Sum Secrecy Rate Maximization for Multi-Carrier MIMOME Systems with Full-Duplex Jamming

Tianyu Yang, Omid Taghizadeh, and Rudolf Mathar

***Abstract*—In this work we study the sum secrecy rate maximization problem for a multi-carrier and multiple-input-multiple-output multiple-antenna eavesdropper (MIMOME) communication system. We consider the setup that the receiver is capable of full-duplex (FD) operation and simultaneously sends jamming signal to a potential eavesdropper. In particular, we intend to achieve a higher security level in the physical layer by simultaneously utilizing the spatial and frequency diversity of the FD-enabled system. In order to deal with the non-convex nature of the problem, we reformulate the problem as a separately convex program and propose an iterative algorithm. The iterative solution has a guaranteed convergence based on block coordinate descent method. Furthermore, for a simplified scenario where the transmitter is only equipped with a single antenna, the system is mitigated to a transmit power allocation problem. We obtain an optimal solution analytically with the assumption of a known jamming strategy. We also study an FD bidirectional secure communication system, where both transceivers are capable of FD operation. The numerical evaluations indicate the gain of an optimized jamming strategy for an FD multi-carrier system.**

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

I. Introduction

Full-Duplex (FD) transceivers are capable of simultaneous transmission and reception on the same channel [2], [3], and thereby can improve wireless communication systems in many aspects, e.g., obtaining higher spectral efficiency and information security. Nevertheless, the performance of such systems has limitations due to the inherent self-interference (SI) of the transmitters. Recently, specialized SI suppression methods, e.g., [4]–[6], have shown a sufficient level of isolation between transmit and receive chains. Thus, the FD communication is facilitated and a broad range of relevant studies are motivated. For instance, the feasibility of the in-band FD is investigated in [7]–[9] and recently the FD implementation is studied in massive MIMO systems via digital beamforming [10], [11].

Benefiting from such capability, FD transceivers are capable to significantly improve the security of wireless systems in the physical layer. Specifically, while the transceiver receives the desired information signal, it is also capable to simultaneously transmit the jamming signal to the potential eavesdroppers. Note that current communication systems typically ensure information security by cryptographic approaches. These secret key based approaches mainly rely on the assumption that the potential eavesdroppers have few available computational power. Therefore, it is hardly possible for them to break the exchanged secret key in a considerable short period of time. On the other hand, due to the significant advances in computing power of digital processors and the growth of quantum computing, this assumption is increasingly undermined. Therefore, it is increasingly interesting to guarantee the information security of wireless communication systems in the physical layer. Moreover, the physical layer security approaches can be combined with the cryptographic approaches to enhance the system security, e.g., the secret key of the cryptographic approaches can be distributed through the secured communication channels.

The fundamental concept of the wiretap channel is introduced in [12]. Within this wiretap channel, a legitimate communicating between Alice (the transmitter) and Bob (the receiver) is eavesdropped by Eve (an illegitimate receiver). In the wiretap channel, secrecy capacity is defined as the maximum information rate that can be communicated under perfect secrecy, i.e., without being accessible by the illegitimate receivers [12]. The secrecy capacity with the consideration of various aspects, e.g., achievable performance, channel coding, system design, and resource optimization, is investigated in recent years, see [13]–[15] and the references therein.

The utilization of FD jamming transceivers for the purpose of enhancing the secrecy capacity is studied in [16]. In this work, an FD Bob as a jammer is capable to transmit jamming signal, considering a single antenna Alice and a passive eavesdropper. The employment of an FD jammer eliminates the requirement of external helpers, which are commonly used for the purpose of cooperative jamming and thereby degrading the received signal quality at the eavesdropper [17], [18]. Thus, the problems of synchronization and trustworthiness in the cooperative jamming schemes are avoided. Then, the FD-enabled system [16] is extended to MIMO systems [19], [20]. Furthermore, the FD-aided systems with simultaneous information and jamming transmission are widely investigated. For instance, in [21] the FD node operates as a base station. In [22] an FD jamming Bob operates as a jamming relay that simultaneously transmits jamming and relays the information signal to other nodes. In [23] a bidirectional wiretap channel is considered with a joint FD operation of both Alice and Bob. In [24] the system with an active eavesdropper, which is capable of FD operation, is studied. In [25], the maximization of the sum secrecy rate in both communication directions is targeted.

In the aforementioned works, all of the physical links are assumed as single-carrier, frequency-flat channel model. In contrast, the security enhancement in multi-carrier, frequency selective systems with half-duplex (HD) links is studied in

Authors are with the Institute for Theoretical Information Technology, RWTH Aachen University, Aachen, 52074, Germany (e-mail: yang, taghizadeh, mathar@ti.rwth-aachen.de).

Part of this work has been presented in ICC'17-WT07, the 2017 IEEE International Conference on Communications Workshops [1].

[26]–[29]. It is known that multi-carrier schemes are at the heart of current wireless standards to facilitate transmit/receive processing, deal with multi-path fading and channel frequency selectivity. In particular, Cyclic Prefix Orthogonal Frequency Division Multiplexing (CP-OFDM) has been recently chosen by 3GPP for the 5G standardization. Hence, it is interesting to investigate the use of FD jamming transceivers for a frequency-selective and multi-carrier communication system. In particular, the diverse channel response in different subcarriers can be opportunistically used, both regarding the jamming and the desired information links, in order to jointly improve the achievable secrecy capacity.

Although FD jammig is considered as a promising mechanism, the main drawback is the impact of residual self-interference, which degrades the capacity of the desired information link. Therefore, a smart design is required in the FD-enabled multi-carrier and multiple-input-multiple-output multiple-antenna eavesdropper (MIMOME) setup with the consideration of residual self-interference. Furthermore, unlike HD transceivers, where the operation of different subcarriers can be separated up to a coupled power constraint, the communication at different subcarriers may not be separated in an FD-enabled system, due to the impact of inter-carrier leakage. In particular, the non-linear hardware distortions, which are inherent in the operation of FD transceivers, due to the strength of the self-interference signal, spread over the active spectrum, and cause inter-carrier leakage (ICL). In the other words, the transmission at one subcarrier, would also lead to an increased impact of distortion at other subcarriers. This requires the use of a distortion-aware modeling of the FD-multi-carrier transceiver, and a joint design of beam/power allocation at all subcarriers taking into account the impact of inter-carrier leakage and the residual self-interference. In this work, we make use of the distortion and ICL-aware analysis to improve the secrecy rate of the multi-carrier MIMOME channel, under the consideration of hardware impairments and ICL.

A. Contribution

In this paper, we address the optimization of transmission strategies in a multi-carrier and MIMOME wiretap channel, with the goal of maximizing the resulting sum secrecy rate. The main contributions are as follows:

- In contrast to the designs [16]–[20], without considering multi-carrier, frequency selective channel systems, or the designs [26]–[29], without considering FD capability, we intend to achieve a higher security level in physical layer by simultaneously utilizing the spatial and frequency diversity of the FD-enabled system. In Section III, a sum secrecy rate maximization problem is formulated. To deal with the non-convex and highly coupled nature of the problem, we reformulate the problem as a separately convex program and propose an iterative algorithm. The iterative solution has a guaranteed convergence based on block coordinate descent method [30, Subsection 2.7].
- The special scenario with a transmitter equipped with a single antenna is researched. An analytic power allocation solution is given using the water-filling method, assuming a known jamming strategy. Thus, the computational complexity is reduced.
- The utilization of FD operation both on Alice and Bob leads a bidirectional information exchange and jamming system. This bidirectional system has the potentials for the improvement of sum secrecy rate, due to the fact that jamming of one node can degrade Eve's decoding capability on both communication directions. Motivated by this, in Section IV we extend the proposed optimization algorithm for a secure FD bidirectional communication system.

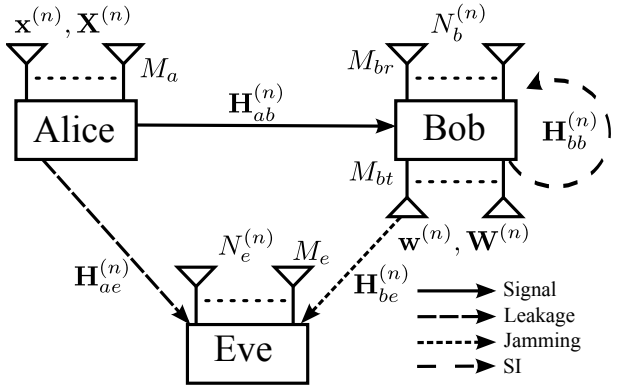

Figure 1. The studied MIMOME wiretap channel. Bob is capable of FD jamming. The subcarrier index is denoted as n.

The numerical results in Section V show that the system using the proposed optimization algorithm can achieve a significant sum secrecy rate gain under high self-interference cancellation levels.

B. Used Notations

The sets of real, non-negative real, complex, natural numbers and the set of all positive semi-definite matrices with Hermitian symmetry are respectively denoted by $\mathbb{R}$, $\mathbb{R}^+$, $\mathbb{C}$, $\mathbb{N}$ and $\mathcal{H}$. Column vectors (matrices) are denoted as lower (upper)-case and bold letters. The notations $\mathbb{E}\{\cdot\}$, $\mathrm{tr}(\cdot)$, $(\cdot)^{-1}$ $|\cdot|$, $(\cdot)^T$, $(\cdot)^*$ and $(\cdot)^H$, respectively represent the expectation, trace, inverse, determinant, transpose, conjugate and Hermitian transpose. The notation $\otimes$ represents the Kronecker product. An identity matrix with K columns is denoted as $\mathbf{I}_K$. The operator $\mathrm{vec}(\cdot)$ stacks the elements as a vector. An all-zero matrix with size $m \times n$ is denoted as $\mathbf{0}_{m\times n}$. $\perp$ represents the statistical independence. $\mathrm{diag}(\cdot)$ returns a diagonal matrix. $\|\cdot\|_F$ returns Frobenius norm of a matrix. $\{a\}^+$ is equal to $a \in \mathbb{R}$ if $a \geq 0$, and zero otherwise. Furthermore, $\mathcal{CN}(\mathbf{x}, \mathbf{X})$ denotes the complex normal distribution with mean $\mathbf{x}$ and covariance $\mathbf{X}$.

II. System Model

We study a classic wiretap channel: Alice (the legitimate transmitter) transmits a message to Bob (the legitimate/desired receiver) while Eve (the illegitimate/undesired receiver) intends to eavesdrop the transmitted information. Furthermore,

we consider a MIMOME system with multi-carrier, where FD-enabled Bob is capable to receive the information signal from Alice and simultaneously transmit jamming signal, i.e., the signal containing artificial noise, to Eve, see Fig. 1. The number of transmit antennas at Alice and receive antennas at Eve are denoted as M_a and M_e, respectively. The number of transmit (receive) antennas at Bob is denoted as M_{bt} (M_{br}). We assume that the channel of each subcarrier follows a quasi-stationary and flat-fading model. Then, Alice to Bob and Alice to Eve channels, i.e., intended communication and information leakage channels, are denoted as $\mathbf{H}_{ab}^{(n)} \in \mathbb{C}^{M_{br}\times M_a}$ and $\mathbf{H}_{ae}^{(n)} \in \mathbb{C}^{M_e\times M_a}$, respectively. Furthermore, Bob to Bob and Bob to Eve channels, i.e., SI and jamming channels, are denoted as $\mathbf{H}_{bb}^{(n)} \in \mathbb{C}^{M_{br}\times M_{bt}}$ and $\mathbf{H}_{be}^{(n)} \in \mathbb{C}^{M_e\times M_{bt}}$, respectively. In the aforementioned notations, $n \in \mathcal{N}$ denotes the subcarrier index, and $\mathcal{N}$ is the index set of all subcarriers.

A. Signal model

The transmit signal in n-th subcarrier from Alice is expressed as

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

where $\mathbf{s}^{(n)} \sim \mathcal{CN}(\mathbf{0}_{d\times 1}, \mathbf{I}_d)$ and $\mathbf{V}^{(n)} \in \mathbb{C}^{M_a\times d}$ represent the data symbol vector to be transmitted and the precoder of n-th subcarrier, respectively. Furthermore, the number of parallelly transmitted data streams is denoted as $d \in \mathbb{N}$. On the other hand, Bob transmits a jamming signal $\mathbf{w}^{(n)} \sim \mathcal{CN}\left(\mathbf{0}_{M_{bt}\times 1}, \mathbf{W}^{(n)}\right)$, where $\mathbf{W}^{(n)} \in \mathbb{C}^{M_{bt}\times M_{bt}}$ is the jamming transmit covariance. In order to prevent Eve from decoding the jamming signal, we use artificial noise to form the jamming signal transmitted by Bob, which is unlike the information-containing signal transmitted by Alice, see [31, Equation (5)]. It is worth to mention that the jamming signal from Bob influences the security level in two antithetical sides. On one hand, the jamming signal acts as an additional interference term to Eve. Thus, it can degrade the undesired Alice to Eve channel. On the other hand, due to the imperfect self-interference cancellation (SIC), the residual SI can also degrade the desired Alice to Bob channel. Due to this antithetical impact, it is crucial to have an optimal scheme for the jamming operation.

The received signal by Bob and Eve are expressed as

$$\mathbf{y}_b^{(n)} = \mathbf{H}_{ab}^{(n)}\mathbf{x}^{(n)} + \mathbf{n}_b^{(n)} + \mathbf{z}_b^{(n)}, \tag{2}$$

$$\mathbf{y}_e^{(n)} = \mathbf{H}_{ae}^{(n)}\mathbf{x}^{(n)} + \mathbf{H}_{be}^{(n)}\mathbf{w}^{(n)} + \mathbf{n}_e^{(n)}, \tag{3}$$

where $\mathbf{n}_b^{(n)} \sim \mathcal{CN}\left(\mathbf{0}_{M_{br}\times 1}, N_b^{(n)}\mathbf{I}_{M_{br}}\right)$ and $\mathbf{n}_e^{(n)} \sim \mathcal{CN}\left(\mathbf{0}_{M_e\times 1}, N_e^{(n)}\mathbf{I}_{M_e}\right)$ are the additive white noise on Bob and Eve, respectively. $\mathbf{z}_b^{(n)} \in \mathbb{C}^{M_{br}}$ represents the residual SI signal after the SIC process in n-th subcarrier.

We assume the perfect CSI on Alice to Bob, Alice to Eve, and Bob to Eve channels. This is achievable for Alice to Eve and Bob to Eve channels when Eve is a collaborative node, e.g., an idle user or an untrusted communication node [32]. In this case, the privacy information should be protected from the decoding of the undesired receiver. Additionally, the study with perfect CSI provides a valuable performance bound of the system. Moreover, in Section V we provide the numerical evaluation on the sensitivity of the resulting system performance to the CSI accuracy.

B. Sum secrecy rate

We intend to enhance the system security by maximizing the achievable sum secrecy rate. The secrecy rate for the n-th subcarrier of the defined system is expressed as

$$\begin{aligned}\mathcal{I}_{\text{sec}}^{(n)} &= \left\{\mathcal{I}_{ab}^{(n)} - \mathcal{I}_{ae}^{(n)}\right\}^+ \\ &= \left\{I\left(\mathbf{x}^{(n)}; \mathbf{y}_b^{(n)}\right) - I\left(\mathbf{x}^{(n)}; \mathbf{y}_e^{(n)}\right)\right\}^+ \\ &= \left\{\log_2\left|\mathbf{I}_d + \mathbf{H}_{ab}^{(n)}\mathbf{X}^{(n)}\left(\mathbf{H}_{ab}^{(n)}\right)^H\left(\mathbf{\Sigma}_b^{(n)}\right)^{-1}\right|\right. \\ &\qquad \left. - \log_2\left|\mathbf{I}_d + \mathbf{H}_{ae}^{(n)}\mathbf{X}^{(n)}\left(\mathbf{H}_{ae}^{(n)}\right)^H\left(\mathbf{\Sigma}_e^{(n)}\right)^{-1}\right|\right\}^+,\end{aligned} \tag{4}$$

where $\mathcal{I}_{\text{sec}}^{(n)}$ is the resulting secrecy rate in the n-th subcarrier, $\mathcal{I}_{ab}^{(n)}$ and $\mathcal{I}_{ae}^{(n)}$ represent the information capacity of Alice to Bob and Alice to Eve paths, respectively. $\mathbf{X}^{(n)} = \mathbb{E}\left\{\mathbf{x}^{(n)}\mathbf{x}^{(n)H}\right\} = \mathbf{V}^{(n)}\mathbf{V}^{(n)H}$ is the transmit covariance from Alice in the n-th subcarrier. Furthermore, $\mathbf{\Sigma}_e^{(n)}$ in (4), calculated as $\mathbf{\Sigma}_e^{(n)} = N_e^{(n)}\mathbf{I}_{M_e} + \mathbf{H}_{be}^{(n)}\mathbf{W}^{(n)}\mathbf{H}_{be}^{(n)H}$, represents the covariance of the received noise-plus-interference signal at Eve. $\mathbf{\Sigma}_b^{(n)}$ in (4) represents the covariance of the aggregate noise-plus-residual-interference signal at Bob. The calculation of $\mathbf{\Sigma}_b^{(n)}$ is presented in (8) in the following Subsection II-C, where the residual SI model is introduced.

Then, the sum secrecy rate of the studied multi-carrier system is expressed as

$$\mathcal{I}_{\text{sum}} = \sum_{n\in\mathcal{N}} \mathcal{I}_{\text{sec}}^{(n)}. \tag{5}$$

C. Residual SI model

According to the recent SIC approaches [33], three different sources of error, which cause residual SI, are recognized. Specifically, in channel estimation domain, the error comes from the inaccuracy of channel state information (CSI) of SI channels. In the analog domain, the error comes from the inaccuracy of hardware in transmit and receive chains. In the following parts, we briefly introduce each part separately and study their impact on our system.

1) Linear SIC error: The estimation accuracy for the CSI of SI channels is limited, especially when the channel coherence time is short, see [34, Subsection 3.4.1], [35, Subsection V.C]. For this reason, the CSI estimation error of the SI channels in n-th subcarrier is expressed 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 the matrix of zero-mean i.i.d. elements with unit variance, and $\mathbf{D}_{bb}^{(n)}$ incorporates spatial correlation, see [33, Equation (8), (9)].

2) Transmitter distortion: The inaccuracy of the analog hardware in the transmit chains, e.g., digital-to-analog converter error, power amplifier noise and oscillator phase noise, can be comprehensively modeled as an additive Gaussian distortion signal for each transmit chain [33]. Hence, the collective impact is formulated as $q_l(t) = e_{\mathrm{T},l}(t) + w_l(t)$, such that

$$\begin{aligned} &e_{\mathrm{T},l}(t) \sim \mathcal{CN}\left(0, \kappa \mathbb{E}\{w_l(t) w_l(t)^*\}\right), \\ &e_{\mathrm{T},l}(t) \perp w_l(t),\ e_{\mathrm{T},l}(t) \perp e_{\mathrm{T},l}(t'),\ e_{\mathrm{T},l}(t) \perp e_{\mathrm{T},l'}(t), \end{aligned} \tag{6}$$

where w_l, $e_{\mathrm{T},l}$ and $q_l \in \mathbb{C}$ are the intended, i.e., distortion-free, transmit signal, additive transmit distortion and the actual transmit signal from the l-th transmit chain, respectively. t represents the instance of time[1]. Furthermore, in (6) $t \neq t^{'}, l \neq l^{'}$ and $\kappa \in \mathbb{R}^+$ represents the distortion coefficient. Note that the distortion coefficient shows a linear relation between the intended transmit power and the collective power of the distortion signal.

3) Receiver distortion: The receiver distortion is analyzed the same way as the transmit chain. The comprehensive impact of the inaccurate hardware, e.g., analog-to-digital converter error, oscillator phase noise and automatic gain control noise, is considered. Similarly, we model the receiver distortion as an additive distortion term $\tilde{q}_l(t) = e_{\mathrm{R},l}(t) + u_l(t)$, such that

$$\begin{aligned} &e_{\mathrm{R},l}(t) \sim \mathcal{CN}\left(0, \beta \mathbb{E}\{u_l(t) u_l(t)^*\}\right), \\ &e_{\mathrm{R},l}(t) \perp u_l(t),\ e_{\mathrm{R},l}(t) \perp e_{\mathrm{R},l}(t^{'}),\ e_{\mathrm{R},l}(t) \perp e_{\mathrm{R},l'}(t), \end{aligned} \tag{7}$$

where u_l, $e_{\mathrm{R},l}$ and $\tilde{q}_l \in \mathbb{C}$ are the intended, i.e., distortion-free, receive signal, additive receive distortion and the actual received signal from the l-th receive chain, respectively. Furthermore, $\beta \in \mathbb{R}^+$ plays a similar role as κ in relation to the distortion signal variance of the receiver chains.

Note that our model of the distortion parts for transmit and receive chains are based on two major intuitions. Firstly, unlike the thermal noise model, in each transmit or receive chain the variance of the distortion parts is proportional to the signal power. Secondly, the distortion signals and the intended transmit or receive signals are statistically independent. Moreover, the distortion signals at different chains or at different time instance are also statistical independent. In general, they follow a spatially and temporally white statistics, see [33, Subsection II.C], and [33, Subsection II.D].

Based on the modeling from (6) and (7), the covariance of the combined noise-plus-residual-interference signal on Bob is formulated as

$$\begin{aligned} \mathbf{\Sigma}_b^{(n)} &= \mathbb{E}\left\{ \left(\mathbf{n}_b^{(n)} + \mathbf{z}_b^{(n)}\right) \left(\mathbf{n}_b^{(n)} + \mathbf{z}_b^{(n)}\right)^H \right\} \\ &= \mathbf{H}_{bb}^{(n)} \left(\kappa^{(n)} \sum_{n \in \mathcal{N}} \mathrm{diag}\left(\mathbf{W}^{(n)}\right) \right) \mathbf{H}_{bb}^{(n)H} \\ &\quad + \beta^{(n)} \mathrm{diag}\left(\sum_{n \in \mathcal{N}} \mathbf{H}_{bb}^{(n)} \mathbf{W}^{(n)} \mathbf{H}_{bb}^{(n)H} \right) \\ &\quad + \mathrm{tr}\left(\mathbf{W}^{(n)}\right) \mathbf{D}_{bb}^{(n)} \mathbf{D}_{bb}^{(n)H} \\ &\quad + N_b^{(n)} \mathbf{I}_{M_{br}}, \end{aligned} \tag{8}$$

where $\kappa^{(n)}$ ($\beta^{(n)}$) represents the transmit (receive) distortion coefficient relating to the collective power of the intended transmit (receive) signal to the distortion signal variance in the n-th subcarrier[2] [36].

Please note that comparing to other links the SI channels are notably stronger, which causes the influences of the studied inaccuracies, i.e., $e_{\mathrm{T},l}, e_{\mathrm{R},l}, \mathbf{E}_{bb}^{(n)}$, significant for an FD transceiver. As an example, after passing through the strong SI channel $\mathbf{H}_{bb}^{(n)}$, the transmit distortion signals would become comparable to the indented signal that passes through the much weaker channel $\mathbf{H}_{ab}^{(n)}$. However, these discussed inaccuracies can be ignored in the links that do not contain the SI paths, i.e., $\kappa \ll 1, \beta \ll 1$ and $\left\|\mathbf{E}_{bb}^{(n)}\right\|_F \ll \left\|\mathbf{H}_{bb}^{(n)}\right\|_F$.

D. Transmit power constraints

We make a practical assumption that the total available transmit power of any device is limited. This is expressed as

$$\mathrm{tr}\left(\sum_{n \in \mathcal{N}} \mathbf{X}^{(n)} \right) \leq X_{\max}, \ \ \mathrm{tr}\left(\sum_{n \in \mathcal{N}} \mathbf{W}^{(n)} \right) \leq W_{\max}, \tag{9}$$

where $X_{\max} \in \mathbb{R}^+$ and $W_{\max} \in \mathbb{R}^+$ represent the maximum transmit power from Alice and Bob, respectively. Since Bob transmits only jamming signals, $W_{\max}$ is also considered as the maximum jamming power.

III. Sum Secrecy Rate Maximization

In this part, we present an optimization algorithm to maximize the system's sum secrecy rate over all subcarriers, see (5), under the defined power constraints for Alice and Bob in (9). This is formulated as the following optimization problem

$$\max_{\mathbb{X}, \mathbb{W}} \quad \mathcal{I}_{\mathrm{sum}} \ \text{ s.t. } (9) \tag{10}$$

where $\mathbb{X}$ ($\mathbb{W}$) is the set of $\mathbf{X}^{(n)} \succeq 0$ ($\mathbf{W}^{(n)} \succeq 0$), $\forall n \in \mathcal{N}$. Via the utilization of (4) as well as the matrix identities [37,

[1]The signal in time domain contains the superposition of signal components 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 is not completely flat.

Eq. (516)] we reformulated the defined problem as

$$\max_{\mathbb{X},\mathbb{W}} \quad \sum_{n\in\mathcal{N}} \Bigg\{ \log_2\left|\mathbf{\Sigma}_b^{(n)}+\mathbf{\Theta}_b^{(n)}\right| - \log_2\left|\mathbf{\Sigma}_b^{(n)}\right| - \log_2\left|\mathbf{\Sigma}_e^{(n)}+\mathbf{\Theta}_e^{(n)}\right| + \log_2\left|\mathbf{\Sigma}_e^{(n)}\right| \Bigg\}^+ \tag{11a}$$

$$\text{s.t.} \;\; \text{tr}\left(\mathbf{\Theta}\right) \leq X_{\max}, \;\; \text{tr}\left(\mathbf{\Sigma}\right) \leq W_{\max}, \tag{11b}$$

where $\mathbf{\Theta} := \sum_{n\in\mathcal{N}} \mathbf{X}^{(n)}$, $\mathbf{\Theta}_b^{(n)} := \mathbf{H}_{ab}^{(n)}\mathbf{X}^{(n)}\left(\mathbf{H}_{ab}^{(n)}\right)^H$, and $\mathbf{\Theta}_e^{(n)} := \mathbf{H}_{ae}^{(n)}\mathbf{X}^{(n)}\left(\mathbf{H}_{ae}^{(n)}\right)^H$ 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 $\mathbf{W}^{(n)}$. Nevertheless, due to the non-linear operation $\{\cdot\}^+$, the above problem is intractable. Furthermore, the maximization of difference of such $\log(\cdot)$ functions lead to a class of difference-of-convex (DC) problems which is jointly or separately a non-convex problem [38]. We firstly remove the non-linear operation $\{\cdot\}^+$ with the following remark. Then, the DC problems are relaxed with the utilization of the lemma III.1 and a more tractable form of the objective function is obtained.

Remark III.1. *The operator $\{\cdot\}^+$ does not influence the objective at the optimum point of (11).*

Proof: It can be observed that the operator $\{\cdot\}^+$ has no effect, when the value inside the operator is non-negative for all of the subcarriers $n \in \mathcal{N}$. In case the value inside the operator is negative for any of the subcarriers at the optimality, Alice and Bob can jointly turn off the transmission in the corresponding subcarrier, i.e., choosing $\mathbf{X}^{(n)} = \mathbf{0}, \mathbf{W}^{(n)} = \mathbf{0}$, and contribute the saved power to another subcarrier with a positive secrecy rate. This leads to an improvement of $\mathcal{I}_{\text{sum}}$, and hence contradicts the initial optimality assumption. ■

Lemma III.1. *The maximization of the term $-log\left|\mathbf{A}\right|$, where $\mathbf{A} \in \mathbb{C}^{l\times l}$ is positive-definite, is equivalent to the following maximization*

$$\max_{\mathbf{A}\succ 0,\mathbf{B}\succ 0} \; log\left|\mathbf{B}\right| - tr\left(\mathbf{BA}\right) + c, \tag{12}$$

in terms of the optimal value of $\mathbf{A}$ and the objective value, where $\mathbf{B} \in \mathbb{C}^{l\times l}$ and c is an arbitrary constant.

Proof: It is observed that (12) is a convex optimization problem over $\mathbf{B}$, when $\mathbf{A}$ is fixed. Hence, by setting the derivative of the objective function to zero, the optimal $\mathbf{B}$ is obtained. Concretely, let $f(\mathbf{B}) = \log|\mathbf{B}| - \text{tr}(\mathbf{BA}) + c$, we have $\frac{\partial f(\mathbf{B})}{\partial \mathbf{B}} = (\mathbf{B}^{-1})^T - \mathbf{A}^T \overset{!}{=} 0$. Accordingly, we have $\mathbf{B}^\star = \mathbf{A}^{-1}$. This leads to an equal objective expression as in (12) to the term $-\log\left|\mathbf{A}\right|$ at the optimality of $\mathbf{B}$, which concludes the proof, see also [39, Lemma 2]. ■

In order to deal with the intractable terms $-\log\left|\mathbf{\Sigma}_b^{(n)}\right|$ and $-\log\left|\mathbf{\Sigma}_e^{(n)}+\mathbf{\Theta}_e^{(n)}\right|$, the auxiliary variables $\mathbf{Q}^{(n)} \in \mathbb{C}^{M_{br}\times M_{br}}$ and $\mathbf{T}^{(n)} \in \mathbb{C}^{M_e\times M_e}$ are additionally introduced following the aforementioned lemma III.1. Then, by applying the defined remark and lemma, we reformulate (11) equivalently as

$$\max_{\mathbb{X},\mathbb{W},\mathbb{Q},\mathbb{T}} \quad \sum_{n\in\mathcal{N}} \Bigg(\log\left|\mathbf{\Sigma}_b^{(n)}+\mathbf{\Theta}_b^{(n)}\right| + \log\left|\mathbf{\Sigma}_e^{(n)}\right| \tag{13a}$$

$$- \text{tr}\left(\mathbf{Q}^{(n)}\mathbf{\Sigma}_b^{(n)}\right) - \text{tr}\left(\mathbf{T}^{(n)}\left(\mathbf{\Sigma}_e^{(n)}+\mathbf{\Theta}_e^{(n)}\right)\right)$$

$$+ \log\left|\mathbf{Q}^{(n)}\right| + \log\left|\mathbf{T}^{(n)}\right| \Bigg) \tag{13b}$$

$$\text{s.t.} \quad \text{tr}\left(\mathbf{\Theta}\right) \leq X_{\max}, \;\; \text{tr}\left(\mathbf{\Sigma}\right) \leq W_{\max}, \tag{13c}$$

where the set $\mathbb{Q}$ ($\mathbb{T}$) is the set of $\mathbf{Q}^{(n)} \succeq 0$ ($\mathbf{T}^{(n)} \succeq 0$), $\forall n \in \mathcal{N}$. Following the calculation described in lemma III.1, the optimal values of the auxiliary variables are then obtained as

$$\mathbf{T}^{(n)\star} = \left(\mathbf{\Sigma}_e^{(n)}+\mathbf{\Theta}_e^{(n)}\right)^{-1}, \tag{14}$$

$$\mathbf{Q}^{(n)\star} = \left(\mathbf{\Sigma}_b^{(n)}\right)^{-1}. \tag{15}$$

Please note that (13) is not a convex optimization problem. However, it is a separately convex problem over the variable sets $\mathbb{X}, \mathbb{W}$ and $\mathbb{Q}, \mathbb{T}$, in each case when the remaining variables are fixed. This enables an alternating solution update following the block coordinate ascend, where in each iteration a convex sub-problem is solved [30, Subsection 2.7]. The first sub-problem is to update the variables $\mathbb{X}, \mathbb{W}$, while fixing the other optimization variables. In this case, the optimum point is efficiently obtained using the MAX-DET algorithm [40]. The second sub-problem is to optimally update the auxiliary variables $\mathbb{Q}, \mathbb{T}$, following the closed-form expressions (14), (15). The aforementioned updates are repeated until a stable point is achieved or a pre-defined number of iterations is expired, see Algorithm 1. It is worth mentioning that the proposed iterative update leads to a necessary convergence, due to the monotonic nature of the objective (13a) value in each optimization iteration, and the fact that the system secrecy capacity is bounded from above. The convergence behavior of the proposed iterative update is investigated in Section V via numerical simulations.

A. Initialization

Note that the solution of Algorithm 1 does not necessarily converge to the global optimum point. Hence, the resulting performance depends on the used initialization. In this section, we discuss two initialization methods that we find efficient for the optimization problem in (13).

1) Uniform covariance with equal power initialization: This simple initialization method initializes the covariance matrix of the transmit signal by uniform covariance matrix with equal power, i.e., $\mathbf{Q} \leftarrow \epsilon\mathbf{I}$, where ϵ is the allocated power of each subcarrier. In our case, $\mathbf{Q}$ represents any matrix of $\mathbf{X}^{(n)}, \mathbf{W}^{(n)}, \forall n \in \mathcal{N}$ at the initial iteration. This initialization method is the most intuitive method and easy to be applied. It can also prevent a bad design where the initial beam is against the optimality, so that a large number of iterations for correcting the wrong beam is avoided.

2) Optimal spatial beam initialization: This initialization method aims to obtain optimal spatial beam, where the transmit signal is orientated to the desired receiver and prevent signal leakage to the undesired directions. This is defined as the following maximization

$$\max_{\mathbf{Q}\in\mathcal{H}} \quad \frac{\text{tr}(\mathbf{F}\mathbf{Q}\mathbf{F}^H)+\nu_f}{\text{tr}(\mathbf{G}\mathbf{Q}\mathbf{G}^H)+\nu_g}, \ \text{ s.t. } \text{tr}(\mathbf{Q})=1, \tag{16}$$

where $\mathbf{Q}$ represents the normalized covariance matrix of the transmit signal, $\mathbf{F}$ and $\mathbf{G}$ are the desired and undesired channels, ν_f, ν_g are the noise variances at the desired and undesired receivers, respectively. An optimal solution to (16) is obtained as

$$\text{vec}(\mathbf{Q}^{\star\frac{1}{2}}) = \mathcal{P}_{\max}\left(\left(\mathbf{I}\otimes\mathbf{G}^H\mathbf{G}+\nu_g\mathbf{I}\right)^{-1}\left(\mathbf{I}\otimes\mathbf{F}^H\mathbf{F}+\nu_f\mathbf{I}\right)\right), \tag{17}$$

where $\mathcal{P}_{\max}(\cdot)$ calculates the dominant eigenvector[3]. The transmit power is equally allocated. Please note that the above approach is applied separately for the initialization of the covariance matrix of information signal ($\mathbf{X}^{(n)}$) and jamming signal ($\mathbf{W}^{(n)}$) in each subcarrier. Specifically, for the design of $\mathbf{X}^{(n)}$, we set $\mathbf{F}\leftarrow\mathbf{H}_{ab}^{(n)}$ and $\mathbf{G}\leftarrow\mathbf{H}_{ae}^{(n)}$. For the design of $\mathbf{W}^{(n)}$ we set $\mathbf{F}\leftarrow\mathbf{H}_{be}^{(n)}$. The choice of $\mathbf{G}$ for $\mathbf{W}^{(n)}$ is related to the impact of distortion terms on Bob, which reflects the effect of the residual self-interference. The distortion power at Bob in n-th subcarrier can be written as

$$\begin{aligned}
&\text{tr}\left(\kappa^{(n)}\mathbf{H}_{bb}^{(n)}\text{diag}\left(\mathbf{W}^{(n)}\right)\mathbf{H}_{bb}^{(n)H}\right)\\
&+\text{tr}\left(\text{tr}\left(\mathbf{W}^{(n)}\right)\mathbf{D}_{bb}^{(n)}\mathbf{D}_{bb}^{(n)H}\right)\\
&+\text{tr}\left(\beta^{(n)}\text{diag}\left(\mathbf{H}_{bb}^{(n)}\mathbf{W}^{(n)}\mathbf{H}_{bb}^{(n)H}\right)\right)\\
&\triangleq \text{tr}\left(\tilde{\mathbf{H}}_{bb}^{(n)}\mathbf{W}^{(n)}\right),
\end{aligned} \tag{18}$$

where $\tilde{\mathbf{H}}_{bb}^{(n)} = \kappa^{(n)}\text{diag}\left(\mathbf{H}_{bb}^{(n)H}\mathbf{H}_{bb}^{(n)}\right)+\beta^{(n)}\mathbf{H}_{bb}^{(n)H}\mathbf{H}_{bb}^{(n)}+\text{tr}\left(\mathbf{D}_{bb}^{(n)}\mathbf{D}_{bb}^{(n)H}\right)\mathbf{I}_{M_{bt}}$, which consequently results in the choice of $\mathbf{G}\leftarrow\left(\tilde{\mathbf{H}}_{bb}^{(n)}\right)^{\frac{1}{2}}$.

In Algorithm 1 we apply the uniform covariance with equal power initialization. The performance of two initialization methods and the optimality gap are numerically compared and analyzed in Subsection V-A by examining multiple random initializations.

B. Analytical computational complexity

To analyze the computational complexity of arithmetic operations we consider the floating-point operations (FLOP)s [41]. One FLOP represents a complex multiplication or a complex summation. Then, the arithmetic operations for the calculation of $\mathbb{Q}_l$ and $\mathbb{T}_l$ via (14), (15) with the inverse terms via Cholesky decomposition in Algorithm 1 are in total

$$\begin{aligned}
&\mathcal{O}\Big(\gamma N\Big(M_e^3+M_{br}^3+M_{bt}Me(2M_{bt}+M_e)\\
&\quad+M_aM_e(2M_a+M_e)+M_{bt}M_{br}(2M_{bt}+3M_{br})\Big)\Big)
\end{aligned}$$

FLOPs [41], where γ is the total number of required iterations until convergence.

The main complexity of Algorithm 1 is incurred in the steps of the determinant maximization. A general MAX-DET optimization problem is formulated as

$$\min_{\mathbf{z}} \ \mathbf{p}^T\mathbf{z}+\log\left|\mathbf{Y}(\mathbf{z})^{-1}\right|, \ \text{s.t. } \mathbf{Y}(\mathbf{z})\succ, \mathbf{F}(\mathbf{z})\succeq 0, \tag{19}$$

such that $\mathbf{z}\in\mathbb{R}^n$, and $\mathbf{Y}(\mathbf{z})\in\mathbb{R}^{n_Y\times n_Y} := \mathbf{Y}_0+\sum_{i=1}^n z_i\mathbf{Y_i}$ and $\mathbf{F}(\mathbf{z})\in\mathbb{R}^{n_F\times n_F} := \mathbf{F}_0+\sum_{i=1}^n z_i\mathbf{F}_i$. The arithmetic complexity of the aforementioned problem, see [40, Section 10], is upper bounded as

$$\mathcal{O}\left(\gamma\sqrt{n}(n^2+n_Y^2)n_F^2\right). \tag{20}$$

In the above expression, γ represents the required number of iterations until a stable solution is reached. For the studied optimization problem, $n = N(M_a^2+M_{bt}^2)$ represents the dimension of real valued scalar variable space. Moreover, $n_Y = N(M_e+M_{br})$ and $n_F = N(M_a+M_{bt})+2$ represent the dimension of the determinant operation and the constraint space, respectively.

It is worth mentioning that the given analysis only shows how the bounds on computational complexity are related to different problem dimensions. In practice, the actual computational load may vary depending on the structure simplifications and used numerical solvers.

Algorithm 1 Iterative coordinate ascend method for sum secrecy rate maximization

1: $\ell\leftarrow 0$; set iteration number to zero
2: $\mathbb{X}_0\leftarrow\epsilon\mathbf{I}_{M_a}$; initialize with equal power in different subcarriers and uniform spatial beam
3: $\mathbb{W}_0\leftarrow\mathbf{0}_{M_{bt}}$; initialize with zero jamming power
4: $\mathbb{Q}_0,\mathbb{T}_0\leftarrow\mathbf{0}$; initialize with zero matrices
5: **repeat**
6: $\quad\ell\leftarrow\ell+1$;
7: $\quad\mathbb{X}_\ell,\mathbb{W}_\ell\leftarrow$ solve MAX-DET (13), with [40]
8: $\quad\mathbb{Q}_\ell,\mathbb{T}_\ell\leftarrow$ calculate (14) and (15)
9: **until** a stable point, or maximum number of ℓ reached
10: **return** $\{\mathbb{X}_\ell,\mathbb{W}_\ell,\mathbb{Q}_\ell,\mathbb{T}_\ell\}$

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

In this part, we investigate the special setup that Alice is equipped with a single antenna. As a result, the optimization of $\mathbf{X}^{(n)}$ reduces to the optimization of transmit power among different subcarriers. In particular, we intend to find an optimal strategy of the transmit power allocation for Alice, assuming that the jamming strategy is already known. This scheme is especially valuable when the joint design for both Alice and Bob is not feasible due to, e.g., computation complexity, feedback delay, and overhead. Furthermore, in a general case with an Alice equipped with multiple antennas, the power

[3]Due to the calculation of the dominant eigenvector, this initialization method has higher complexity.

$$X^{(n)\star} = \frac{1}{2}\left\{-\left(\frac{1}{\beta^{(n)}}+\frac{1}{\alpha^{(n)}}\right)+\sqrt{\left(\frac{1}{\beta^{(n)}}+\frac{1}{\alpha^{(n)}}\right)^2-4\left(\frac{1}{\alpha^{(n)}\beta^{(n)}}-\frac{1}{\lambda^\star}\left(\frac{1}{\beta^{(n)}}-\frac{1}{\alpha^{(n)}}\right)\right)}\right\}^+ \tag{21}$$

allocation solution obtained from the single antenna case can also provide a basis for a sub-optimal solution within the low-complexity design.

The corresponding optimization problem of single antenna Alice case is expressed as

$$\max_{X^{(n)}\geq 0,\ \forall n\in\mathcal{N}} \quad \sum_{n\in\mathcal{N}} f_n\left(X^{(n)}\right) \quad \text{s.t.} \quad \sum_{n\in\mathcal{N}} X^{(n)} \leq X_{\max}, \tag{22}$$

where

$$f_n\left(X^{(n)}\right) := \log\left(\frac{1+\alpha^{(n)}X^{(n)}}{1+\beta^{(n)}X^{(n)}}\right). \tag{23}$$

In (23), $\alpha^{(n)} := \mathbf{H}_{ab}^{(n)H}\left(\mathbf{\Sigma}_b^{(n)}\right)^{-1}\mathbf{H}_{ab}^{(n)}$ and $\beta^{(n)} := \mathbf{H}_{ae}^{(n)H}\left(\mathbf{\Sigma}_e^{(n)}\right)^{-1}\mathbf{H}_{ae}^{(n)}$, where $\alpha^{(n)},\beta^{(n)} \in \mathbb{R}^+$. $f_n\left(X^{(n)}\right)$ represents the realized secrecy capacity in the n-th subcarrier. It is noted that in [28], [42] similar power allocation schemes for sum secrecy rate maximization are investigated within HD broadcast multi-carrier systems. However, because of the existence of FD jamming in our system, the influence of the residual SI on Bob as well as the influence of the received jamming signal on Eve are respectively incorporated in $\alpha^{(n)}$ and $\beta^{(n)}$. The optimization problem in (22) is in general not convex. Nevertheless, the following lemma shows a solution with a convex sub-problem.

Lemma III.2. *The optimization problem in (22) can be mitigated to a convex sub-optimization problem, which has the optimization form in (22) with $n \in \tilde{\mathcal{N}}$, where $\tilde{\mathcal{N}} \subseteq \mathcal{N}$ and $\alpha^{(n)} > \beta^{(n)}$, $\forall n \in \tilde{\mathcal{N}}$.*

Proof: From (23) it is noticed that for $\alpha^{(n)} \leq \beta^{(n)}$ the optimal solution is zero, i.e., $X^{(n)\star} = 0$. Conversely, 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 $X^{(n)}$. Therefore, it is a concave function, see [38, Subsection 3.2.4]. Maximization of a concave function together with the convex constraints leads a convex sub-problem of (22) under the condition of $\alpha^{(n)} > \beta^{(n)}$. ■

To obtain an optimal solution of the convex sub-problem of (22) we consider the Lagrangian function of the objective function:

$$\mathcal{L}\left(\mathbb{X},\lambda,\boldsymbol{\tau}\right) = \sum_{n\in\tilde{\mathcal{N}}} f_n(X^{(n)}) + \lambda\left(X_{\max}-\sum_{n\in\tilde{\mathcal{N}}}X^{(n)}\right) + \sum_{n\in\tilde{\mathcal{N}}}\tau^{(n)}X^{(n)}, \tag{24}$$

where λ and $\boldsymbol{\tau}$, which is the set of $\tau^{(n)}, n \in \tilde{\mathcal{N}}$, are the Lagrange multipliers for the inequality constraints.

As a result of lemma III.2, we obtain the necessary and sufficient optimality conditions of the convex sub-problem of (22) via the corresponding Karush-Kuhn-Tucker (KKT) conditions:

$$\frac{\partial\mathcal{L}\left(\mathbb{X},\lambda,\boldsymbol{\tau}\right)}{\partial X^{(n)}} = 0\ , \quad \forall n\in\tilde{\mathcal{N}}, \tag{25a}$$

$$X^{(n)} \geq 0\ , \quad \forall n\in\tilde{\mathcal{N}}, \tag{25b}$$

$$X_{\max}-\sum_{n\in\tilde{\mathcal{N}}}X^{(n)} \geq 0, \tag{25c}$$

$$\lambda \geq 0, \tag{25d}$$

$$\tau^{(n)} \geq 0\ , \quad \forall n\in\tilde{\mathcal{N}}, \tag{25e}$$

$$\lambda\left(X_{\max}-\sum_{n\in\tilde{\mathcal{N}}}X^{(n)}\right) = 0\ , \tag{25f}$$

$$\tau^{(n)}X^{(n)} = 0\ , \quad \forall n\in\tilde{\mathcal{N}}. \tag{25g}$$

The following lemma reveals an important property of the allocated power values at the optimality.

Lemma III.3. *Let $\mathcal{N}_0 \subseteq \tilde{\mathcal{N}}$ be the set of subcarriers with zero allocated power at the optimality, i.e., $X^{(n)\star} = 0, \forall n \in \mathcal{N}_0$. Then we have*

$$\frac{\partial f_n\left(X^{(n)\star}\right)}{\partial X^{(n)}} = \lambda, \ \ \forall n\in\tilde{\mathcal{N}}\setminus\mathcal{N}_0. \tag{26}$$

Proof: For the subcarrier with $X^{(n)\star} > 0$, we have $\tau^{(n)} = 0$, due to (25g). Moreover, from (25a) we calculate $\frac{\partial f_n\left(X^{(n)\star}\right)}{\partial X^{(n)}} - \lambda + \tau^{(n)} = 0$. The two aforementioned arguments conclude the proof. ■

The above lemma follows the interesting intuition that for the subcarriers with positive allocated power, the slope of the objective function should be equal. This is expected since if a slope of the objective is not equal for different subcarriers, we can take power from the subcarrier with smaller slope and reallocate it to the subcarrier with a higher slope in the objective.

From (26) we obtain a water-filling solution which can be formulated as in (21), where $\lambda > 0$ represents the water level, c.f. [28, Equation (17)]. This identity shows that at the optimum the values of $X^{(n)\star}$ can be uniquely calculated for all subcarriers, once the value of $\lambda^\star$ is obtained. Moreover, we have a feasible range for $\lambda^\star$ as

$$0 \leq \lambda^\star \leq \left(\max_{n\in\tilde{\mathcal{N}}}\frac{\alpha^{(n)}-\beta^{(n)}}{\left(1+\alpha^{(n)}X_{\max}\right)\left(1+\beta^{(n)}X_{\max}\right)}\right) =: \lambda_{\max}. \tag{27}$$

Thus, we can obtain the optimal power allocation solution via the water-filling procedure. Specifically, we perform a

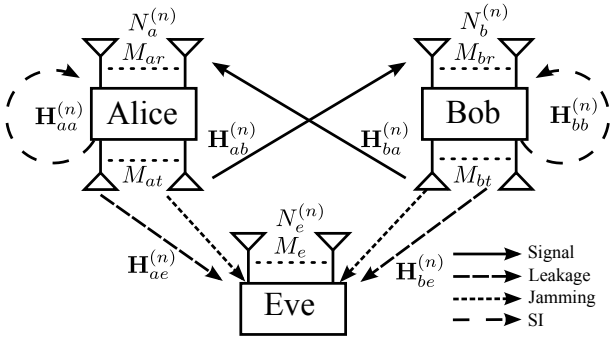

Figure 2. The studied bidirectional multi-carrier wiretap channel, where both Alice and Bob are FD nodes and able to jamming Eve.

bisection search to find the optimal water-level $\lambda^\star$. The detailed procedure is shown in Algorithm 2.

Algorithm 2 Binary search based Water-filling optimization algorithm

1: $h \leftarrow \lambda_{\max}$, see (27); Initialize the upper bound of the binary search
2: $l \leftarrow 0$, see (27); Initialize the lower bound of the binary search
3: **repeat**
4: $\lambda \leftarrow (h+l)/2$; Set water-level as middle point of the search range
5: $X^{(n)} \leftarrow$ see (21); Update power allocation
6: $\tilde{X} \leftarrow \sum_{n\in\mathcal{N}} X^{(n)}$; Calculate current total power
7: **if** $(X_{\max} - \tilde{X}) < 0$ **then**
8: $l \leftarrow \lambda$; Update the lower bound of the search range
9: **else**
10: $h \leftarrow \lambda$; Update the upper bound of the search range
11: **end if**
12: **until** $0 \le X_{\max} - \tilde{X} < \epsilon_0$
13: **return** $X^{(n)}$

IV. Secure Bidirectional Full-Duplex Communication

The proposed solution in Section III acts as an efficient optimization framework for the underlying multi-carrier system defined in Section II. In this part, we extend the same framework to support a more general setup where both Alice and Bob are capable of FD operation. This includes a bidirectional data communication between Alice and Bob, as well as the jamming capability at both nodes. The bidirectional system can improve the performance since it results in a higher spectral efficiency [33], and the jamming signal from each node (Alice or Bob) can degrade Eve's reception quality at both directions.

For the purpose of updating our system to a bidirectional setup, the number of transmit (receive) antennas at Alice, the channel from Bob to Alice and Alice's SI channel in n-th subcarrier are denoted as $M_{at}, M_{ar}, \mathbf{H}_{ba}^{(n)}$ and $\mathbf{H}_{aa}^{(n)}$, respectively, see Fig. 2. Moreover, we denote $\mathbf{s}_{\mathcal{X}}^{(n)}, \mathbf{x}_{\mathcal{X}}^{(n)}, \mathbf{w}_{\mathcal{X}}^{(n)}, \mathbf{V}_{\mathcal{X}}^{(n)}, \mathbf{X}_{\mathcal{X}}^{(n)}, \mathbf{W}_{\mathcal{X}}^{(n)}$ as the same signal types as in Section II, but specific for the node $\mathcal{X}$, such that $\mathcal{X} \in \{a, b\}$. Thus, the transmit signal from each node is updated as $\mathbf{u}_{\mathcal{X}}^{(n)} = \mathbf{x}_{\mathcal{X}}^{(n)} + \mathbf{w}_{\mathcal{X}}^{(n)}$ with $\mathbf{x}_{\mathcal{X}}^{(n)} = \mathbf{V}_{\mathcal{X}}^{(n)} \mathbf{s}_{\mathcal{X}}^{(n)}$, containing both the information and jamming signal from each node. Then, the received interference-plus-noise covariance matrix in the n-th subcarrier at Alice, Bob and Eve are updated as

$$\begin{aligned}\tilde{\mathbf{\Sigma}}_{\mathcal{X}}^{(n)} &= N_{\mathcal{X}}^{(n)} \mathbf{I}_{M_{\mathcal{X}r}} + \mathbf{H}_{\mathcal{Y}\mathcal{X}}^{(n)} \mathbf{W}_{\mathcal{Y}}^{(n)} {\mathbf{H}_{\mathcal{Y}\mathcal{X}}^{(n)}}^H \\ &\quad + \text{tr}\left(\mathbf{X}_{\mathcal{X}}^{(n)} + \mathbf{W}_{\mathcal{X}}^{(n)}\right) \mathbf{D}_{\mathcal{X}\mathcal{X}}^{(n)} {\mathbf{D}_{\mathcal{X}\mathcal{X}}^{(n)}}^H \\ &\quad + \mathbf{H}_{\mathcal{X}\mathcal{X}}^{(n)} \left(\kappa_{\mathcal{X}}^{(n)} \sum_{n\in\mathcal{N}} \text{diag}\left(\mathbf{X}_{\mathcal{X}}^{(n)} + \mathbf{W}_{\mathcal{X}}^{(n)}\right)\right) {\mathbf{H}_{\mathcal{X}\mathcal{X}}^{(n)}}^H \\ &\quad + \beta_{\mathcal{X}}^{(n)} \text{diag}\left(\sum_{n\in\mathcal{N}} \mathbf{H}_{\mathcal{X}\mathcal{X}}^{(n)} \left(\mathbf{X}_{\mathcal{X}}^{(n)} + \mathbf{W}_{\mathcal{X}}^{(n)}\right) {\mathbf{H}_{\mathcal{X}\mathcal{X}}^{(n)}}^H\right),\end{aligned} \tag{28}$$

$$\tilde{\mathbf{\Sigma}}_{e}^{(n)} = N_{e}^{(n)} \mathbf{I}_{M_e} + \mathbf{H}_{ae}^{(n)} \mathbf{W}_{a}^{(n)} {\mathbf{H}_{ae}^{(n)}}^H + \mathbf{H}_{be}^{(n)} \mathbf{W}_{b}^{(n)} {\mathbf{H}_{be}^{(n)}}^H, \tag{29}$$

where $\mathcal{X} \neq \mathcal{Y} \in \{a, b\}$. Moreover, $\kappa_a^{(n)}(\kappa_b^{(n)}) \in \mathbb{R}^+$ and $\beta_a^{(n)}(\beta_b^{(n)}) \in \mathbb{R}^+$ are the transmit and receive distortion coefficients at Alice (Bob) in the n-th subcarrier, $N_a^{(n)}$ represents the thermal noise variance at Alice in the n-th subcarrier. Please note that in (29) we consider the worst case scenario where the information signal from Alice and Bob as interference can be decoded by Eve [43]. The defined system secrecy rate is hence written as

$$\tilde{\mathcal{I}}_{\text{sec}}^{(n)} = \left\{\tilde{\mathcal{I}}_{ab}^{(n)} - \tilde{\mathcal{I}}_{ae}^{(n)}\right\}^+ + \left\{\tilde{\mathcal{I}}_{ba}^{(n)} - \tilde{\mathcal{I}}_{be}^{(n)}\right\}^+, \tag{30}$$

where $\tilde{\mathcal{I}}_{ab}^{(n)} - \tilde{\mathcal{I}}_{ae}^{(n)}$ is obtained by applying (28) and (29) into (4), $\tilde{\mathcal{I}}_{ba}^{(n)} - \tilde{\mathcal{I}}_{be}^{(n)}$ is obtained as

$$\begin{aligned}\tilde{\mathcal{I}}_{ba}^{(n)} - \tilde{\mathcal{I}}_{be}^{(n)} &= \log_2 \left|\mathbf{I}_d + \mathbf{H}_{ba}^{(n)} \mathbf{X}_b^{(n)} {\mathbf{H}_{ba}^{(n)}}^H \left(\tilde{\mathbf{\Sigma}}_a^{(n)}\right)^{-1}\right| \\ &\quad - \log_2 \left|\mathbf{I}_d + \mathbf{H}_{be}^{(n)} \mathbf{X}_b^{(n)} {\mathbf{H}_{be}^{(n)}}^H \left(\tilde{\mathbf{\Sigma}}_e^{(n)}\right)^{-1}\right|,\end{aligned} \tag{31}$$

and the sum secrecy rate is defined the same as (5).

A. Bidirectional sum secrecy rate maximization

Similarly to Section III, to maximize the sum secrecy rate in bidirectional communication system the optimization problem is written as

$$\max_{\tilde{\mathbb{X}}, \tilde{\mathbb{W}}} \quad \sum_{n\in\mathcal{N}} \tilde{\mathcal{I}}_{\text{sec}}^{(n)} \tag{32a}$$

$$\text{s.t.} \quad \text{tr}\left(\tilde{\mathbf{\Theta}}_a\right) \le P_{A,\max}, \tag{32b}$$

$$\text{tr}\left(\tilde{\mathbf{\Theta}}_b\right) \le P_{B,\max}, \tag{32c}$$

where $\tilde{\mathbb{X}}$ ($\tilde{\mathbb{W}}$) express the set of $\mathbf{X}_{\mathcal{X}}^{(n)} \succeq 0$ ($\mathbf{W}_{\mathcal{X}}^{(n)} \succeq 0$), $\forall n \in \mathcal{N}$, $\tilde{\mathbf{\Theta}}_{\mathcal{X}} := \sum_{n\in\mathcal{N}} \left(\mathbf{X}_{\mathcal{X}}^{(n)} + \mathbf{W}_{\mathcal{X}}^{(n)}\right)$, $\mathcal{X} \in \{a, b\}$ and $P_{A,\max}, P_{B,\max} \in \mathbb{R}^+$ express the maximum transmit power of Alice and Bob.

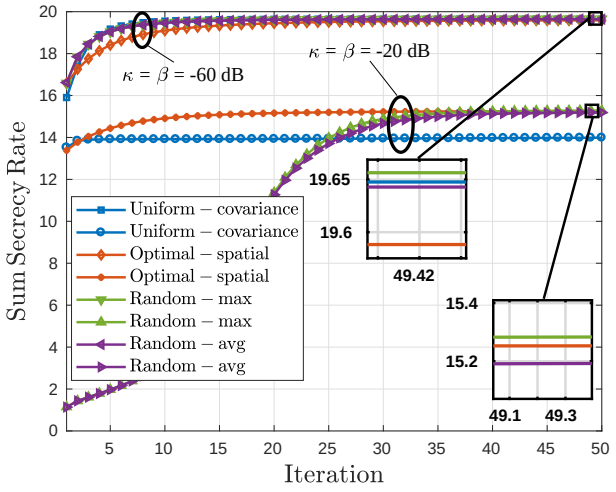

Figure 3. Average convergence behavior and the impact of initialization on the proposed iterative method.

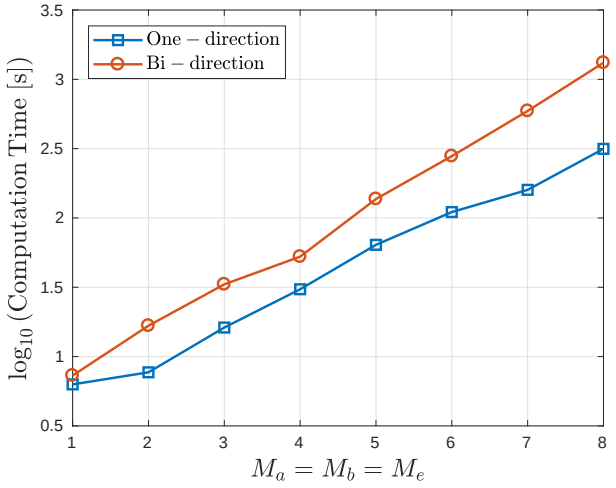

Figure 4. Average computation time of the proposed iterative algorithm.

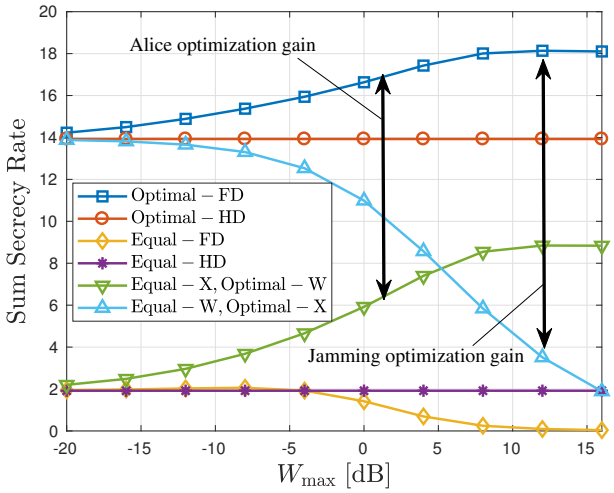

Figure 5. Sum secrecy rate vs. maximum jamming power from Bob.

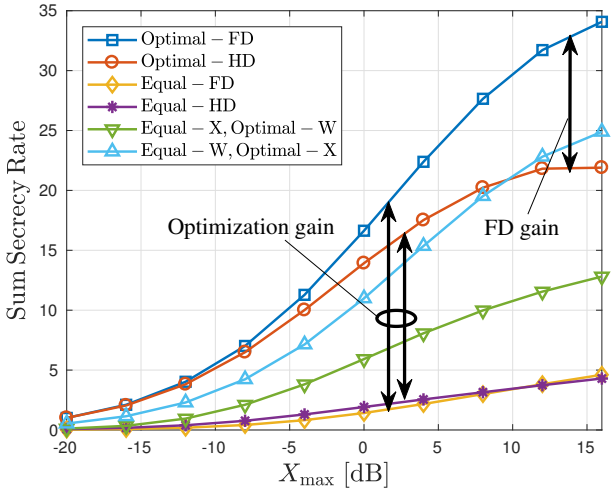

Figure 6. Sum secrecy rate vs. maximum transmit power from Alice.

It is observed that the optimization problem in (32) remains a similar mathematical structure as the formulation in (11), relating to the matrices of transmit covariance, i.e., $\mathbf{X}_{\mathcal{X}}^{(n)}$, $\mathbf{W}_{\mathcal{X}}^{(n)}$, $\mathcal{X} \in \{a, b\}, \forall n \in \mathcal{N}$. Thus, following the result of the Remark III.1 and Lemma III.1, we apply a similar procedure as in the Algorithm 1 to achieve an optimal solution. The computational complexity of the steps for the determinant maximization is obtained similar to (20), where $n = 2N(M_{at}^2 + M_{bt}^2)$, $n_Y = N(M_e + M_{ar} + M_{br})$ and $n_F = 2N(M_{at} + M_{bt}) + 2$.

V. Simulation Results

In this section, we investigate the achievable sum secrecy rate via numerical simulations, comparing different designs and system possibilities. We assume that the channels $\mathbf{H}_X^{(n)}$ are following an uncorrelated Rayleigh distribution, with variance η_X for each element, where $X \in \{ab, ba, ae, be\}$. Moreover, $\mathbf{H}_{bb}^{(n)} \sim \mathcal{CN}\left(\sqrt{\frac{\sigma_{\text{SI}}^2 K_R}{1+K_R}}\mathbf{H}_0, \frac{\sigma_{\text{SI}}^2}{1+K_R}\mathbf{I}_{M_{br}} \otimes \mathbf{I}_{M_{bt}}\right)$, following [44], where $\mathbf{H}_0$ is a matrix where all elements are equal to 1, K_R is the Rician coefficient, and σ_{SI}^2 represents the self-interference channel strength. The SI channel statistics for Alice, i.e., $\mathbf{H}_{aa}^{(n)}$, is defined similarly. The obtained sum secrecy rate is then averaged by examining 200 channel instances. Unless otherwise is stated, the default values of simulation parameters are as follows: $M_a = M_{at} = M_{ar} = 4$, $M_b = M_{bt} = M_{br} = 4$, $M_e = 4$, $|\mathcal{N}| = 4$, $X_{\max} = W_{\max} = P_{A,\max} = P_{B,\max} = 0$dB, $\kappa = \kappa^{(n)} = -30$dB, $\beta = \beta^{(n)} = -30$dB, $N_a = N_a^{(n)} = -30$dB, $N_b = N_b^{(n)} = -30$dB, $N_e = N_e^{(n)} = -30$dB, $\eta_{ab} = \eta_{ba} = \eta_{ae} = \eta_{be} = -20$dB, $K_R = 10$, $\sigma_{\text{SI}}^2 = 0$dB, $\hat{\mathbf{D}}_{\mathcal{X}\mathcal{X}} = \hat{\mathbf{D}}_{\mathcal{X}\mathcal{X}}^{(n)} = \mathbf{D}_{\mathcal{X}\mathcal{X}}^{(n)}\mathbf{D}_{\mathcal{X}\mathcal{X}}^{(n)\,H} = \mathbf{0}_{M_{\mathcal{X}r} \times M_{\mathcal{X}r}}, \mathcal{X} \in \{a, b\}$.

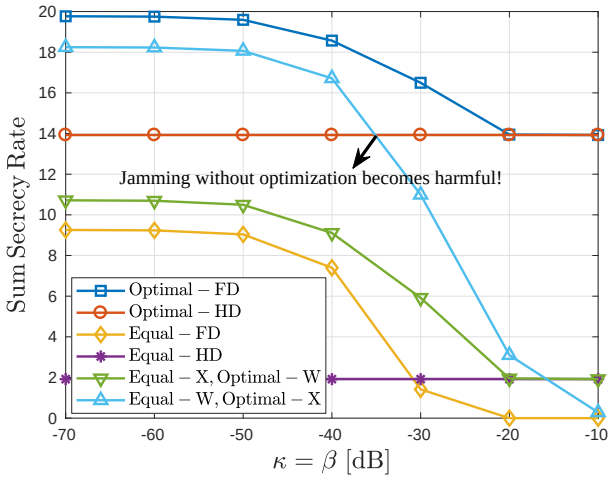

Figure 7. Sum secrecy rate vs. transceiver dynamic range $\kappa = \beta$.

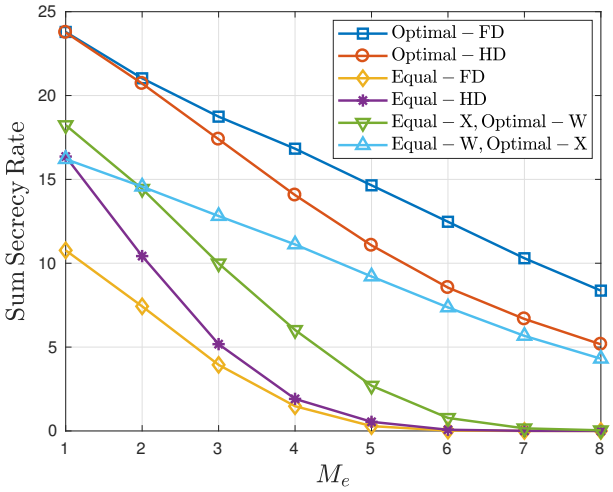

Figure 9. Sum secrecy rate vs. number of the receive antennas at Eve.

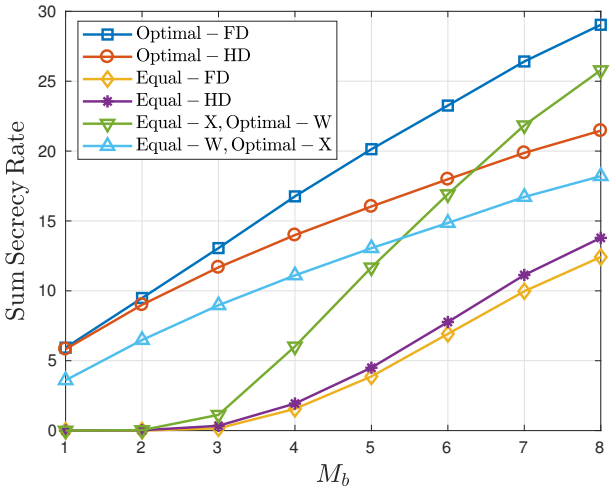

Figure 8. Sum secrecy rate vs. number of the transmit/receive antennas at Bob $M_b = M_{bt} = M_{br}$.

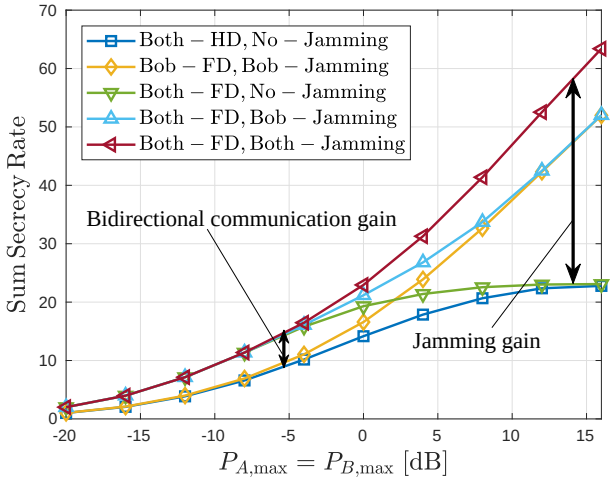

Figure 10. Performance of bidirectional secure communication related to maximum transmit power per node.

A. *Algorithm analysis*

In this part, the average convergence behavior and the effect of algorithm initialization are studied. Moreover, the computational complexity of the proposed design is investigated.

In Fig. 3 the convergence behavior and the impact of the initialization method are depicted. 'Uniform-covariance', 'Optimal-spatial', 'Random-max', 'Random-avg' represent the uniform covariance with equal power allocation initialization, optimal spatial beam initialization, the maximal and average value of random initialization, respectively. As observed, by using the proposed initialization, the convergence is obtained within 15-20 iterations. It is also observed that under high SIC level, i.e., low κ, β, the uniform covariance with equal power allocation initialization method reaches close to the benchmark performance[4]. Nevertheless, the optimal spatial beam initialization method results in a worse sum secrecy rate, however, within 0.36% of the relative difference. Conversely, under low SIC level, i.e., high κ, β, the algorithms associated with uniform covariance with equal power allocation initialization converge to a local optimal point with a very small number of iterations, which results in a relatively large difference margin (6-7%) compared to the benchmark. Nevertheless, the optimal spatial beam initialization method has a close performance compared to the benchmark in this case.

In Fig. 4 the average required computation time for single directional system ('One-direction') and bidirectional system ('Bi-direction') related to the equipped transmit/receive an-

[4]The benchmark performance is obtained by repeating the algorithm with 20 random initializations and choosing the highest obtained sum secrecy rate.

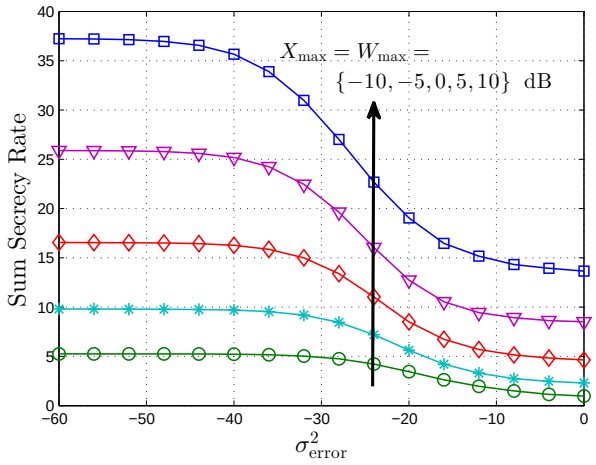

Figure 11. Sensitivity of proposed design with respect to the CSI error.

tenna number of all nodes are depicted[5]. One can observe that a higher antenna array size leads to a higher required computational complexity, associated with slower convergence and larger problem dimensions. Moreover, due to the additional problem complexity, the bidirectional communication system with joint FD-enabled jamming results in higher computation time.

B. Performance comparison

In this part, the sum secrecy rate obtained by the proposed FD-enabled systems is evaluated under different system conditions. The performance between the FD-enabled setup and HD setup are also compared.

1) FD jamming: In Figs. 5-9 the obtained performance, in terms of the system sum secrecy rate, is illustrated for different available designs. The legend 'Optimal-FD' corresponds to the design introduced in Section III, supporting an FD jamming receiver. The legend 'Optimal-HD' corresponds to a similar setup without FD jamming capability, i.e., with an HD Bob. 'Equal-FD' ('Equal-HD') corresponds to the scenario without optimization of transmit strategies, i.e., where a uniform power and beam allocation is used in all subcarriers for a system with an FD (HD) Bob. Moreover, the legend 'Equal-X, Optimal-W', corresponds to the scenario where equal power and beam allocation over all subcarriers is implemented for Alice together with an optimal design of the jammer. On the other hand, the legend 'Equal-W, Optimal-X' corresponds to the scenario where equal power and beam allocation is used for Bob, together with an optimal design for the transmit strategy for Alice.

In Fig. 5 the sum secrecy rate is illustrated for different values of the available jamming power from Bob. A notable improvement is observed for a system with an optimized jamming strategy. However, the observed improvement saturates as $W_{\max}$ grows large. This is grounded in the fact that while FD-jamming degrades Eve's reception quality, the secrecy rate is upper-bounded by the Alice-Bob channel capacity. Furthermore, a large optimization gain is observed as the available jamming power grows large. This shows the significant impact of the residual SI on the Alice-Bob communication as the jamming power increases, which should be controlled via jamming optimization. Hence, when no optimization is applied on the jamming strategy, the system secrecy capacity degrades rapidly as $W_{\max}$ increases.

In Fig. 6 the system sum secrecy rate is illustrated for different values of the available transmit power from Alice. It is observed that an increase in $X_{\max}$ leads to a higher sum secrecy rate. Moreover, it is observed that a notable performance gain is obtained, both via the optimization of the transmit strategies and also by enabling an FD jamming strategy at Bob, as $X_{\max}$ grows large.

In Fig. 7, the influence of the transceiver distortions is illustrated. It is observed that as the system dynamic range decreases, i.e., as the values of κ, β grow large, the jamming gain decreases due to the impact of residual SI. Moreover, it is observed that the optimization of the jamming strategy becomes essential, as the dynamic range decreases. This stems in the fact that for a transceiver with a low dynamic range, the jamming is usually turned-off for an optimally-designed system, in order to avoid a severe residual SI. Conversely, a high κ leads to a severe degradation of the system performance, if the jamming strategy is not optimally controlled.

In Fig. 8 and Fig. 9 the obtained sum secrecy rate is evaluated for different number of antennas at Bob and Eve. As expected, a more powerful Eve, i.e., higher M_e, results in reduced system secrecy. In this respect, the gain of FD jamming becomes clear in combating the increasing quality of Alice-Eve channel. On the other hand, it is observed that the resulting secrecy improves as M_b increases. In particular, the gain of FD jamming becomes significant as M_b increases, as the jamming beam can be directed to Eve more efficiently. Furthermore, for a smaller number of antennas at Bob, the optimization at Alice gains significance. This is perceivable, as a smaller M_b results in a smaller design freedom at Bob, and also a weaker Alice-Bob channel.

2) FD jamming and bidirectional communication: In Fig. 10 a secure bidirectional communication system is numerically studied. We consider three scenarios with respect to jamming capability. Specifically, 'Both-FD, No-Jamming', 'Both-FD, Bob-Jamming' and 'Both-FD, Both-Jamming' represent the FD-enabled bidirectional communication system without jamming capability, with jamming capability only at Bob and with jamming capability at both Alice and Bob, respectively. Moreover, two scenarios of the single direction communication system are also evaluated. Specifically, 'Both-HD, No-Jamming' represents the system with HD operation at Alice and Bob without jamming capability and 'Bob-FD, Bob-Jamming' represents the system with an HD Alice and an FD Bob as a jamming receiver.

It is observed that the bidirectional communication system

[5]The reported computation time is obtained using an Intel Core i7 4790S processor with the clock rate of 3.2 GHz and 16 GB of random access memory (RAM). The software platform is CVX [45], [46] with MATLAB 2014a on a 64-bit operating system.

leads to a considerable enhancement of sum secrecy rate in a wide range of $P_{A,\max}, P_{B,\max}$. Moreover, the jamming impact is more significant with large available power. From the results of 'Both-FD, Both-Jamming' and 'Both-FD, Bob-Jamming', it is also observed that the bidirectional jamming leads to a higher sum secrecy rate in the studied bidirectional system, because of the reused jamming power for both communication directions.

C. Sensitivity to CSI error

In Fig. 11 the impact of CSI error is illustrated for the proposed design[6]. In particular, the CSI error is modeled as $\tilde{H}_{\mathcal{X}}^{(n)} = H_{\mathcal{X}}^{(n)} + E_{\mathcal{X}}^{(n)}$, $\mathcal{X} \in \{ab, ae, be\}$, where $E_{\mathcal{X}}^{(n)}$ follows a Gaussian distribution with i.i.d. elements and with variance σ^2_{error}. One can observe that the performance of the proposed design decreases when the CSI accuracy decreases. However, as σ^2_{error} increases the sum secrecy rate slightly converges to a minimum level. This is because that a high σ^2_{error} is equivalent to holding *no knowledge* of the communication channels. Moreover, the results show that the sensitivity of the system performance to CSI error increases as the available power budget increases. It is grounded in the fact that for a system with low power budget the significance of the user noise increases. With regards to this, since the signal uncertainty is dominated by noise, the CSI error makes less impact.

It is worth to mention that in order to obtain a more reliable coding strategy in facing with CSI error, the coding can be applied over all subcarriers, or over all channels present in the communication duration, thereby reducing the dependency of the coding strategy to the instantaneous channel situation. In such a case, optimization objective in (11) will be replaced with

$$\left\{ \sum_{n\in\mathcal{N}} \left(\log_2 \left| \mathbf{\Sigma}_b^{(n)} + \mathbf{\Theta}_b^{(n)} \right| - \log_2 \left| \mathbf{\Sigma}_b^{(n)} \right| \right. \right. \\ \left. \left. -\log_2 \left| \mathbf{\Sigma}_e^{(n)} + \mathbf{\Theta}_e^{(n)} \right| + \log_2 \left| \mathbf{\Sigma}_e^{(n)} \right| \right) \right\}^+ \quad (33)$$

for both optimization and evaluation of the achievable rate. When the available CSI is strongly erroneous, this results in occasional negative values of secrecy rate for some of the subcarriers, leading to a slightly lower secrecy rate, see the numerical simulation with 200 channel realizations in Fig. 12.

D. Performance evaluation in WiFi standard

In order to verify the advantage of the proposed scheme in a practical scenario, in this subsection the proposed design is evaluated in a system following the WiFi standard. Specifically, we consider the uplink (UL) of a WiFi standard. The active UL user corresponds to Alice, the FD WiFi access point

[6]Please note that the illustrated values regarding the secrecy rate, are only subject to the existence of a channel code that achieve the corresponding secrecy rate. However, when the perfect CSI is not available, the exact coding strategy may not be directly calculated, and hence the reported values should be viewed as theoretical limits.

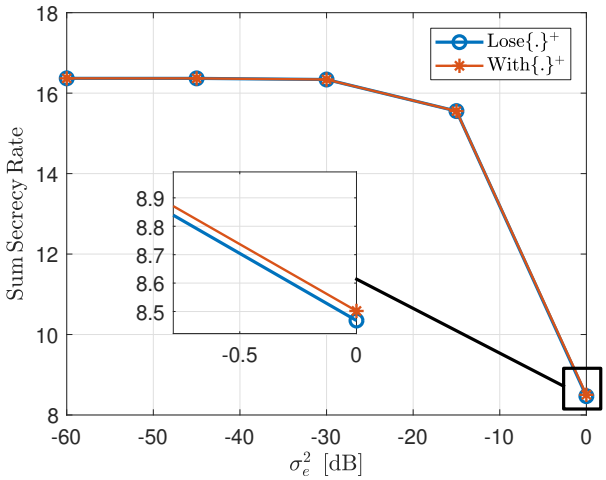

Figure 12. CSI error evaluation with the coding over all subcarriers and channels (Lose $\{.\}^+$) and the coding over each subcarrier, i.e., previous proposed method (With $\{.\}^+$).

corresponds to Bob, and an undesired receiver (an idle receiver, or a node belonging to another communication process) corresponds to Eve. The carrier frequency is 2.4 GHz with the bandwidth of 1 MHz. We adopt an indoor path loss model $20\log 2.4 + 30\log x + 46$ (dB) [47], where x in meters is the distance between the transmitter and receiver. Furthermore, all wireless channels experience Rayleigh fading with unit variance. The transmission power of each node is 20dBm, i.e., $X_{\max} = W_{\max} = 20$dBm. Nodes are placed symmetrically with distances of 10 meters. The noise power is -174 dBm/Hz. Moreover, we have $M_a = 4$, $M_{bt} = M_{at} = 4$, $M_e = 2$, $|\mathcal{N}| = 4$, $K_R = 10$, $\sigma^2_{\text{SI}} = -80$dB.

In Fig. 13 the performance of the proposed FD design, denoted as 'FD' in Fig. 13, is evaluated in terms of the sum secrecy rate. The following benchmarks are implemented to provide a meaningful comparison.

- 'HD': An HD system without FD jamming.
- 'Freq-Flat': A FD frequency-flat design where the same design is applied for all subcarriers.
- 'No-Distortion': A FD design without the awareness of distortion.
- 'ZF': The zero-forcing approach where the system achieves zero information rate to Eve by employing zero-forcing precoding.
- 'Rate-Max': The rate maximization approach which is described in (16), Subsection III-A2.
- 'Random-max': The maximal results of the random initializations which is described in Subsection V-A.
- 'Upper-Bound': The result of the ideal case where the perfect successive cancellation of self-interference is achieved, i.e., $\kappa = \beta = 0$.

It is observed from Fig. 13 that the proposed design outperforms the others in a large range of the transceiver distortion. A notable FD gain is observed with the high transceiver accuracy, i.e., low κ and β. Although the resulting sum secrecy rate of

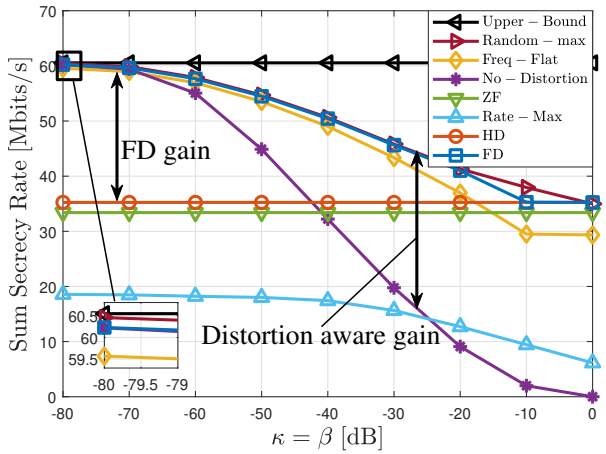

Figure 13. Performance evaluation in a practical scenario following the WiFi standard.

the proposed FD design converges to the result of the HD system with the increasing κ and β, the performance is still better than the zero-forcing and rate maximization approaches. Moreover, a significant distortion awareness gain is observed when κ and β are larger than -60dB. It indicates that the FD design without distortion awareness can be severely damaged by the high distortion level. Furthermore, the performance gain between the proposed design and the frequency-flat design shows the benefit from exploiting the frequency diversity of the channels. In addition, the results of 'Random-max' and 'FD' are very close to each other in a wide range of κ and β, which shows the robustness of the used uniform covariance with equal power allocation initialization method. Finally, the result of the proposed FD design at -80dB of κ and β is very close to the upper bound, which indicates that the level of -80dB of κ and β is adequate to achieve a good performance in the practical case.

VI. Conclusion

In this work, we have jointly investigated the power allocation problem and beam optimization problem for a multi-carrier and MIMOME wiretap channel in both single directional and bidirectional communication systems. The impact of FD jamming transceivers in the context of security enhancement is evaluated. It is observed that the transmission of an optimized jamming signal results in a notable enhancement of the sum secrecy capacity if the system is capable of high SI cancellation. In particular, for a system with high frequency selectivity the frequency diversity among all subcarriers is able to be exploited. By exploiting this frequency diversity both regarding the jamming and the desired information links, the achievable secrecy capacity is jointly enhanced. However, the numerical results show that the optimization of the jamming strategy is crucial as FD transceiver dynamic range decreases. Furthermore, a promising gain of sum secrecy rate is obtained from the FD-enabled bidirectional communication system, where the jamming signal can be used to improve security simultaneously for both directions.

References

[1] O. Taghizadeh, T. Yang, and R. Mathar, "Joint power and beam optimization in a multi-carrier MIMO wiretap channel with full-duplex jammer," in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2017, pp. 1316–1322.

[2] S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5g and beyond," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 114–121, February 2014.

[3] C. Pradhan and G. R. Murthy, "Full-duplex communication for future wireless networks: Dynamic resource block allocation approach," *Physical Communication*, vol. 19, pp. 61–69, 2016.

[4] D. Bharadia and S. Katti, "Full duplex MIMO radios," in *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*. Seattle, WA: USENIX Association, 2014, pp. 359–372.

[5] Y. Hua, P. Liang, Y. Ma, A. C. Cirik, and Q. Gao, "A method for broadband full-duplex mimo radio," *IEEE Signal Processing Letters*, vol. 19, no. 12, pp. 793–796, Dec 2012.

[6] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, ser. SIGCOMM '13. New York, NY, USA: ACM, 2013, pp. 375–386.

[7] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking*. ACM, 2010, pp. 1–12.

[8] M. Duarte and A. Sabharwal, "Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results," in *Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference on*. IEEE, 2010, pp. 1558–1562.

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

[10] N. M. Gowda and A. Sabharwal, "Jointnull: Combining reconfigurable analog cancellation with transmit beamforming for large-antenna full-duplex wireless," *IEEE Transactions on Wireless Communications*, no. 99, 2018.

[11] E. Everett, C. Shepard, L. Zhong, and A. Sabharwal, "Softnull: Many-antenna full-duplex wireless via digital beamforming," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8077–8092, 2016.

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

[13] 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.

[14] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO–OFDM systems by beamforming and artificial noise generation," *Physical Communication*, vol. 4, no. 4, pp. 313–321, 2011.

[15] M. Obeed and W. Mesbah, "Efficient algorithms for physical layer security in two-way relay systems," *Physical Communication*, vol. 28, pp. 78–88, 2018.

[16] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, Oct 2013.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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, no. 24, pp. 6391–6401, Dec 2014.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] D. P. Bertsekas, *Nonlinear programming*. Athena scientific Belmont, 1999.

[31] 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.

[32] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, Oct 2012.

[33] 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.

[34] M. Jain, J. I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '11. New York, NY, USA: ACM, 2011, pp. 301–312.

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

[36] O. Taghizadeh, V. Radhakrishnan, A. C. Cirik, R. Mathar, and L. Lampe, "Hardware impairments aware transceiver design for bidirectional full-duplex MIMO OFDM systems," *IEEE Transactions on Vehicular Technology*, pp. 1–1, 2018.

[37] K. B. Petersen and M. S. Pedersen, "The matrix cookbook," nov 2012, version 20121115.

[38] S. Boyd and L. Vandenberghe, *Convex Optimization*. New York, NY, USA: Cambridge University Press, 2004.

[39] 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.

[40] L. Vandenberghe, S. Boyd, and S.-P. Wu, "Determinant maximization with linear matrix inequality constraints," *SIAM J. Matrix Anal. Appl.*, vol. 19, no. 2, pp. 499–533, Apr. 1998.

[41] R. Hunger, *Floating point operations in matrix-vector calculus*. Munich University of Technology, Inst. for Circuit Theory and Signal Processing Munich, 2005.

[42] 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.

[43] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4599–4615, Aug 2014.

[44] M. Duarte, C. Dick, and A. Sabharwal, "Experiment-driven characterization of full-duplex wireless systems," *IEEE Transactions on Wireless Communications*, vol. 11, no. 12, pp. 4296–4307, December 2012.

[45] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.1," Mar. 2014.

[46] ——, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Springer-Verlag Limited, 2008, pp. 95–110.

[47] P. Series, "Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 mhz to 100 ghz," *Recommendation ITU-R*, pp. 1238–7, 2012.