambling like coding scheme. However, the authors do not present an optimization of this filter regarding different design criteria.

A transmit and the corresponding matched receive filter should satisfy the Nyquist criteria to minimize the inter-symbol interference which results in a set of constraints in the resulting optimization problem [15], [16]. The authors of [16] propose a scheme to design orthogonal wave-forms with matched filters in a multiuser scenario. The inter-symbol interference, defined by the auto-correlation function and the co-channel interference, defined by the cross-correlation, is minimized.

B. Contribution

We propose a novel filter design maximizing the stop-band attenuation of the matched filter and a methodology satisfying the matched filter constraints for the legitimate user and the secrecy constraints against the eavesdropper.

Figure 1 shows two different approaches for PHY-layer security. If the channel state information (CSI) of the eavesdropper is available (left branch), e.g., location-based methods can achieve secrecy based on Eve's CSI. However, an eavesdropper is usually a passive user, consequently, no CSI of Eve is known. Therefore, this paper proposes a matched filter optimization, where no CSI is required.

Figure 2 depicts the concept of the proposed idea. Alice and Bob use the same optimizer to design their matched filter with the coefficients $\mathbf{x}$. The optimization is unique regarding the matched filter coefficients $\mathbf{x}$ for Alice and Bob, due to the deterministic convex optimization technique. If the solution is

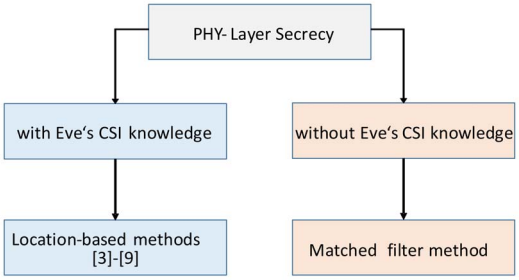

Fig. 1: Concepts of PHY-layer secrecy.

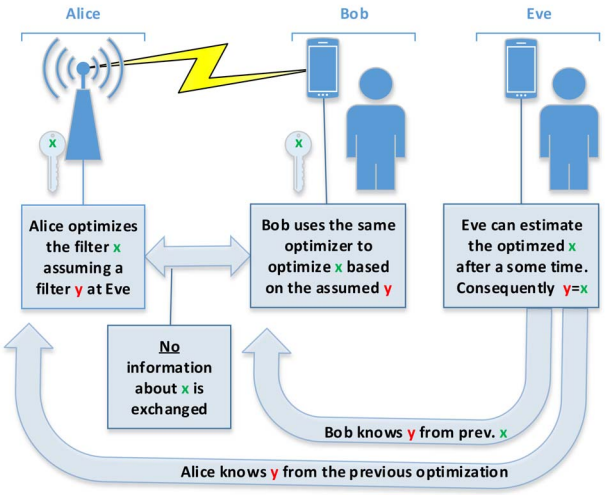

Fig. 2: Idea of the proposed method.

not unique, the filter is not guaranteed to be a matched filter. Eve uses her own receive filter $\mathbf{y}$. However, Eve could be able to estimate the matched filter after some time. Therefore, the system must be adaptive and self-optimizing. Bob and Alice must continuously optimize and update $\mathbf{x}$. The optimization is based on the worst-case assumption that Eve correctly estimates the previous $\mathbf{x}$, hence $\mathbf{y} \leftarrow \mathbf{x}$. The optimization at Alice and Bob then targets to update a filter $\mathbf{x}$ such that the inter-symbol interference at Eve is maximized.

The paper is organized as follows: Section II defines the signal model. Section III introduces two possible optimization problems to design matched filters with improved secrecy and proposes a convex relaxation technique to solve these problems. Section IV presents an exemplary filter design by assuming an initial root-raised-cosine filter at Eve's receiver. Finally, Section V summarizes the results and Section VI gives an outlook.

II. Signal Model

The signal model is depicted in Fig. 3. We assume real valued signals and unit norm signal power. Alice transmits the pulse $x(k)$ and Bob receives over the channel $h_B(k)$ the signal $s(k)$ by using the matched filter $x(-k)$. The eavesdropper jointly receives the signal over the channel $h_E(k)$. Assuming

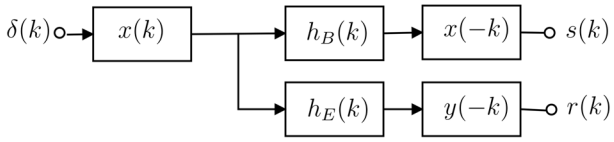

Fig. 3: Bob uses $\mathbf{x}$ as the matched receive filter and Eve uses $\mathbf{y}$ as a receive filter. The filter $\mathbf{x}$ maximizes the SINR at Bob and minimizes the SINR at Eve.

that Eve uses a standard root-raised cosine filter with the impulse response $y(-k)$, she will receive the signal $r(k)$. We desire a design without knowledge of CSI. Furthermore, we assume that Bob is able to compensate the channel by means of an equalizer, as frequently used in practice. Then the signal received at Bob is given by:

$$s(k) = \mathbf{x}^T \mathbf{E}^k \mathbf{x}. \tag{1}$$

As in [17], the matrix $\mathbf{E} \in \mathbb{R}^{N \times N}$ denotes the unit shift matrix consisting of zeros except on the first lower sub-diagonal and the matrix $\mathbf{E}^k$ denotes the k-th power of $\mathbf{E}$. The vector $\mathbf{x}$ is the vector containing all filter coefficients $\mathbf{x} = [x(0), x(1), \ldots, x(N-1)]^T$. With the worst-case assumption that Eve can compensate her channel, we can define the signal received by the eavesdropper:

$$r(k) = \mathbf{x}^T \mathbf{E}^k \mathbf{y}, \tag{2}$$

where $\mathbf{y} = [y(0), y(1), \ldots, y(N-1)]^T$ is the vector containing all filter coefficients of the filter which is used by Eve. Using (1), the signal power received by Bob is:

$$s^2(k) = (\mathbf{x}^T \mathbf{E}^k \mathbf{x}) \cdot (\mathbf{x}^T \mathbf{E}^k \mathbf{x}) \tag{3}$$

and the signal power received by Eve can be formulated as follows:

$$\begin{aligned} r^2(k) &= (\mathbf{x}^T \mathbf{E}^k \mathbf{y}) \cdot (\mathbf{x}^T \mathbf{E}^k \mathbf{y})^T \\ &= (\mathbf{x}^T \mathbf{E}^k \mathbf{y}) \cdot (\mathbf{E}^k \mathbf{y})^T \mathbf{x} \\ &= \mathbf{x}^T \mathbf{E}^k \mathbf{y} \mathbf{y}^T (\mathbf{E}^k)^T \mathbf{x}. \end{aligned}$$

With $\mathbf{Y} = \mathbf{y}\mathbf{y}^T$ and $\mathbf{V}_k = \mathbf{E}^k \mathbf{Y} (\mathbf{E}^k)^T$, we can simplify the notation to:

$$r^2(k) = \mathbf{x}^T \mathbf{V}_k \mathbf{x}. \tag{4}$$

As we can observe from (3), the signal power of Bob can be formulated in terms of finite auto-correlation sequences (FAS). However, the signal power received at Eve is a cross-correlation when $\mathbf{x} \neq \mathbf{y}$. In the following section, we make use of the cross-correlation in order to increase the secrecy level of the system.

III. Optimization Problems

This section presents a two step optimization approach.

- Step 1: The QoS-based filter design approach uses signal-to-interference (SIR) constraints for Bob and Eve, while the stop-band attenuation is minimized for the matched filter. The QoS-based filter design can find the optimal

auto-correlation sequence $s(k)$ and the optimal squared cross-correlation function $r^2(k)$.

- Step 2: The filter design for $\mathbf{x}$ of Step 1 is optimal for $s(k)$, however, sub-optimal for $r^2(k)$. Therefore, an additional post-processing optimization tries to find a filter $\mathbf{x}$ which is optimal for $s(k)$ and $r^2(k)$ in a least squares sense.

A. Step 1: QoS-based Filter Design

This optimization approach searches for the optimal sequences $s(k)$ and $r^2(k)$. The optimization maximizes the stop-band attenuation of the matched filter while SIR constraints for Bob and Eve are satisfied. The SIR constraints can be formulated as follows. The interference at Eve's receiver is given by:

$$\sum_{l=1}^{M} r^2(l \cdot L) = \sum_{l=1}^{M} \mathbf{x}^T \mathbf{V}_{l \cdot L} \mathbf{x}. \tag{5}$$

where $M = N/L \in \mathbb{N}$. Note that the interference occurs in repetitions of L samples. Hence, at multiples of L samples Bob and Eve detect the received symbol power. Similar, the interference of Bob is given by:

$$\sum_{l=1}^{M} s^2(l \cdot L) = \sum_{l=1}^{M} (\mathbf{x}^T \mathbf{E}^{l \cdot L} \mathbf{x})^2. \tag{6}$$

With (5) and (6), we can state the SIR of Eve as:

$$\gamma_E = \frac{r^2(0)}{\sum_{l=1}^{M} r^2(l \cdot L)} \leq \frac{1}{\gamma_{QoS}} \tag{7}$$

and the SIR of Bob is:

$$\gamma_B = \frac{s^2(0)}{\sum_{l=1}^{M} s^2(l \cdot L)} \geq \gamma_{QoS}. \tag{8}$$

Here γ_{QoS} denotes the desired QoS SIR for both Bob and Eve. Note that we here only consider one half of the auto-correlation sequence $s(k)$ and the cross-correlation sequence $r(k)$. The sequence $s(k)$ is symmetric, therefore, we can ignore one half of the samples in the optimization. For $r(k)$ we actually need $2N-1$ samples. In this paper, we design $r(k)$ only for one half of the samples. The second half $(N-1)$ will generate additional interference which is not considered in the optimization.

It is often desired to spectrally shape of the signals $s(k)$, e.g., the filters should have a high stop-band attenuation or a narrow bandwidth to avoid interference to other systems. The signal $s(k)$ is a symmetric signal and the spectrum of $s(k)$ is given by:

$$S(\omega) = s(0) + 2 \sum_{k=1}^{N-1} s(k) \cos(k\omega). \tag{9}$$

The function (9) is linear in $\mathbf{s} = [s(0), \ldots, s(N-1)]$. According to [17], $s(k)$ is FAS, if and only if the spectrum is non-negative $S(\omega) \geq 0$. Assuming $\mathcal{B}_{stop}$ denotes domain of the stop-band frequencies and using (8) and (7), the QoS-based filter design problem can be stated as:

$$\begin{aligned} \mathcal{P}_1: \quad \eta = \min_{\mathbf{x}} \; & \int_{\mathcal{B}_{stop}} S(\omega) d\omega \\ \text{s.t.} \quad & \gamma_{QoS} \cdot r^2(0) \leq \sum_{l=1}^{M} r^2(l \cdot L), \\ & s^2(0) \geq \gamma_{QoS} \cdot \sum_{l=1}^{M} s^2(l \cdot L), \\ & s(0) = 1. \end{aligned} \tag{10}$$

Problem $\mathcal{P}_1$ is non-convex in general. In the next section, we propose a convex relaxation technique to approximate the problem $\mathcal{P}_1$.

B. Convex Relaxation

As shown in [17], if $f(k)$ is a FAS, the following Lemma can be used:

Lemma 1: (Page 334, [17]) The sequence $f(k) = \mathbf{x}^T \mathbf{E}^k \mathbf{x} = \mathrm{Tr}\{\mathbf{E}^k \mathbf{x}\mathbf{x}^T\}$ is a FAS if and only if:

$$f(k) = \mathrm{Tr}\{\mathbf{E}^k \mathbf{X}\} \tag{11}$$

for some symmetric matrix $\mathbf{X} \succeq 0$.

Therefore, as in [17], we obtain for (1) the same set if we ignore the rank-1 constraint $\mathbf{X} = \mathbf{x}\mathbf{x}^T$. Consequently, we can rewrite (1) as follows:

$$s(k) = \mathrm{Tr}\{\mathbf{E}^k \mathbf{X}\}. \tag{12}$$

With (12), we can rewrite all constraints of problem $\mathcal{P}_1$ as convex constraints. We can also relax the eavesdropper constraints when we use

$$r^2(k) = \mathbf{x}^T \mathbf{V}_k \mathbf{x} = \mathrm{Tr}\{\mathbf{V}_k \mathbf{X}\} \tag{13}$$

and relax the non-convex rank-1 constraint $\mathbf{X} = \mathbf{x}\mathbf{x}^T$. Using these convex relaxations, we can state the following proposition:

Proposition 1: Introducing a new symmetric matrix variable $\mathbf{X}$, the lower bound of problem $\mathcal{P}_1$ is given by:

$$\begin{aligned} \tilde{\mathcal{P}}_1: \eta \geq \tilde{\eta}(\mathbf{Y}) = \min_{\mathbf{s},\mathbf{X}} \; & \int_{\mathcal{B}_{stop}} S(\omega) d\omega \\ \text{s.t. } & \gamma_{QoS} \cdot \mathrm{Tr}\{\mathbf{Y}\mathbf{X}\} \leq \sum_{l=1}^{M} \mathrm{Tr}\{\mathbf{V}_{l \cdot L} \mathbf{X}\}, \\ & 1 \geq \gamma_{QoS} \cdot \sum_{l=1}^{M} s^2(l \cdot L), \;\; s^2(0) = 1, \\ & s(k) = \mathrm{Tr}\{\mathbf{E}^k \mathbf{X}\} \;\; \forall k = 0, \ldots, N-1, \\ & \mathbf{X} \succeq 0. \end{aligned} \tag{14}$$

Proof: Lemma 1 states that the constraints of Bob and the objective function can be equivalently rewritten as in (12). Hence, no relaxation is made by this constraint. However, dropping the rank-1 constraint $\mathbf{X} = \mathbf{x}\mathbf{x}^T$ in Eve's signal power in (4) results in a larger feasible set than in the original problem $\mathcal{P}_1$, consequently, the minimum $\tilde{\eta}$ can be smaller than η. ■

C. Step 2: Post-Processing

Due to $S(\omega) \geq 0$, the filter coefficients $x(k)$ can be obtained by spectral factorization techniques from the FAS $s(k)$ [18], [19]. In this paper, we used the same technique as in [19]. However, the obtained filter $\mathbf{x}$ is only optimal for the sequence $s(k)$ and sub-optimal for $r^2(k)$. This is also problematic if an iterative filter optimization according to Figure 2 is used, e.g., a second filter $\mathbf{x}_2$ is optimized assuming Eve was able to estimate the previously optimized filter $\mathbf{x}_1$.

A solution $\mathbf{x}$ of problem $\tilde{\mathcal{P}}_1$ will be quasi-optimal for $s(k)$. If the optimization is unchanged, the same auto-correlation function $s(k)$ (optimally designed for Bob's constraints) can be the result. Consequently, the spectral factorization will result in the same filter, hence $\mathbf{x}_2 = \mathbf{x}_1$. The same FAS allows different cross-correlation sequences. The problem lies in finding the best $\mathbf{x}$ which is also optimal for the eavesdropper constraints.

However, an algorithm solving the optimization problem $\tilde{\mathcal{P}}_1$ is able to find the sequence $r^2(k)$ which corresponds to one half (N) of the $2N-1$ samples of the cross-correlation. Based on this information, a post-processing is proposed.

The sequences $r^2_{opt}(k) = \mathrm{Tr}\{\mathbf{V}_k\mathbf{X}\}$ and $s(k)$ as a result from Problem $\tilde{\mathcal{P}}_1$, are quasi optimal. Consequently, this information can be used to find a filter which is optimal regarding the eavesdropper and legitimate user constraints. Hence, the quadratic constraints

$$s(k) = \mathbf{x}^T\mathbf{E}^k\mathbf{x} \;\Rightarrow\; f_k(\mathbf{x}) = \mathbf{x}^T\mathbf{E}^k\mathbf{x} - s(k)\;\forall k \qquad (15)$$

and

$$r^2_{opt}(k) = \mathbf{x}^T\mathbf{V}_k\mathbf{x} \;\Rightarrow\; g_k(\mathbf{x}) = \mathbf{x}^T\mathbf{V}_k\mathbf{x} - r^2_{opt}(k)\;\forall k \quad (16)$$

should be satisfied. The constraints (15) and (16) can are satisfied (in a least squares sense) if the least-squares problem

$$\mathcal{P}_2: \qquad r = \min_{\mathbf{x}} \sum_{k=0}^{N-1} g_k^2(\mathbf{x}) + f_k^2(\mathbf{x}) \qquad (17)$$

is minimized. Problem (17) is an unconstrained non-linear least-squares problem. This problem is non-convex in general and the solution depends on the initial value. A good initial solution $\mathbf{x}_0$ is the result of the spectral factorization of the FAS $s(k)$. In this paper, the Matlab function *lsqnonlin()* with a Levenberg Marquardt algorithm is used to find a local optimal solution for problem $\mathcal{P}_2$.

IV. Filter Design

This section present an example for a filter design with secrecy. Eve is not able to optimize her filter coefficients. We assume Eve uses a standard root-raised cosine filter as initial filter. For the QoS-based filter design $\tilde{\mathcal{P}}_1$, a length of $N = 49$ samples and an oversampling factor of $L = 6$ is used. The QoS SIR is set to $\gamma_{QoS} = 16$ dB and the pass-bandwidth is $1/4$. Figure 4 depicts the filter coefficients of the initial filter $\mathbf{y}$. The signal power is maximized at the sampling position T (Without loss of generality, we assume $T = 0$). The optimization of the problems $\tilde{\mathcal{P}}_1$ to $\tilde{\mathcal{P}}_1$ is based on [20] (with SDPT3 and a medium precision) and the optimization of problem $\mathcal{P}_2$ is

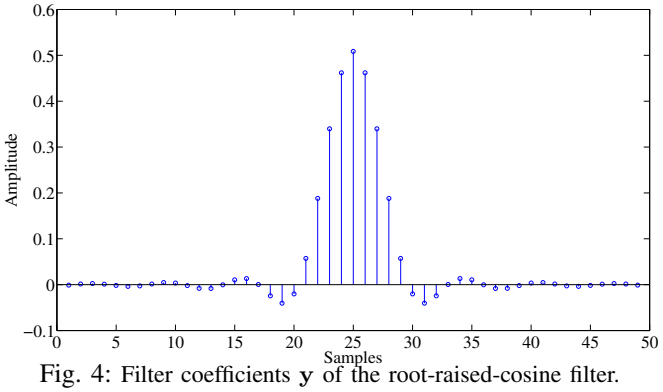

Fig. 4: Filter coefficients $\mathbf{y}$ of the root-raised-cosine filter.

solved with the Matlab function *lsqnonlin()*. The numerical approximation of the power spectral density $S(\omega)$ is performed by $N_\omega = 4 \cdot N$ equidistant discrete values of ω.

Figures 5 depicts the sequences $s^2(k)$ and $r^2(k)$ as a result of a spectral factorization after solving problem $\tilde{\mathcal{P}}_1$ and post-processing $\mathcal{P}_2$ and the relaxed sequence $r^2_{opt}(k) = \mathrm{Tr}\{\mathbf{V}_k\mathbf{X}\}$. The solution of the post-processing $r^2(k)$ is a least-squares solution of $r^2_{opt}(k)$. The solution of $s(k)$ is quasi optimal, however, $s(k)$ allows multiple solutions for $r(k)$. Consequently, the relaxed sequence $r^2_{opt}(k) = \mathrm{Tr}\{\mathbf{V}_k\mathbf{X}\}$ can be different to the sequence $r^2(k) = \mathbf{x}^T\mathbf{V}_k\mathbf{x}$ obtained with $\mathbf{x}$ after the spectral factorization of $s(k)$. The post-processing has only a marginal influence on the FAS $s^2(k)$. Figure 6 depicts the FAS $s^2(k)$ after solving problem $\mathcal{P}_2$ and the optimal sequence as a result of problem $\tilde{\mathcal{P}}_1$. For the FAS $s(k)$ multiple sequences $r^2(k)$ are feasible. Note, problem $\tilde{\mathcal{P}}_1$ can design the FAS $s^2(k)$ which is a symmetric sequence based on only N samples. A cross-correlation is not symmetric. Actually, we need $2N-1$ samples to completely design the cross-correlation. In this paper, the sequence $r^2_{opt}(k)$ is only designed for N values and not for the $2N-1$ values. However, a reduction of the eavesdropper SIR can be already achieved with half of the samples. $\mathcal{P}_2$ has also an impact on the objective function. Figures 7 compares the power spectral density $|S_{opt}(\omega)|^2$ of $\tilde{\mathcal{P}}_1$ and $|S(\omega)|^2$ after applying $\mathcal{P}_2$. The stop-band attenuation is decreased after applying $\mathcal{P}_2$. The SIR of Bob satisfies the QoS constraint of $\gamma_{QoS} = 16$ dB. After solving $\mathcal{P}_2$, the resulting cross-correlation is optimized and close to the sequence $r^2_{opt}(k) = \mathrm{Tr}\{\mathbf{V}_k\mathbf{X}\}$, consequently the SIR of Eve decreased in this design example.

The Figures 8-10 present the results of sequence of $K = 4$ consecutively designed filters. The filters are optimized according to the concept explained in Figure 2. Figure 8 shows the sequence $r^2_m(k)$ for the four consecutively designed filters. In the majority of the cases the post-processing is able to find a good least squares solution. For the second filter, the sequence $r^2_{opt}(k)$ is not perfectly matched. Finally, Figure 10 depicts the power spectral densities $|S_m(\omega)|^2$ of the four filters. For the presented design the eavesdropper SIR $\gamma_{E,PP}$ after post-processing (PP) $\mathcal{P}_2$ mostly out-performs the eavesdropper SIR $\gamma_{E,nPP}$ without post-processing (nPP), where $\mathbf{x}$ is directly obtained from the spectral factorization.

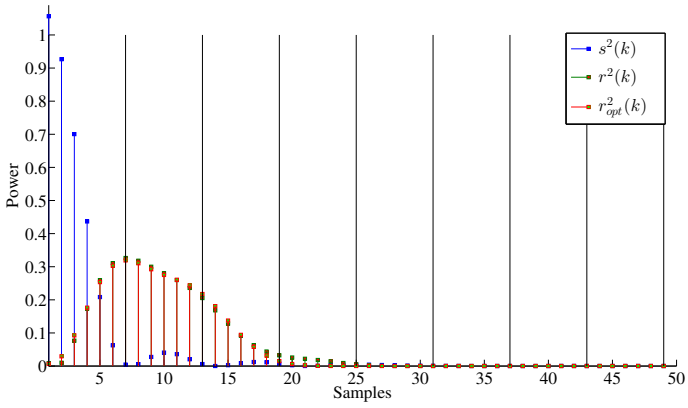

Fig. 5: The sequences $s^2(k)$, $r^2(k)$ (after spectral factorization and post-processing), and $r^2_{opt}(k) = \mathrm{Tr}\{\mathbf{V}_k\mathbf{X}\}$ for problem $\tilde{\mathcal{P}}_1$. The sampling position is at $k = 0$. The black vertical lines denote multiples of L.

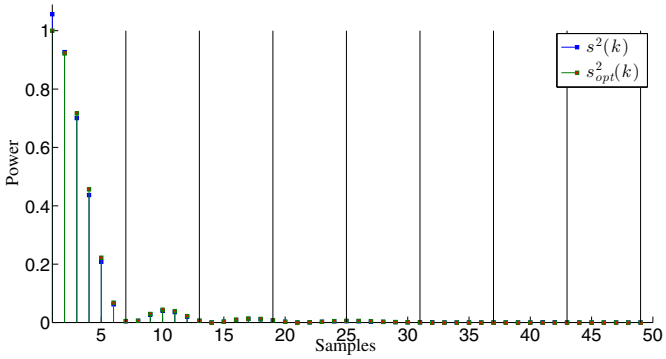

Fig. 6: The sequence $s^2(k)$ after solving problem $\mathcal{P}_2$ and $s^2_{opt}(k)$ as a solution of problem $\tilde{\mathcal{P}}_1$. The sampling position is at $k = 0$. The black vertical lines denote multiples of L.

V. Summary

This paper presents an optimization technique to design arbitrary matched filters with improved secrecy. Using a set of different filters, the proposed design can further improve the secrecy. The optimization is based on convex optimization with finite auto-correlation sequences which results in globally optimal solutions regarding the matched filter constraints for Bob's filter, which is important due to the independent optimization at Bob and Alice. The optimization is not globally optimal regarding the constraints on Eve's received signal power. Eve's signal is a finite cross-correlation sequence and the resulting constraints on Eve's filter require a convex relaxation. The optimization can deliver the cross-correlation sequences, however, not a filter resulting in these cross-correlation sequences. Therefore, an additional post-processing can be used to get filter coefficients matching the auto-correlation sequences of the legitimate user and the cross-correlation sequences of the eavesdropper.

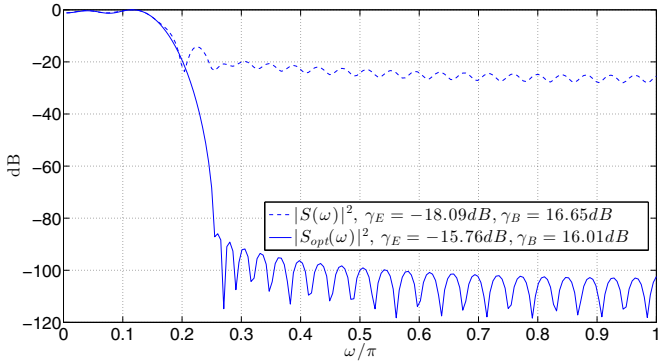

Fig. 7: Power spectral density $|S_{opt}(\omega)|^2$ as a solution of problem $\tilde{\mathcal{P}}_1$ and $|S(\omega)|^2$ with additional post-processing.

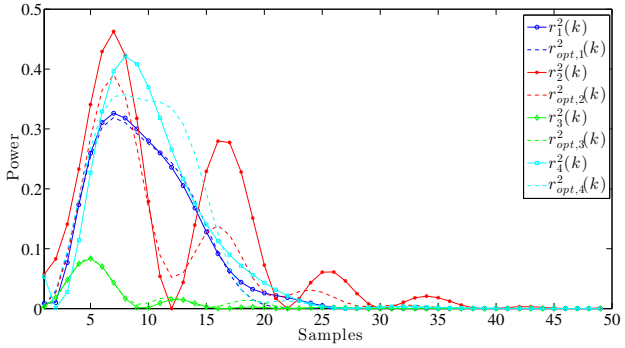

Fig. 8: The sequences $r^2_m(k)$ optimized according to $\tilde{\mathcal{P}}_1$ with post-processing ($\mathcal{P}_2$) for four consecutively designed filters and $r^2_{opt,m}(k) = \mathrm{Tr}\{\mathbf{V}_k\mathbf{X}\}$ as a solution of problem $\tilde{\mathcal{P}}_1$.

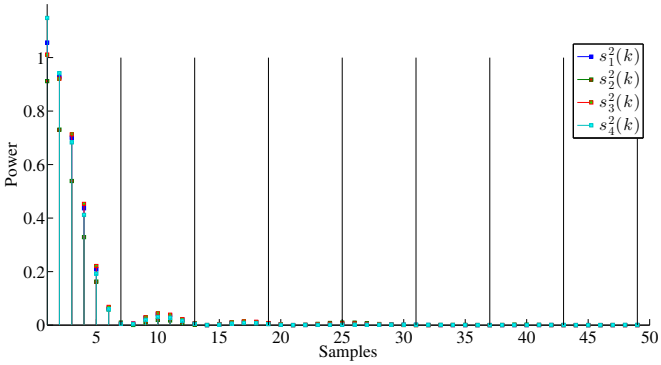

Fig. 9: The sequences $s^2_m(k)$ optimized according to $\tilde{\mathcal{P}}_1$ with post-processing ($\mathcal{P}_2$) for four consecutively designed filters. The sampling position is at $k = 0$. The black vertical lines denote multiples of L.

VI. Future Work

A future work should determine how many consecutively optimized filters can be generated and what are the limiting parameters, e.g, band-width, QoS SIR, or filter length. The post-processing is a difficult non-convex least-squares problem. The solver is not always able to find a filter which results in desired cross-correlation sequence (e.g. the second filter in Figure 8). Therefore, the SIR constraints are not satisfied for every design example. An investigation of improved and also faster

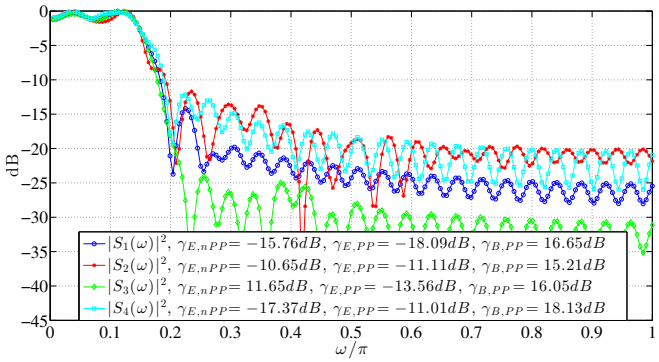

Fig. 10: Power spectral densities $|S_m(\omega)|^2$ optimized according to $\tilde{\mathcal{P}}_1$ with post-processing ($\mathcal{P}_2$) for four consecutively designed filters. $\gamma_{QoS} = 16$dB.

customized Levenberg-Marquardt methods can result in better solutions. An alternative optimization approach considering all samples of the cross-correlation sequence can result in higher better SIRs for Eve and Bob.

Eve could know the optimizer, therefore, another future work the use of a pre-shared information set that can be exchanged between the legitimate users (similar to an encryption key). According to this information-set, a filter change period, randomization constraints, and different initializations can be determined among Alice and Bob in pseudo-random way.

Another idea is the off-line optimization of a set of filters and a random number generation system which chooses the filters at Alice and Bob in the same order. At each time interval Alice and Bob restarts the transmission with the same a randomly selected filter which is orthogonal to the previously optimized filters to ensure, that Eve can not receive a signal in case she was able to detect one on the previously optimized filters.

Furthermore, this work can be integrated in new filter-bank based multi-carrier (FMBC) systems which are considered in the next generation of wireless communication standards.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[2] C. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal, Vol 28, pp. 656715*, vol. 28, pp. 656–715.

[3] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *41st Annual Conference on Information Sciences and Systems, (CISS)*, 2007, pp. 905–910.

[4] A. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *IEEE International Conference on Acoustics, Speech and Signal Processing, (ICASSP)*, 2009, pp. 2437–2440.

[5] S. Gerbracht, C. Scheunert, and E. Jorswieck, "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.

[6] A. Wolf and E. Jorswieck, "On the zero forcing optimality for friendly jamming in MISO wiretap channels," in *11th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2010.

[7] 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.

[8] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Processing Letters*, vol. 19, no. 2, pp. 71–74, 2012.

[9] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.

[10] Ö. Cepheli, G. Dartmann, G. Karabulut Kurt, and G. Ascheid, "Beamforming aided interference management for improved secrecy in multi-cell environments," in *European Wireless 2014*, Mar. 2014.

[11] G. Dartmann, Ö. Cepheli, G. Karabulut Kurt, and A. G., "Beamforming aided interference management with improved secrecy for correlated channels," in *Proceedings of IEEE Vehicular Technology Conference (VTC-Spring)*, May 2014.

[12] H. Reboredo, J. Xavier, and M. Rodrigues, "Filter design with secrecy constraints: The MIMO gaussian wiretap channel," *IEEE Transactions on Signal Processing*, vol. 61, no. 15, pp. 3799–3814, Aug. 2013.

[13] R. Nishi, K. Morozov, Y. Hori, and K. Sakurai, "Improvement on secrecy capacity of wireless lan using matched filter," in *Seventh International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, 2011, pp. 463–469.

[14] M. Baldi, M. Bianchi, and F. Chiaraluce, "Increasing physical layer security through scrambled codes and ARQ," in *International Conference on Communications Workshops (ICC)*, 2011.

[15] J. Sullivan, J. Adams, R. Reisner, and R. Armstrong, "New optimization algorithm for digital communication filters," in *36th Asilomar Conference on Signals, Systems and Computers*, 2002, pp. 323–327.

[16] Z. Zang and S. Nordholm, "Orthogonal digital waveform set for multidimensional signaling and multiuser communications with matched filter receivers," in *10th Asia-Pacific Conference on Communications and 5th International Symposium on Multi-Dimensional Mobile Communications*, vol. 2, 2004, pp. 883–887.

[17] B. Alkire and L. Vandenberghe, "Convex optimization problems involving finite autocorrelation sequences," *Mathematical Programming*, vol. 93, no. 3, pp. 331–359, Dec. 2002.

[18] S.-P. Wu and S. Boyd, "FIR filter design via spectral factorization and convex optimization," in *Applied and Computational Control, Signals and Circuits*. B. Datta Ed. Boston, MA: Birkauser, 1998, vol. 1, pp. 215–245.

[19] E. Karipidis, N. D. Sidiropoulos, and Z.-Q. Luo, "Far-field multicast beamforming for uniform linear antenna arrays," *IEEE Transactions on Signal Processing*, vol. 55, no. 10, pp. 4916–4927, Oct. 2007.

[20] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," http://cvxr.com/cvx, Jun. 2014.