Joint Power and Beam Optimization in a Multi-Carrier MIMO Wiretap Channel with Full-Duplex Jammer

Omid Taghizadeh, Tianyu Yang, and Rudolf Mathar
Institute for Theoretical Information Technology, RWTH Aachen University, D-52074 Aachen, Germany
Email: {taghizadeh, yang, mathar}@ti.rwth-aachen.de

***Abstract*—In this paper we address a sum secrecy rate maximization problem for a multi-carrier and MIMO communication system. We consider the case that the receiver is capable of full-duplex (FD) operation and simultaneously sends jamming signal to a potential eavesdropper. In particular, we simultaneously take advantage of the spatial and frequency diversity in the system in order to obtain a higher level of security in the physical layer. Due to the non-convex nature of the resulting mathematical problem, we propose an iterative solution with a guaranteed convergence, based on block coordinate descent method, by re-structuring our problem as a separately convex program. Moreover, for the special case that the transmitter is equipped with a single antenna, an optimal transmit power allocation strategy is obtained analytically, assuming a known jamming strategy. The performance of the proposed design is then numerically evaluated compared to the other design strategies, and under different system assumptions.**

***Keywords*—Full-duplex, wiretap channel, secrecy rate, jamming, multi-carrier, MIMO.**

I. Introduction

Full-Duplex transceivers are known for their capability to enhance various aspects of wireless communication systems, e.g., achieving higher spectral efficiency and physical layer security, due to the simultaneous transmission and reception capability on the same channel [1]. Nevertheless, such systems suffer from the inherent self-interference (SI) from their own transmitter. Recently, specialized cancellation techniques, e.g., [2]–[4], have demonstrated an adequate level of isolation between Tx and Rx directions to facilitate a FD communication and motivated a wide range of related studies, see, e.g., [5]. As an interesting use case of such capability, it is known that a FD receiver can significantly enhance the security of a wireless system in physical layer, by simultaneously transmitting a jamming signal to a potential eavesdropper, while receiving the useful information from the legitimate transmitter. Note that the information security of the current communication systems are typically addressed by distributing secret keys, using cryptographic approaches. This approach mainly relies on the assumption that a potential eavesdropper has a limited computational power and hence may not break the exchanged secret key. On the other hand, this assumption is increasingly undermined due the advances in the production of digital processors, and leads to a growing interest to ensure the security of information systems in the physical layer. In this regard, the concept of the wiretap physical channel is introduced in [6], including a legitimate transmitter, namely Alice, a legitimate receiver, namely Bob, as well as an eavesdropper, namely Eve. In this regard, the secrecy capacity of a wiretap channel is defined as the information capacity that can be exchanged among the legitimate users, without being accessible by Eve. The secrecy capacity of the defined wiretap model have been since extensively studied for various systems, regarding performance bounds, channel coding and information theoretic aspects, as well as the system design and resource optimization, see [7] and the references therein.

The application of FD capability for secrecy rate maximization in a wiretap channel is studied in [8] where a FD Bob is capable of transmitting jamming signal, considering a single antenna Alice and a passive eavesdropper. In particular the utilization of a FD jammer reduces the need to external helpers, which are commonly used to degrade the reception capability of the eavesdropper via cooperative jamming [9], [10], without having to trust external nodes, or demanding additional resources. The studied system [8] is then extended to a setup where all nodes are equipped with multiple antennas [11], [12]. Moreover, extensions on the operation the FD Bob is introduced by considering a simultaneous information and jamming transmission, i.e., operating as a base station [13], and considering a FD jamming Bob that simultaneously relays information to a third node, i.e., operating as a jamming relay [14]. The consideration of a joint FD operation of both Alice and Bob, i.e., a bi-directional wiretap channel, as well as the possibility of the FD operation at Eve, i.e., an active eavesdropper, is respectively studied in [15], [16], and in [17], targeting at sum-secrecy rate maximization in both communication directions.

The aforementioned works study different system possibilities considering a single-carrier, frequency-flat channel model for all of the physical links. In contrast, the consideration of a frequency selective, multi-carrier system in the context of sum secrecy rate maximization is extensively studied for a wireless system with half-duplex links, see [18]–[21]. In this respect, extension of the prior works with FD transceivers to a frequency-selective and multi-carrier design is interesting. This is since the usual flat-fading assumption of the previous studies limits the usability of the proposed designs. Furthermore, in a frequency selective setup, the frequency diversity in different subcarriers can be opportunistically used, both regarding the jamming and the desired information link to jointly enhance the resulting secrecy capacity. In this respect, a power-auction game is proposed in [22] for maximizing the sum secrecy rate in a FD and multi-carrier system, where all nodes are equipped with a single antenna. However, such studies are not yet extended for a system with multiple-antenna FD transceivers.

In this paper we address a joint power and beam optimization problem for sum secrecy rate maximization in a multi-carrier and MIMO wiretap channel. We consider the

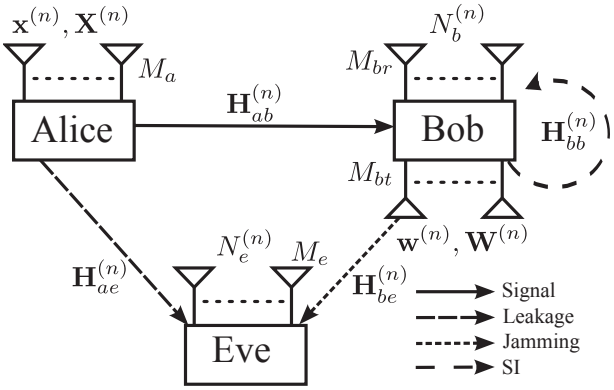

Figure 1. The studied multi-carrier wiretap channel, including Alice (legitimate transmitter), Bob (legitimate receiver) and Eve (eavesdropper). Bob is capable of FD operation. Upper-index n is the subcarrier index.

case that the receiver is capable of full-duplex (FD) operation and simultaneously sends jamming signal to a potential eavesdropper. In particular, we simultaneously take advantage of the spatial and frequency diversity in the system in order to obtain a higher level of security in the physical layer. In Section II, the system model is presented. In Section III the corresponding optimization strategy is defined. Due to the non-convex nature of the resulting mathematical problem, we propose an iterative solution with a guaranteed convergence, based on block coordinate descent method [23, Subsection 2.7], by re-structuring our problem as a separately convex program. Moreover, for special case that the transmitter is equipped with a single antenna, an optimal transmit power allocation strategy is obtained analytically, assuming a known jamming strategy. The performance of the proposed design is then numerically evaluated in Section IV.

A. Mathematical Notation:

Throughout this paper, column vectors and matrices are denoted as lower-case and upper-case bold letters, respectively. Mathematical expectation, trace, inverse, determinant, transpose, conjugate and Hermitian transpose are denoted by $\mathbb{E}\{\cdot\}$, $\mathrm{tr}(\cdot)$, $(\cdot)^{-1}$ $|\cdot|$, $(\cdot)^T$, $(\cdot)^*$ and $(\cdot)^H$, respectively. The Kronecker product is denoted by $\otimes$. The identity matrix with dimension K is denoted as $\mathbf{I}_K$ and $\mathrm{vec}(\cdot)$ operator stacks the elements of a matrix into a vector. $\mathbf{0}_{m\times n}$ represents an all-zero matrix with size $m \times n$. $\perp$ represents the statistical independence. $\mathrm{diag}(\cdot)$ returns a diagonal matrix by putting the off-diagonal elements to zero. The sets of real, non-negative real, complex and natural numbers are respectively denoted by $\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{C}$ and $\mathbb{N}$. $\|\cdot\|_F$ represents Frobenius norm. $\{a\}^+$ is equal to $a \in \mathbb{R}$ if $a \geq 0$, and zero otherwise.

II. System Model

We consider a classic wiretap channel: Alice transmits a massage to Bob while Eve intends to eavesdrop the transmitted message. Moreover, we consider a multi-carrier and MIMO system, where Bob is capable of FD operation by sending a jamming signal to Eve while receiving the message from Alice, see Fig. 1. Alice and Eve are respectively equipped with M_a and M_e transmit and receive antennas, where Bob is equipped with M_{bt} (M_{br}) transmit (receive) antennas. In each subcarrier, channels are assumed to follow a quasi-stationary and flat-fading model. In this regard, channels from Alice to Bob (desired communication channel), Alice to Eve (information leakage channel), Bob to Bob (SI channel), and Bob to Eve (jamming channel) are respectively denoted as $\mathbf{H}_{ab}^{(n)} \in \mathbb{C}^{M_{br}\times M_a}$, $\mathbf{H}_{ae}^{(n)} \in \mathbb{C}^{M_e\times M_a}$, $\mathbf{H}_{bb}^{(n)} \in \mathbb{C}^{M_{br}\times M_{bt}}$ and $\mathbf{H}_{be}^{(n)} \in \mathbb{C}^{M_e\times M_{bt}}$, where $n \in \mathcal{N}$, and $\mathcal{N}$ is the index set of all subcarriers. The transmit signal from Alice can be written as

$$\mathbf{x}^{(n)} = \mathbf{V}^{(n)}\mathbf{s}^{(n)}, \tag{1}$$

where $\mathbf{s}^{(n)} \sim \mathcal{C}\left(\mathbf{0}_{d\times 1}, \mathbf{I}_d\right)$ and $\mathbf{V}^{(n)} \in \mathbb{C}^{M_a\times d}$ respectively represent the vector of data symbols to be transmitted, and the transmit precoder for subcarrier n. Moreover, $d \in \mathbb{N}$ is the number of data streams which are transmitted in parallel. On the other hand, the jamming signal transmitted by Bob is described as $\mathbf{w}^{(n)} \sim \mathcal{CG}\left(\mathbf{0}_{M_{bt}\times 1}, \mathbf{W}^{(n)}\right)$, where $\mathbf{W}^{(n)} \in \mathbb{C}^{M_{bt}\times M_{bt}}$ is the jamming transmit covariance, and $\mathcal{G}$ represents Gaussian distribution. Note that the transmitted jamming signal by Bob impacts the wiretap channel in two opposite directions. Firstly, the jamming signal impacts the signal received by Eve as an additional interference term, and degrades the Alice to Eve channel. Secondly, due to the imperfect SI cancellation, the residual interference terms lead to the degradation of the communication channel between Alice and Bob. Since the aforementioned effects impact the achievable system secrecy in opposite directions, a smart design of the jamming strategy is crucial. The received signal by Eve is written as

$$\mathbf{y}_e^{(n)} = \mathbf{H}_{ae}^{(n)}\mathbf{x}^{(n)} + \mathbf{H}_{be}^{(n)}\mathbf{w}^{(n)} + \mathbf{n}_e^{(n)}, \tag{2}$$

where $\mathbf{n}_e^{(n)} \sim \mathcal{CG}\left(\mathbf{0}_{M_e\times 1}, N_e^{(n)}\mathbf{I}_{M_e}\right)$ is the additive white noise on Eve. Similarly, the received signal at Bob is formulated as

$$\mathbf{y}_b^{(n)} = \mathbf{H}_{ab}^{(n)}\mathbf{x}^{(n)} + \mathbf{n}_b^{(n)} + \mathbf{z}_b^{(n)}, \tag{3}$$

where $\mathbf{n}_b^{(n)} \sim \mathcal{CG}\left(\mathbf{0}_{M_{br}\times 1}, N_b^{(n)}\mathbf{I}_{M_{br}}\right)$ is the additive white noise on Bob, and $\mathbf{z}_b^{(n)} \in \mathbb{C}^{M_{br}}$ is the baseband representation of the residual SI signal in subcarrier n, remaining from the SI cancellation process.

A. Residual SI model

We recognize three different sources of error considering the state-of-the-art SI cancellation methods [24]. This includes inaccuracy of the channel state information (CSI) regarding SI path as well as the inaccuracy of the transmit/receive chain elements in the analog domain. In the following we study the impact of each part separately.

1) Linear SI cancellation error: The estimation accuracy of the CSI in the SI path is limited, particularly in the environments with limited channel coherence time, see [25, Subsection 3.4.1], [26, Subsection V.C]. In this respect, the error of the CSI estimation regarding the SI path is defined as $\mathbf{E}_{bb}^{(n)}$, such that $\mathbf{E}_{bb}^{(n)} = \mathbf{D}_{bb}^{(n)}\bar{\mathbf{E}}_{bb}^{(n)}$ where $\bar{\mathbf{E}}_{bb}^{(n)}$ is matrix of zero-mean i.i.d. elements with unit variance, and $\mathbf{D}_{bb}^{(n)}$ incorporates spatial correlation, see [24, Equation (8), (9)].

2) Transmitter distortion: Similar to [24], the inaccuracy of the analog (hardware) elements in the transmit chains, e.g., digital-to-analog converter error, power amplifier noise and oscillator phase noise, are jointly modeled by injecting an additive Gaussian distortion signal term for each transmit

chain. This is written as $q_l(t) = e_{\mathrm{t},l}(t) + w_l(t)$, see Fig. 2 such that

$$e_{\mathrm{t},l}(t) \sim \mathcal{CG}\left(0, \kappa \mathbb{E}\{w_l(t) w_l(t)^*\}\right), \\ e_{\mathrm{t},l}(t) \perp w_l(t),\ e_{\mathrm{t},l}(t) \perp e_{\mathrm{t},l}(t'),\ e_{\mathrm{t},l}(t) \perp e_{\mathrm{t},l'}(t), \tag{4}$$

where w_l, $e_{\mathrm{t},l}$, and $q_l \in \mathbb{C}$ respectively represent the intended (distortion-free) transmit signal, additive transmit distortion, and the actual transmit signal from the l-th transmit chain, and t denotes the instance of time[1]. Moreover, we have $t \neq t^{'}, l \neq l^{'}$, and $\kappa \in \mathbb{R}^+$ is the distortion coefficient, relating the collective power of the distortion signal to the intended transmit power.

3) Receiver distortion: Similar to the transmit chain, the combined effect of the inaccurate hardware elements, e.g., analog-to-digital converter error, oscillator phase noise and automatic gain control noise, are presented as an additive distortion term $\tilde{q}_l(t) = e_{\mathrm{r},l}(t) + u_l(t)$ such that

$$e_{\mathrm{r},l}(t) \sim \mathcal{CG}\left(0, \beta \mathbb{E}\{u_l(t) u_l(t)^*\}\right), \\ e_{\mathrm{r},l}(t) \perp u_l(t),\ e_{\mathrm{r},l}(t) \perp e_{\mathrm{r},l}(t^{'}),\ e_{\mathrm{r},l}(t) \perp e_{\mathrm{r},l'}(t), \tag{5}$$

where u_l, $e_{\mathrm{r},l}$, and , $\tilde{q}_l$ respectively represent the intended (distortion-free) receive signal, additive receive distortion, and the received signal from the l-th receive antenna. Moreover, $\beta \in \mathbb{R}^+$ holds a similar role as κ regarding the distortion signal variance in the receiver side.

Note that the defined model for transmit/receive distortion terms follow two important intuitions. Firstly, unlike the usual thermal noise model, the variance of the distortion terms are proportional to the transmit/receive signal power in each chain. Secondly, the distortion signal is statistically independent to the intended transmit/receive signals. Such statistical independence also holds for distortion signal terms at different chains, or at different time instance, i.e., they follow a spatially and temporally white statistics, see [24, Subsection II.C], and [24, Subsection II.D]. Consequently from (5) and (4), the covariance of the aggregate noise-plus-residual-interference signal on Bob is obtained as

$$\begin{aligned} \mathbf{\Sigma}_b^{(n)} &= \mathbb{E}\left\{ \left(\mathbf{n}_b^{(n)} + \mathbf{z}_b^{(n)}\right) \left(\mathbf{n}_b^{(n)} + \mathbf{z}_b^{(n)}\right)^H \right\} \\ &= N_b^{(n)} \mathbf{I}_{M_{br}} + \mathrm{trace}\left(\mathbf{W}^{(n)}\right) \mathbf{D}_{bb}^{(n)} \mathbf{D}_{bb}^{(n)H} \\ &+ \mathbf{H}_{bb}^{(n)} \left(\kappa^{(n)} \sum_{n \in \mathcal{N}} \mathrm{diag}\left(\mathbf{W}^{(n)}\right) \right) \mathbf{H}_{bb}^{(n)H} \\ &+ \beta^{(n)} \mathrm{diag}\left(\sum_{n \in \mathcal{N}} \mathbf{H}_{bb}^{(n)} \mathbf{W}^{(n)} \mathbf{H}_{bb}^{(n)H} \right), \end{aligned} \tag{6}$$

where $\kappa^{(n)}$ ($\beta^{(n)}$) represents the transmit (receive) distortion coefficient relating the collective power of the intended transmit (receive) signal to the distortion signal variance in the n-th subcarrier[2].

It is worth mentioning that the impacts of the discussed inaccuracies, i.e., $e_{\mathrm{t},l}, e_{\mathrm{r},l}, \mathbf{E}_{bb}^{(n)}$, become significant for a FD transceiver due to the strong SI channel. For instance, the transmit distortion signals pass through the strong SI channel $\mathbf{H}_{bb}^{(n)}$ and become comparable to the desired signal from Alice which is passing through a much weaker channel $\mathbf{H}_{ab}^{(n)}$. Nevertheless, such inaccuracies are ignorable in the other links which do not involve an SI path, i.e., $\kappa \ll 1, \beta \ll 1$ and $\left\|\mathbf{E}_{bb}^{(n)}\right\|_F \ll \left\|\mathbf{H}_{bb}^{(n)}\right\|_F$.

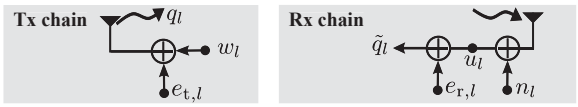

Figure 2. FD transceiver inaccuracy model. The impact of the limited transmitter/receiver dynamic range is modeled as additive distortion terms.

B. Transmit power constraints

It is common to assume that the average transmit power from each device is practically limited due to, e.g., limited battery and energy storage. This is written as

$$\mathrm{trace}\left(\sum_{n \in \mathcal{N}} \mathbf{X}^{(n)}\right) \leq X_{\max},\ \ \mathrm{trace}\left(\sum_{n \in \mathcal{N}} \mathbf{W}^{(n)}\right) \leq W_{\max}, \tag{7}$$

where

$$\mathbf{X}^{(n)} = \mathbb{E}\left\{\mathbf{x}^{(n)} \mathbf{x}^{(n)H}\right\} = \mathbf{V}^{(n)} \mathbf{V}^{(n)H} \tag{8}$$

is the transmit covariance from Alice in the subcarrier n. Moreover, $X_{\max}, W_{\max} \in \mathbb{R}^+$ respectively represent the maximum transmit power from Alice, and the maximum transmit power from Bob, i.e., jamming power.

C. Sum secrecy capacity

The secrecy capacity of the defined system, for the subcarrier n is written as

$$\begin{aligned} \mathcal{I}_{\mathrm{sec}}^{(n)} &= \left\{ \mathcal{I}_{ab}^{(n)} - \mathcal{I}_{ae}^{(n)} \right\}^+ \\ &= \left\{ \log_2 \left| \mathbf{I}_d + \mathbf{V}^{(n)H} \mathbf{H}_{ab}^{(n)H} \left(\mathbf{\Sigma}_b^{(n)}\right)^{-1} \mathbf{H}_{ab}^{(n)} \mathbf{V}^{(n)} \right| \right. \\ &\quad \left. - \log_2 \left| \mathbf{I}_d + \mathbf{V}^{(n)H} \mathbf{H}_{ae}^{(n)H} \left(\mathbf{\Sigma}_e^{(n)}\right)^{-1} \mathbf{H}_{ae}^{(n)} \mathbf{V}^{(n)} \right| \right\}^+, \end{aligned} \tag{9}$$

where $\mathcal{I}_{\mathrm{sec}}^{(n)}$ is the resulting secrecy rate in subcarrier n, and $\mathcal{I}_{ab}^{(n)}$, $\mathcal{I}_{ae}^{(n)}$ respectively represent the information capacity of Alice-Bob and Alice-Eve paths. In the above formulation, $\mathbf{\Sigma}_e^{(n)} = N_e^{(n)} \mathbf{I}_{M_e} + \mathbf{H}_{be}^{(n)} \mathbf{W}^{(n)} \mathbf{H}_{be}^{(n)H}$ is the covariance of the received noise-plus-interference signal at Eve and $\mathbf{\Sigma}_b^{(n)}$ is calculated from (6).

Consequently, the sum-secrecy capacity of the defined multi-carrier system is obtained as

$$\mathcal{I}_{\mathrm{sum}} = \sum_{n \in \mathcal{N}} \mathcal{I}_{\mathrm{sec}}^{(n)}. \tag{10}$$

D. Remarks

i) Unlike the information-containing signal from Alice, the jamming signal from Bob contains artificial noise, see [27, Equation (5)]. This is to prevent Eve to decode the jamming signal.

[1]Note that the signal representation in time domain includes the superposition of signal parts in all subcarriers.

[2]The distortion coefficients associated with different subcarriers may be different if, e.g., the subcarrier spacing is not equal over all bands, or the power spectral density of the distortion signals are not completely flat.

ii) We consider a case where Alice is not contributing in the jamming process. This is to simplify the task of Alice as a usual end-user device. The extension of the considered system to a setup with different jamming strategies is a goal of our future research.

iii) In this work we assume the availability of CSI on Alice-Bob, Alice-Eve, and Bob-Eve channels. Other than scenarios where the position of Eve is stationary and known, this assumption does not hold in practice. The sensitivity of the resulting system performance to the CSI accuracy is numerically evaluated in Section IV.

III. Sum Secrecy Rate Maximization

In this part our goal is to maximize the defined sum secrecy rate of the system over all subcarriers, see (10), considering the transmit power constraints for Alice and Bob, see (7). The corresponding optimization problem is written as

$$\max_{\mathbb{X},\mathbb{W}} \quad \mathcal{I}_{\text{sum}} \ \text{s.t.} \ (7) \tag{11}$$

where $\mathbb{X}$ ($\mathbb{W}$) represents the set of $\mathbf{X}^{(n)} \succeq 0$ ($\mathbf{W}^{(n)} \succeq 0$), $\forall n \in \mathcal{N}$. By recalling (9) and known matrix identities [28, Eq. (516)] the defined problem is reformulated as

$$\max_{\mathbb{X},\mathbb{W}} \quad \sum_{n\in\mathcal{N}} \Bigg\{ \log_2 \left|\mathbf{\Sigma}_b^{(n)} + \mathbf{\Theta}_b^{(n)}\right| - \log_2 \left|\mathbf{\Sigma}_b^{(n)}\right| - \log_2 \left|\mathbf{\Sigma}_e^{(n)} + \mathbf{\Theta}_e^{(n)}\right| + \log_2 \left|\mathbf{\Sigma}_e^{(n)}\right| \Bigg\}^+ \tag{12a}$$

$$\text{s.t.} \ \ \text{trace}\left(\mathbf{\Theta}\right) \leq X_{\max}, \ \ \text{trace}\left(\mathbf{\Sigma}\right) \leq W_{\max}, \tag{12b}$$

where $\mathbf{\Theta} := \sum_{n\in\mathcal{N}} \mathbf{X}^{(n)}$, $\mathbf{\Theta}_b^{(n)} := \mathbf{H}_{ab}^{(n)} \mathbf{X}^{(n)} {\mathbf{H}_{ab}^{(n)}}^H$, and $\mathbf{\Theta}_e^{(n)} := \mathbf{H}_{ae}^{(n)} \mathbf{X}^{(n)} {\mathbf{H}_{ae}^{(n)}}^H$ are affine compositions of the Alice transmit covariance matrices $\mathbf{X}^{(n)}$. Moreover, $\mathbf{\Sigma} = \sum_{n\in\mathcal{N}} \mathbf{W}^{(n)}$, $\mathbf{\Sigma}_e^{(n)}$, and $\mathbf{\Sigma}_b^{(n)}$ are affine compositions of the transmit jamming covariance matrices $\mathbf{X}^{(n)}$. Nevertheless, the above problem is intractable, due to the $\{.\}^+$ operation in the defined secrecy value. Moreover, the maximization of difference of such $\log()$ functions lead to a class of difference-of-convex (DC) problems which is jointly or separately a non-convex problem [29]. The following two lemmas transform the objective function into a more tractable form.

Lemma III.1. *At the optimality of (12), the operator $\{.\}^+$ has no impact.*

Proof: The operator $\{.\}^+$ impacts the problem only when the value inside becomes negative, for at least one of the subcarriers $n \in \mathcal{N}$. In such a situation, Alice and Bob can turn off transmission in the corresponding subcarrier, i.e., choosing $\mathbf{X}^{(n)} = \mathbf{0}, \mathbf{W}^{(n)} = \mathbf{0}$, and contribute the reduced power to another subcarrier with a positive $\mathcal{I}_{\text{sec}}^{(n)}$. Such action results in the enhancement of $\mathcal{I}_{\text{sum}}$ and contradicts the initial optimality assumption. ∎

Lemma III.2. *Let $\mathbf{R} \in \mathbb{C}^{l\times l}$ be a positive definite matrix. The maximization of the term $-log\,|\mathbf{R}|$ is equivalent in terms of the optimal $\mathbf{R}$ and objective value to*

$$\max_{\mathbf{R}\succ 0, \mathbf{Q}\succ 0} \ log\,|\mathbf{Q}| - tr\,(\mathbf{QR}) + l, \tag{13}$$

where $\mathbf{Q} \in \mathbb{C}^{l\times l}$.

Proof: Since (13) is an unconstrained concave maximization over $\mathbf{Q}$ for a fixed $\mathbf{R}$, the corresponding optimal $\mathbf{R}$ is obtained by equalizing the derivative of the objective function to zero. In this way we obtain $\mathbf{Q}^\star = \mathbf{R}^{-1}$. This equalizes the objective in (13) to the term $-\log|\mathbf{R}|$ at the optimality of $\mathbf{Q}$, which concludes the proof, see also [30, Lemma 2]. ∎

Via the utilization of the defined lemmas, the problem (12) can be restructured as

$$\max_{\mathbb{X},\mathbb{W},\mathbb{Q},\mathbb{L}} \quad \sum_{n\in\mathcal{N}} \Bigg(\log \left|\mathbf{\Sigma}_b^{(n)} + \mathbf{\Theta}_b^{(n)}\right| + \log \left|\mathbf{\Sigma}_e^{(n)}\right| \tag{14a}$$

$$- \text{trace}\left(\mathbf{Q}^{(n)}\mathbf{\Sigma}_b^{(n)}\right) - \text{trace}\left(\mathbf{T}^{(n)}\left(\mathbf{\Sigma}_e^{(n)} + \mathbf{\Theta}_e^{(n)}\right)\right) + \log\left|\mathbf{Q}^{(n)}\right| + \log\left|\mathbf{T}^{(n)}\right| \Bigg) \tag{14b}$$

$$\text{s.t.} \quad \text{trace}\left(\mathbf{\Theta}\right) \leq X_{\max}, \ \ \text{trace}\left(\mathbf{\Sigma}\right) \leq W_{\max}, \tag{14c}$$

where $\log()$ is natural logarithm, $\mathbf{Q}^{(n)} \in \mathbb{C}^{M_{br}\times M_{br}}$ and $\mathbf{T}^{(n)} \in \mathbb{C}^{M_e\times M_e}$ are introduced as auxiliary variables, and the sets $\mathbb{Q}$ and $\mathbb{T}$ are defined similar to that of $\mathbb{X}$, $\mathbb{W}$. Following Lemma III.2 optimal values of the auxilliary variables are obtained as

$$\mathbf{T}^{(n)\star} = \left(\mathbf{\Sigma}_e^{(n)} + \mathbf{\Theta}_e^{(n)}\right)^{-1}, \tag{15}$$

$$\mathbf{Q}^{(n)\star} = \left(\mathbf{\Sigma}_b^{(n)}\right)^{-1}. \tag{16}$$

Please note that the obtained problem structure (14) is not a jointly convex problem. Nevertheless, it is a convex problem separately over the sets $\mathbb{X}, \mathbb{W}$ and $\mathbb{Q}, \mathbb{T}$. Hence, we follow an iterative coordinate ascend update where in each iteration the original problem is solved over a subset of the original variable space, see [23, Subsection 2.7]. Firstly, the problem is solved over the variable sets $\mathbb{X}, \mathbb{W}$, assuming the auxiliary variables $\mathbf{Q}^{(n)}$ and $\mathbf{T}^{(n)}$ are fixed. This results in a convex sub-problem, where the optimum point is efficiently obtained using the MAX-DET algorithm [31]. Secondly, the problem is solved over the auxiliary variable sets $\mathbb{Q}, \mathbb{T}$, where the optimum solution is obtained in closed-form from (15), (16). This procedure is repeated until a stable point is obtained, see Algorithm 1. Please note that due to the monotonic increase of the objective (14a) in each optimization iteration, and the fact that the system secrecy capacity is bounded from above, the proposed algorithm leads to a necessary convergence. The average convergence behavior of Algorithm 1 is numerically studied in Section IV.

Algorithm 1 Iterative coordinate ascend method for sum secrecy rate maximization

1: $\ell \leftarrow 0$; set iteration number to zero
2: $\mathbb{X}_0 \leftarrow \epsilon \mathbf{I}_{M_a}$; initialization: equal power in different subcarriers and uniform spatial beam
3: $\mathbb{W}_0 \leftarrow \mathbf{0}_{M_{bt}}$; initialization: initialize with zero jamming power
4: $\mathbb{Q}_0, \mathbb{T}_0 \leftarrow \mathbf{0}$; initialization with zero matrices
5: **repeat**
6: $\quad \ell \leftarrow \ell + 1$;
7: $\quad \mathbb{X}_\ell, \mathbb{W}_\ell \leftarrow$ solve MAX-DET (14), with [31]
8: $\quad \mathbb{Q}_\ell, \mathbb{T}_\ell \leftarrow$ calculate (15) and (16)
9: **until** a stable point, or maximum number of ℓ reached
10: **return** $\{\mathbb{X}_\ell, \mathbb{W}_\ell, \mathbb{Q}_\ell, \mathbb{T}_\ell\}$

A. Optimal power allocation on Alice ($M_a = 1$)

In this part we study a special case where Alice is equipped with a single antenna, and hence the problem of finding

$\mathbf{X}^{(n)}$ reduces into a transmit power allocation problem among different subcarriers. In this regard, we focus on finding an optimal transmit strategy from Alice assuming a known jamming strategy. This approach is particularly interesting where a joint design for Bob and Alice is not possible due to, e.g., feedback delay and overhead, computation complexity. Moreover, the obtained power allocation solution may also serve as a basis for a low-complexity sub-optimal design for a general case where Alice is facilitated with multiple antennas.

The resulting power allocation problem on Alice, assuming a known jamming covariance is formulated as

$$\max_{X^{(n)}\geq 0,\ \forall n\in\mathcal{N}} \quad \sum_{n\in\mathcal{N}} f_n\left(X^{(n)}\right) \quad \text{s.t.} \quad \sum_{n\in\mathcal{N}} X^{(n)} \leq X_{\max}, \tag{17}$$

where

$$f_n\left(X^{(n)}\right) := \log\left(\frac{1+\alpha^{(n)}X^{(n)}}{1+\beta^{(n)}X^{(n)}}\right). \tag{18}$$

In the above formulation $f_n\left(X^{(n)}\right)$ is the realized secrecy capacity in the sub-carrier n, $\alpha^{(n)} := \mathbf{H}_{ab}^{(n)H}\left(\mathbf{\Sigma}_b^{(n)}\right)^{-1}\mathbf{H}_{ab}^{(n)}$ and $\beta^{(n)} := \mathbf{H}_{ae}^{(n)H}\left(\mathbf{\Sigma}_e^{(n)}\right)^{-1}\mathbf{H}_{ae}^{(n)}$, where $\alpha^{(n)}, \beta^{(n)} \in \mathbb{R}^+$. Note that a similar power allocation approach for sum secrecy rate maximization, in the context of HD broadcast multi-carrier systems is studied in [20], [32]. Nevertheless, due to the presence of FD jamming in our system, the impact of the residual SI at Bob as well as the impact of the received jamming signal at Eve are respectively incorporated in $\alpha^{(n)}$ and $\beta^{(n)}$. Referring to a similar mathematical structure as given in [20, Subsection III.A], in the following, we summarize necessary steps to obtain an optimal solution to (17).

It is observable from (18) that for $\alpha^{(n)} \leq \beta^{(n)}$ we have $X^{(n)\star} = 0$. On the other hand, for $\alpha^{(n)} > \beta^{(n)}$, the function $f_n\left(X^{(n)}\right)$ is a concave and increasing composition of a concave and increasing function in $X^{(n)}$, and hence is a concave function, see [29, Subsection 3.2.4]. As a result, we obtain the necessary and sufficient optimality conditions of (17) by via the corresponding KKT conditions. This results in a water-filling solution structure and can be expressed as in (20), where $\lambda > 0$ holds the concept of water level, c.f. [20, Equation (17)]. Moreover we have

$$0 \leq \lambda^\star \leq \left(\max_n \frac{\alpha^{(n)}-\beta^{(n)}}{\left(1+\alpha^{(n)}X_{\max}\right)\left(1+\beta^{(n)}X_{\max}\right)}\right) =: \lambda_{\max}, \tag{19}$$

which provides a feasible range for $\lambda^\star$ and is directly obtained from the KKT conditions. Hence, by choosing λ as a search variable, the optimal power allocation solution can be obtained with a water-filling procedure, see Algorithm 2 for the detailed procedure.

IV. Simulation Results

In this section we numerically evaluate the resulting sum secrecy rate of the defined system, comparing different system aspects and design strategies. In this respect, we assume that the channels $\mathbf{H}_X^{(n)}$ are following an uncorrelated Rayleigh distribution, with variance η_X for each element, where $X \in \{ab, ae, be\}$. Furthermore, $\mathbf{H}_{bb}^{(n)} \sim \mathcal{CN}\left(\sqrt{\frac{K_R}{1+K_R}}\mathbf{H}_0, \frac{1}{1+K_R}\mathbf{I}_{M_{br}} \otimes \mathbf{I}_{M_{bt}}\right)$, following [33], where

Algorithm 2 Water-filling optimization algorithm based on binary search

```
h ← λ_max, see (19)
l ← 0, see (19)
repeat
    λ ← (h + l)/2
    X^(n) ← see (20)
    X̃ ← Σ_{n∈N} X^(n)
    if (X_max − X̃) < 0 then
        l ← λ
    else
        h ← λ
    end if
until 0 ≤ X_max − X̃ < ε_0
return X^(n)
```

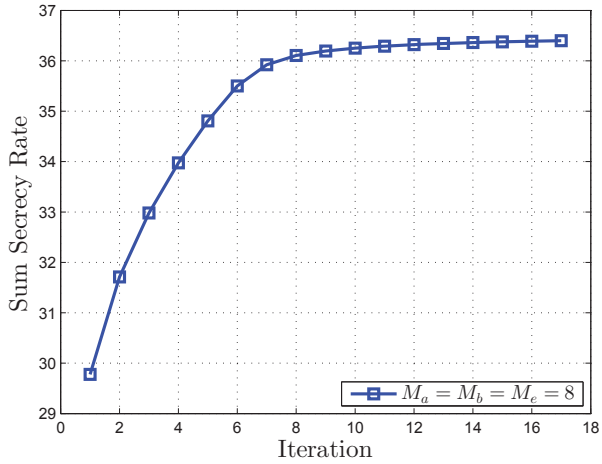

Figure 3. Average convergence behavior of the proposed iterative method. The proposed method converges to a stable point within 10-20 optimization iterations.

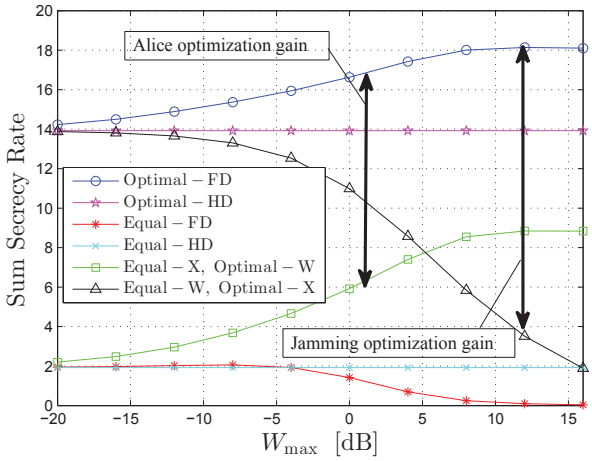

Figure 4. Obtained sum secrecy rate vs. maximum jamming power from Bob.

$\mathbf{H}_0$ is a matrix with all elements equal to 1 and K_R is the Rician coefficient. The resulting system performance is then averaged over 200 channel realizations. Unless otherwise is stated we use the following values to define our default setup: $M_a = 4$, $M_e = 4$, $M_b = M_{bt} = M_{br} = 4$, $|\mathcal{N}| = 4$, $K_R = 10$, $X_{\max} = W_{\max} = 1$, $\kappa = \kappa^{(n)} = -30$ dB, $\beta^{(n)} = \beta = -30$ [dB], $N_e = N_e^{(n)} = 0.1$, $N_b = N_b^{(n)} = 0.1$, $\eta_{ab} = \eta_{ae} = \eta_{be} = 0.01$.

$$X^{(n)\star} = \frac{1}{2}\left\{-\left(\frac{1}{\beta^{(n)}}+\frac{1}{\alpha^{(n)}}\right)+\sqrt{\left(\frac{1}{\beta^{(n)}}+\frac{1}{\alpha^{(n)}}\right)^2-4\left(\frac{1}{\alpha^{(n)}\beta^{(n)}}-\frac{1}{\lambda^\star}\left(\frac{1}{\beta^{(n)}}-\frac{1}{\alpha^{(n)}}\right)\right)}\right\}^+ \quad (20)$$

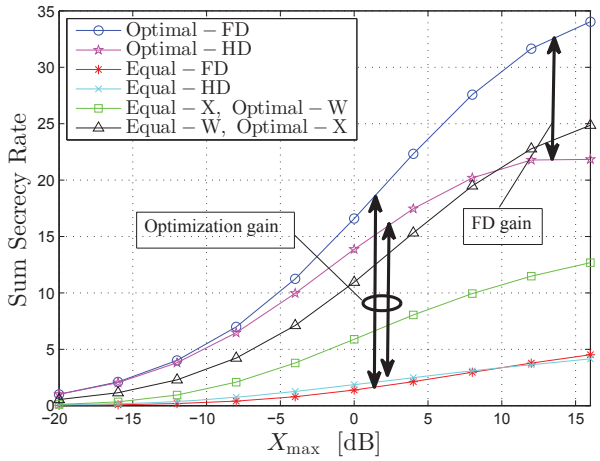

Figure 5. Obtained sum secrecy rate vs. maximum transmit power from Alice.

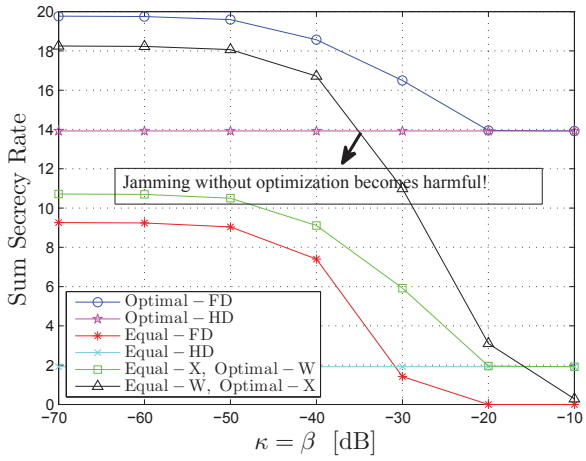

Figure 6. Obtained sum secrecy rate vs. transceiver dynamic range $\kappa = \beta$.

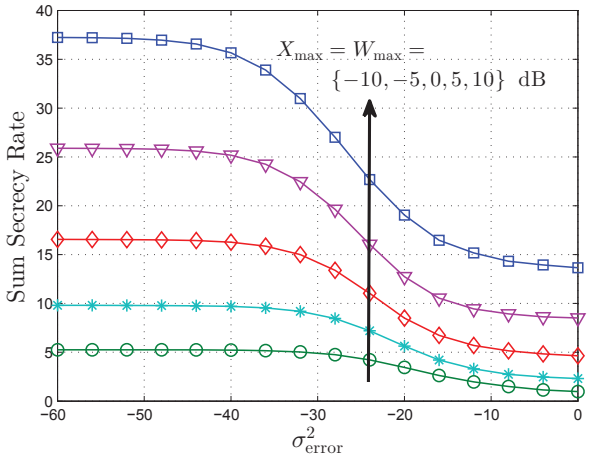

Figure 7. Average convergence behavior of the proposed iterative method. The proposed method converges to a stable point within fewer than 10 optimization iterations.

In Fig. 3 the average convergence behavior of the proposed iterative method is depicted. As it is observed, the convergence is obtained within 10-20 optimization iterations, which indicates the efficiency of the proposed iterative algorithm in terms of the required computational effort.

In Figs. 4-6 the resulting sum secrecy rate is depicted considering different design strategies. In this respect, 'Optimal-FD' represents the proposed design in Section III, supporting a FD jamming receiver. 'Optimal-HD' represents a similar setup with a HD Bob. 'Equal-FD' ('Equal-HD') is the setup with no optimization, i.e., a uniform power and beam allocation in all subcarriers for a system with an FD (HD) Bob. Furthermore, 'Equal-X, Optimal-W', represents the case with equal power and beam allocation over all subcarriers for Alice together with an optimal design of the jammer. Conversely, 'Equal-W, Optimal-X' represents the case with equal power and beam allocation for Bob together with an optimal design for Alice.

In Fig. 4 the impact of the maximum jamming power from Bob is depicted. A considerable gain is observed in this respect for a system with optimized jamming. Nevertheless, such gain is limited as $W_{\max}$ increases. This stems from the fact that while jamming results in the degradation of Alice-Eve channel, the secrecy rate is bounded due to the limited Alice-Bob channel capacity. Moreover, it is observed that such jamming gain is only obtained by applying an optimally designed jamming transmit strategy. This emphasizes the impact of residual SI on the Alice-Bob communication, which should be controlled via jamming optimization. As a result, for a system with no jamming optimization, a high $W_{\max}$ results in a significantly lower secrecy rate due to the impact of residual SI.

In Fig. 5 the impact of the maximum transmit power from Alice on the obtained sum secrecy rate is depicted. Is is observed that as $X_{\max}$ increases, the system obtains a higher sum secrecy rate. The performance gain, due to the optimization of transmit strategies, and due to the jamming capability at Bob is observed.

In Fig. 6 the impact of the transceiver dynamic range is depicted. It is observed that as $\kappa(=\beta)$ increases, the jamming gain decreases due to the impact of residual SI. In this respect, for a transceiver with large values of $\kappa = \beta$ the jamming is turned-off for an optimally-designed system. On the other hand, a high κ results in a sever degradation of the system performance due to the impact of residual SI, if the jamming strategy is not optimally controlled.

A. *Sensitivity to CSI error*

In Fig. 7 the sensitivity of the proposed design, in terms of the resulting sum system secrecy rate, is observed with respect to the CSI error. The CSI error is modeled as $\tilde{H}_X^{(n)} = H_X^{(n)} + E_X^{(n)}$, $X \in \{ab, ae, be\}$, where $E_X^{(n)}$ is modeled as a matrix with Gaussian i.i.d. elements with variance σ^2_{error}. It is observed that as the CSI accuracy decreases, the performance of the proposed design decreases. Nevertheless, the performance converges to its minimum level as σ^2_{error} increases, as a high σ^2_{error}, is equivalent of having *no knowledge* of the

communication channels. Moreover, a system with a higher power level is more sensitive to CSI accuracy, compared to a system with a smaller $W_{\max} = X_{\max}$. This stems in the fact that as the transmit power decreases, the significance of the user noise increases and acts as the dominant factor in the system. In this respect, the impact of the CSI error becomes less significant, as noise acts as the dominant source of signal uncertainty.

V. Conclusion

In this paper we have studied a joint power and beam optimization problem for a multi-carrier and MIMO wiretap channel, where Bob is capable of FD jamming. It is observed that for a system with an adequately high SI cancellation capability, an optimal jamming strategy results in a significant improvement of the sum secrecy capacity. In particular, in a frequency selective setup, the frequency diversity in different subcarriers can be opportunistically used, both regarding the jamming and the desired information link, to jointly enhance the resulting secrecy capacity. Nevertheless, it is observed that a jamming strategy with no power and/or beam optimization may lead to a reduced system secrecy, particularly as the SI cancellation capability decreases.

References

[1] S. Hong, J. Brand, J. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5G and beyond," *IEEE Communications Magazine*, February 2014.

[2] D. Bharadia and S. Katti, "Full duplex MIMO radios," in *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation*, ser. NSDI'14, Berkeley, CA, USA, 2014, pp. 359–372.

[3] Y. Hua, P. Liang, Y. Ma, A. Cirik, and G. Qian, "A method for broadband full-duplex MIMO radio," *IEEE Signal Processing Letters*, vol. 19, Dec. 2011.

[4] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proceedings of the ACM SIGCOMM*, Aug. 2013.

[5] A. Sabharwal, P. Schniter, D. Guo, D. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *Selected Areas in Communications, IEEE Journal on*, vol. 32, no. 9, pp. 1637–1652, Sept 2014.

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

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[8] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, Oct 2013.

[9] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, March 2010.

[10] G. Zheng, L. C. Choo, and K. K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1317–1322, March 2011.

[11] L. Li, Z. Chen, D. Zhang, and J. Fang, "A full-duplex bob in the mimo gaussian wiretap channel: Scheme and performance," *IEEE Signal Processing Letters*, vol. 23, no. 1, pp. 107–111, Jan 2016.

[12] Y. Zhou, Z. Z. Xiang, Y. Zhu, and Z. Xue, "Application of full-duplex wireless technique into secure mimo communication: Achievable secrecy rate based optimization," *IEEE Signal Processing Letters*, vol. 21, no. 7, pp. 804–808, July 2014.

[13] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Transactions on Signal Processing*, vol. 62, Dec 2014.

[14] S. Parsaeefard and T. Le-Ngoc, "Full-duplex relay with jamming protocol for improving physical-layer security," in *2014 IEEE 25th Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, Sept 2014, pp. 129–133.

[15] S. Vishwakarma and A. Chockalingam, "Sum secrecy rate in miso full-duplex wiretap channel with imperfect csi," in *2015 IEEE Globecom Workshops (GC Wkshps)*, Dec 2015, pp. 1–6.

[16] A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in mimo wiretap channels: Construction and countermeasures," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov 2011, pp. 265–269.

[17] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Secure robust resource allocation in the presence of active eavesdroppers using full-duplex receivers," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Sept 2015, pp. 1–5.

[18] C. Jeong and I. M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5428–5442, Nov 2011.

[19] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for ofdm transmissions over fading channels," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1354–1367, Aug 2012.

[20] X. Wang, M. Tao, J. Mo, and Y. Xu, "Power and subcarrier allocation for physical-layer security in ofdma-based broadband wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 693–702, Sept 2011.

[21] H. Qin, Y. Sun, T. H. Chang, X. Chen, C. Y. Chi, M. Zhao, and J. Wang, "Power allocation and time-domain artificial noise design for wiretap ofdm with discrete inputs," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2717–2729, June 2013.

[22] M. Li, Y. Guo, K. Huang, and F. Guo, "Secure power and subcarrier auction in uplink full-duplex cellular networks," *China Communications*, vol. 12, no. Supplement, pp. 157–165, 2015.

[23] D. Bertesekas, "Nonlinear programming. athena scientific," *Belmont, Massachusetts*, 1999.

[24] B. P. Day, A. R. Margetts, D. W. Bliss, and P. Schniter, "Full-duplex bidirectional MIMO: Achievable rates under limited dynamic range," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3702–3713, July 2012.

[25] M. Jain, J. I. Choi, T. Kim, D. Bharadia, K. Srinivasan, S. Seth, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," in *Proceedings of 17th Annual International Conference on Mobile Computing and Networking (MobiCom)*, Las Vegas, NV, Sep. 2011.

[26] V. Aggarwal, M. Duarte, A. Sabharwal, and N. Shankaranarayanan, "Full-or half-duplex? a capacity analysis with bounded radio resources," in *Information Theory Workshop (ITW), 2012 IEEE*. IEEE, 2012, pp. 207–211.

[27] Y. Sun, D. W. K. Ng, J. Zhu, and R. Schober, "Multi-objective optimization for robust power efficient and secure full-duplex wireless communication systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 8, pp. 5511–5526, Aug 2016.

[28] S. Petersen and M. Pedersen, *Matrix Cookbook*, 2008.

[29] S. P. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.

[30] J. Jose, N. Prasad, M. Khojastepour, and S. Rangarajan, "On robust weighted-sum rate maximization in MIMO interference networks," in *2011 IEEE International Conference on Communications (ICC)*, June 2011, pp. 1–6.

[31] L. Vandenberghe, S. Boyd, and S.-P. Wu, "Determinant maximization with linear matrix inequality constraints," *SIAM Journal on matrix analysis and applications*, vol. 19, no. 2, pp. 499–533, 1998.

[32] 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.

[33] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Transactions on Wireless Communications*, December 2012.