Physical-Layer Security for Proximal Legitimate User and Eavesdropper: A Frequency Diverse Array Beamforming Approach

Jingran Lin, *Member, IEEE* Qiang Li, *Member, IEEE*, Jintai Yang, Huaizong Shao, *Member, IEEE*, and Wen-Qin Wang, *Senior Member, IEEE*

***Abstract*— Transmit beamforming and artificial noise-based methods have been widely employed to achieve physical-layer (PHY) security. However, these approaches may fail to provide satisfactory secure performance if the channels of legitimate user (LU) and eavesdropper (Eve) are highly correlated, which usually occurs in the case of close-located LU and Eve. The goal of this paper is to address the PHY security problem for proximal LU and Eve in millimeter-wave transmissions. To this end, we propose a novel frequency diverse array (FDA) beamforming approach, which intentionally introduces some frequency offsets across array antennas to decouple the highly correlated channels of LU and Eve. By exploiting this decoupling capability, the FDA beamforming can degrade Eve's reception and thus enhance PHY security. Leveraging FDA beamforming, we aim to maximize the secrecy rate by jointly optimizing the frequency offsets and the transmit beamformer. This secrecy rate maximization problem is difficult due to the tightly coupled variables. However, we show that it can be reformulated into a form only depending on the frequency offsets. Building upon this reformulation, we further employ the block successive upper-bound minimization method to iteratively obtain a solution with stationary convergence guarantee. Numerical results demonstrate that FDA beamforming can provide higher secrecy rate than conventional beamforming, especially for proximal LU and Eve.**

***Index Terms*— Physical-layer (PHY) security, frequency diverse array (FDA), beamforming, block successive upper-bound minimization (BSUM).**

I. Introduction

As an efficient method to secure wireless communications, the physical-layer (PHY) security technique has been intensively researched recently; see the recent survey paper [1] and the references therein. PHY security is an information theoretic approach to achieving some confidentiality at the PHY without upper-layer encryptions [2]. One key performance measure of PHY security is the secrecy rate, at which the information can be confidentially transmitted. Generally, the secrecy rate is characterized by the channel capacity difference between the legitimate user (LU) and the eavesdropper (Eve). Popular PHY security approaches include transmit beamforming [3]–[8] and artificial-noise (AN)-aided designs [7]–[13], which explore certain channel statistical independence to either enhance LU's reception or jam Eve's reception. However, these approaches may fail to provide satisfactory secrecy performance if the independence assumption does not hold. For instance, recently there is an increasing attention in utilizing millimeter-wave (mmWave) bands for next generation wireless networks [14]. One important feature of mmWave communication is the highly directional transmission, especially in line-of-sight (LOS) scenarios [15]. If LUs and Eves are well separated in transmit direction, PHY security can be achieved easily since the Eve's channel has a low probability of falling into the subspace spanned by the LU's [16]. However, in the case of proximal LU and Eve, highly correlated channels may result. Therefore, transmit beamforming and/or AN-aided schemes suffer from severe performance degradation.

To achieve PHY security for proximal LU and Eve, transmit schemes that can discriminate receivers with highly correlated channels should be sought. Frequency diverse array (FDA) [17], [18] is a potential solution to this problem. Basically, FDA employs small frequency offsets across the array to yield distinct accumulating phase lags among array antennas, thus helping decouple the channels of LU and Eve. By exploiting this capability, the received signal levels of proximal LU and Eve can be differentiated.

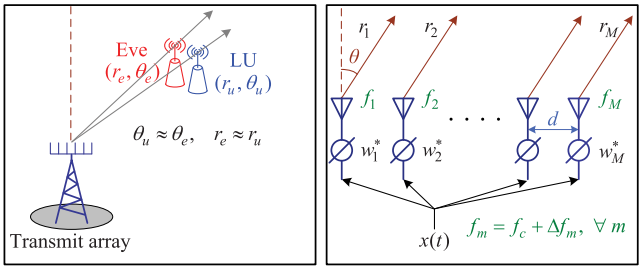
Current studies on FDA mainly focus on analyzing the FDA range-dependent beampattern characteristics, and exploring its application in radar and navigation systems [19]–[23]. Departing from the existing research, we propose to employ the FDA technique to achieve PHY security for proximal LU and Eve in highly directional transmissions. In particular, as shown in Fig. 1(a), we consider an LOS mmWave communication system, where a single-antenna LU receives confidential information from a multi-antenna transmit array, with a single-antenna Eve located very close to the LU. For simplicity, we ignore the very few multi-path components (MPCs) in mmWave transmission, and hence the LOS channel reduces to a directional channel. This is acceptable in LOS mmWave

Manuscript received January 24, 2017; revised May 22, 2017, August 6, 2017, and September 17, 2017; accepted October 10, 2017. Date of publication October 23, 2017; date of current version December 19, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61671120, Grant 61401073, and Grant 61471103 and in part by the Fundamental Research Funds for the Central Universities under Grant ZYGX2016J007 and Grant ZYGX2016J011. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Eduard A. Jorswieck. *(Corresponding author: Jingran Lin.)*

The authors are with the School of Communication and Information Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: jingranlin@uestc.edu.cn; lq@uestc.edu.cn; j.t.yang@std.uestc.edu.cn; hzshao@uestc.edu.cn; wqwang@uestc.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2017.2765500



(a) (b)

Fig. 1. FDA beamforming for PHY security with proximal LU and Eve. (a) Proximal LU and Eve. (b) FDA beamforming.

communications since the MPCs have been found to be attenuated by 20dB compared to the LOS component [14]. In such circumstance, the Eve channel is highly correlated with the LU's, thereby defeating the commonly used PHY secrecy approaches, e.g., beamforming and AN-based designs. To handle such a PHY security problem, we propose to employ the FDA's channel-decoupling capability to enhance LU's reception and degrade Eve's. In addition, to maximally explore the array's potential, we further integrate beamforming into FDA and finally develop a novel *FDA beamforming* approach to addressing the PHY security problem for proximal LU and Eve.

By leveraging FDA beamforming, we aim to maximize the secrecy rate by judiciously designing the FDA beamforming parameters — the frequency offsets across the antennas and the transmit beamformer. The secrecy rate maximization (SRM) problem is challenging due to the nonconcave objective and the tightly coupled frequency-offset variables and beamforming variables. To handle this SRM problem, we first explore the SRM problem structure to obtain some insights into the FDA beamforming design. Specifically, we found that in FDA beamforming, the frequency offsets essentially play a role of changing the phase lags among different array antennas. As a consequence, the channels of proximal LU and Eve may be decoupled, and hence the conventional secrecy beamforming approaches can be employed. In view of this, we develop a two-stage algorithm for the SRM problem. In the first stage, we aim to maximally decouple the channels of LU and Eve by optimizing the frequency offsets across the array antennas; next, in the second stage, the transmit beamformer is optimized based on the given frequency offsets. Since the second stage is the same as the conventional secrecy beamformer design, the main difficulty lies in the frequency offsets optimization. We propose an algorithm based on the block successive upper-bound minimization (BSUM) method [24] to iteratively find a stationary solution of the frequency offsets. Since each BSUM iteration admits a closed-form solution, the proposed two-stage algorithm has very low complexity.

A. Related Works

There are several related works on FDA-based secure communication that are worth mentioning. In [25], the authors design an orthogonal frequency-division multiplexing (OFDM) secure transmitter, utilizing FDA with some fixed frequency offsets. An AN-based FDA secure communication scheme is proposed in [26], where the frequency offset of each antenna is randomly chosen from a given set with linearly increasing frequency offsets, and then the ergodic secrecy capacity (ESC) is maximized via optimizing the transmission power allocation between the useful signal and AN. Actually, our work differs from [25] and [26] in both problem formulation and algorithm design. Firstly, without the help of AN, the proposed method optimizes the transmit beamformer to improve PHY security, while [26] employs fixed beamformer. Secondly, it provides a general FDA-based solution to the PHY security problem with proximal LU and Eve, which is not limited to the OFDM technique. Last but not least, we optimize the frequency offsets in the FDA beamforming design, while in [25] and [26], the frequency offsets are both known (although the frequency offsets are randomly chosen from a set in [26], the elements of the set are known and fixed). Consequently, the proposed FDA beamforming formulation and the solution approach are completely different from those in [25] and [26].

B. Organization and Notations

The rest of this paper is organized as follows. The system model and problem statement are described in Section II. In Section III, we first provide some insights into the solution of the SRM problem; then, we develop a two-stage algorithm to solve the problem. In Section IV, we extend our approach to the cases of imperfect Eve channel state information (CSI) and multi-antenna Eve. In Section V, several numerical simulations are provided to demonstrate efficacy of the proposed approach. Finally, we conclude this paper in Section VI.

Notations: Boldface uppercase and lowercase letters denote matrices and vectors, respectively. Italic letters denote scalars. For some given matrix $\mathbf{A}$, we denote its transpose, Hermitian, and inverse by $\mathbf{A}^T$, $\mathbf{A}^\dagger$, and $\mathbf{A}^{-1}$, respectively. Similarly, we denote the transpose and Hermitian of a vector $\mathbf{x}$ by $\mathbf{x}^T$ and $\mathbf{x}^\dagger$. Denote $\|\cdot\|_2$ as ℓ_2-norm. Use $\mathbb{R}^{M\times N}$ and $\mathbb{C}^{M\times N}$ to indicate the real and complex $M \times N$ matrices.

II. System Model and Problem Statement

A. Frequency Diverse Array

As shown in Fig. 1(a), here we consider an LOS mmWave communication system that consists of an M-antenna uniform linear array, a single-antenna LU, and a single-antenna Eve. The array forwards confidential information to the LU, in the presence of a close-located Eve overhearing the transmission. To achieve confidentiality, we employ the FDA beamforming approach to provide PHY security. As opposed to the conventional phase array, FDA introduces some small frequency offsets across the array antennas. As shown in Fig. 1(b), the radiation frequency of the mth antenna is $f_m = f_c + \Delta f_m$ for $m = 1, 2, \ldots, M$, with f_c and Δf_m being the carrier frequency and the frequency offsets, respectively. We assume $0 \le \Delta f_m \le \Delta F$ and $\Delta F \ll f_c$ in this paper. Let d denote the uniform antenna spacing of the transmit array, which is set as $d = c/[2(f_c + \Delta F)] \simeq c/(2f_c)$ to avoid aliasing effects with c being the speed of light.

Without loss of generality, we define the first antenna as the origin of the $(range, angle)$ coordinate system. Moreover, to concentrate on the SRM problem for proximal LU and Eve, we ignore the very few multi-path components (MPCs) in LOS mmWave transmission, since they were found to be attenuated by 20dB compared to the LOS component [14]. Thus, for the user at (r, θ), the LOS channel associated with the mth antenna is given by [19], [25], [26]

$$h_m(f_m, r, \theta, t) = a(r)e^{-j2\pi(f_c+\Delta f_m)\left[t-\frac{r-(m-1)d\sin\theta}{c}\right]}, \quad (1)$$

where $a(r)$ is the signal attenuation factor at the range of r. Notice that we have assumed far-field model in order to obtain $h_m(f_m, r, \theta, t)$, i.e., parallel wavefront and $a(r_m) \simeq a(r)$. For mmWave array transmission, the far-field and LOS assumptions can hold simultaneously due to the tiny array size, usually in magnitude of millimeters.

To focus on the FDA characteristics, we temporarily ignore the attenuation factor $a(r)$ and assume an all-one beamformer. Then, the FDA beampattern at (r, θ) is computed as

$$\begin{aligned}
&\mathrm{B}(\mathbf{f}, r, \theta, t) \\
&= \sum_{m=1}^{M} h_m(f_m, r, \theta, t) \\
&= e^{-j2\pi f_c(t-\frac{r}{c})} \sum_{m=1}^{M} e^{-j2\pi\left\{f_c\frac{(m-1)d\sin\theta}{c}+\Delta f_m\left[t-\frac{r-(m-1)d\sin\theta}{c}\right]\right\}} \\
&= e^{-j2\pi f_c(t-\frac{r}{c})} \sum_{m=1}^{M} e^{j[\Phi_{0,m}(\theta)+\Phi_{1,m}(\Delta f_m, r, \theta, t)]} \qquad (2)
\end{aligned}$$

where $\Phi_{0,m}(\theta) = -2\pi f_c\frac{(m-1)d\sin\theta}{c}$, $\Phi_{1,m}(\Delta f_m, r, \theta, t) = -2\pi\Delta f_m[t - \frac{r-(m-1)d\sin\theta}{c}]$, $\forall m$, and $\mathbf{f} = [f_1, f_2, \ldots, f_M]^T \in \mathbb{R}^{M\times 1}$.

Obviously, the phase terms $\{\Phi_{1,m}(\Delta f_m, r, \theta, t)\}_{m=1}^{M}$ in (2) depend on the frequency offsets $\{\Delta f_m\}_{m=1}^{M}$, the range r, the angle θ, and the time t. By choosing $\{\Delta f_m\}_{m=1}^{M}$ appropriately, FDA can generate some "*S-shape*" beampattern owing to the distinct accumulating phase lags among different antennas. To show this, we display the typical beampatterns of conventional phase array and FDA in Fig. 2. For the sake of simplicity, we have assumed $t = 0$ and linearly increasing frequency offsets in FDA, i.e., $\Delta f_m = (m-1)\Delta f$, $\forall m$. In the case of $\Delta f = 0$, we have $\Phi_{1,m}(\Delta f_m, r, \theta, t) = 0$, $\forall m$, and then FDA reduces to conventional phase array as shown in Fig. 2(a). The array cannot differentiate the proximal LU and Eve (e.g., $\theta_e \simeq \theta_u$) due to the highly correlated channels. Then, the conventional PHY security approaches, such as transmit beamforming and AN-aided design, fail to provide PHY security. As a contrast, we set $\Delta f = 1.5$KHz, $t = 0$ in Fig. 2(b), and hence an "*S-shape*" beampattern is activated due to the nonzero phase terms $\{\Phi_{1,m}(\Delta f_m, r, \theta, t)\}_{m=1}^{M}$. Intuitively speaking, the frequency offsets yield distinct accumulating phase lags among antennas and thus help decouple the channels of proximal LU and Eve. In the FDA "*S-shape*" beampattern, LU and Eve are separated well, making it possible to provide PHY security.

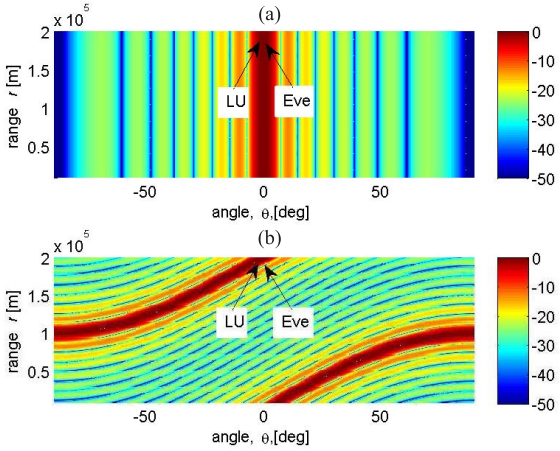


Fig. 2. Typical beampatterns, i.e., $|\mathrm{B}(\mathbf{f}, r, \theta)|$, of phase array and FDA for $M = 16$, $f_c = 60$GHz, $\Delta f = 1.5$KHz, and $t = 0$. (a) Phase array beampattern ($\Delta f = 0$). (b) FDA beampattern ($\Delta f \neq 0$).

B. Problem Statement

We see from (2) that FDA has a deterministic beampattern for some given $\mathbf{f}$ and t. In general, there is no guarantee that the LU and Eve are located at the beampattern peak and valley simultaneously. Thus, we need to choose the frequency offsets appropriately. To maximally explore the array's potentials in achieving PHY security, we further integrate beamforming into FDA, yielding a novel FDA beamforming strategy.

We should mention that since the channel and beampattern of FDA depend on time t, the solution to FDA beamforming, e.g., the transmit beamformer, is also time-varying.

Define $\mathbf{w}(t) \triangleq [w_1(t), w_2(t), \ldots, w_M(t)]^T \in \mathbb{C}^{M\times 1}$ as the array transmit beamformer at time instant t. The channel vector between the array and the receiver at (r, θ) is $\mathbf{h}(\mathbf{f}, r, \theta, t) \triangleq [h_1(f_1, r, \theta, t), h_2(f_2, r, \theta, t), \ldots, h_M(f_M, r, \theta, t)]^T \in \mathbb{C}^{M\times 1}$. Since the signal emitted at time instant t arrives at the receiver after a time period of $\frac{r}{c}$, the instantaneous signal-to-noise ratio (SNR) for the signal emitted at time t is computed as

$$\mathrm{SNR}(t) = \sigma^{-2}|\mathbf{w}^{\dagger}(t)\mathbf{h}(\mathbf{f}, r, \theta, t + \tfrac{r}{c})|^2, \quad (3)$$

where σ^2 is the noise power at receiver.

Define (r_u, θ_u) and (r_e, θ_e) as the coordinates of the proximal LU and Eve, respectively. To simplify the notations, we use $\mathbf{h}_u(\mathbf{f}, t)$ and $\mathbf{h}_e(\mathbf{f}, t)$ to denote the associated channels when the signal emitted at time t arrives at LU and Eve; i.e., $\mathbf{h}_u(\mathbf{f}, t) \triangleq \mathbf{h}(\mathbf{f}, r_u, \theta_u, t + \frac{r_u}{c})$ and $\mathbf{h}_e(\mathbf{f}, t) \triangleq \mathbf{h}(\mathbf{f}, r_e, \theta_e, t + \frac{r_e}{c})$. The instantaneous achievable rates at LU and Eve for the signal emitted at time instant t are given by

$$R_u(t) = \log(1 + \sigma_u^{-2}|\mathbf{w}^{\dagger}(t)\mathbf{h}_u(\mathbf{f}, t)|^2), \quad (4)$$

$$R_e(t) = \log(1 + \sigma_e^{-2}|\mathbf{w}^{\dagger}(t)\mathbf{h}_e(\mathbf{f}, t)|^2), \quad (5)$$

where σ_u^2 and σ_e^2 denote the noise powers at LU and Eve, respectively. The instantaneous SRM problem based on FDA

beamforming is then formulated as[1]

$$\max_{\{\mathbf{f},\mathbf{w}(t)\}} \; R_s(t) \triangleq R_u(t) - R_e(t) \tag{P1}$$

$$\text{s.t. } |\mathbf{w}(t)\|_2^2 \le P, \tag{6}$$

$$f_c \le f_m \le f_c + \Delta F, \quad \forall m, \tag{7}$$

where P is the transmit power budget.

In brief, our target is to achieve PHY security for proximal LU and Eve. To this end, we employ the FDA beamforming strategy to maximize the secrecy rate by appropriately selecting the frequency offsets and the transmit beamformer.

III. A Two-Stage Algorithm for SRM Problem

The SRM problem (P1) is challenging due to the nonconcave objective and the tightly coupled variables $\mathbf{f}$ and $\mathbf{w}(t)$. In this section, we first provide some insights into the solution of (P1). By leveraging these insights, we then develop a low-complexity two-stage algorithm to (P1).

A. Some Insights to the Solution of (P1)

In order to gain some insights into why FDA can provide PHY security, even for proximal LU and Eve, let us first fix the frequency $\mathbf{f}$ and briefly review the classical PHY secrecy beamforming design [27]–[29]. Clearly, for fixed $\mathbf{f}$ in (P1), the SRM problem is the same as the classical multi-input, single-output, single-eavesdropper (MISOSE) secrecy design problem in [27], and the optimal beamformer can be obtained via generalized eigendecomposition [30]. In particular,

Lemma 1 [27]: Given $\mathbf{f}$ *in* (P1)*, let us denote*

$$\mathbf{H}_u(\mathbf{f},t) = \tilde{\mathbf{h}}_u(\mathbf{f},t)\tilde{\mathbf{h}}_u^{\dagger}(\mathbf{f},t), \quad \tilde{\mathbf{h}}_u(\mathbf{f},t) = \sigma_u^{-1}\mathbf{h}_u(\mathbf{f},t), \tag{8}$$

$$\mathbf{H}_e(\mathbf{f},t) = \tilde{\mathbf{h}}_e(\mathbf{f},t)\tilde{\mathbf{h}}_e^{\dagger}(\mathbf{f},t), \quad \tilde{\mathbf{h}}_e(\mathbf{f},t) = \sigma_e^{-1}\mathbf{h}_e(\mathbf{f},t), \tag{9}$$

$$\tilde{\mathbf{H}}_e(\mathbf{f},t) = \mathbf{H}_e(\mathbf{f},t) + \tfrac{1}{P}\mathbf{I}, \tag{10}$$

$$\mathbf{\Sigma}(\mathbf{f},t) = \tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f},t)[\mathbf{H}_u(\mathbf{f},t) - \mathbf{H}_e(\mathbf{f},t)]\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f},t). \tag{11}$$

Then, the optimal secrecy rate in (P1) *is given by*

$$R_s^{\star}(t;\mathbf{f}) = \log(1 + [\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)]^+), \tag{12}$$

where $[\,\cdot\,]^+ \triangleq \max\{\cdot, 0\}$*, and* $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$ *is the principal eigenvalue of* $\mathbf{\Sigma}(\mathbf{f},t)$*. Moreover, the optimal beamformer* $\mathbf{w}^{\star}(t;\mathbf{f})$ *is given by,*

$$\mathbf{w}^{\star}(t;\mathbf{f}) = \text{sgn}\{\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)\} \cdot \frac{\sqrt{P}\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f},t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f},t)}{\|\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f},t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f},t)\|_2}, \tag{13}$$

where sgn$\{\cdot\}$ *returns* 1 *for positive argument, and* 0 *otherwise;* $\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f},t)$ *is the principal eigenvector of* $\mathbf{\Sigma}(\mathbf{f},t)$.

We should mention that the secrecy rate expression in (12) slightly differs from the original form in [27]. Since (12) serves our purpose better in the subsequent development, we use (12) and provide a brief proof of Lemma 1 in Appendix A for self-containedness.

[1]Notice that $R_s(t)$ is related to $\mathbf{h}_u(\mathbf{f},t)$ and $\mathbf{h}_e(\mathbf{f},t)$, and thus varies with time. In this case, it is more reasonable to consider an average SRM problem (cf. (P6) in Sec. III-C). Actually, our final target in this work is to maximize the average secrecy rate. The reason why we consider the instantaneous SRM problem (P1) here is that the average SRM problem (P6) can be equivalently handled by solving (P1). We will elaborate more on this in Sec. III.

From (12), we know that the optimal secrecy rate depends on the principal eigenvalue of $\mathbf{\Sigma}(\mathbf{f},t)$. Let us assume $\Delta f_m = 0, \forall m$; i.e., the case of conventional phase array beamforming. For the proximal LU and Eve in Fig. 1(a), e.g., $\theta_u \simeq \theta_e$ and $r_u \simeq r_e$, $\mathbf{h}_e(\mathbf{f},t)$ and $\mathbf{h}_u(\mathbf{f},t)$ are not only highly correlated, but also have similar strength. In consequence, we have very small $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$, and then the conventional beamforming suffers from severe performance degradation.

However, by introducing frequency offset Δf_m across the antennas, the LU and Eve channels are decoupled (cf. Eq. (1) and Fig. 2(b)). Then, larger $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$ and higher secrecy rate may be achieved. Intuitively, the frequency offsets in FDA play a role of changing the phase lags among antennas, and thus the highly-correlated channels of LU and Eve can be decoupled. This key observation not only explains why FDA is capable to provide PHY security even for proximal LU and Eve, it also sheds some lights on how to design the frequency offsets.

According to Lemma 1 and the previous discussion, we see that (P1) boils down to finding the optimal frequency offsets, such that the principal eigenvalue $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$ is maximized, i.e.,

$$\max_{\mathbf{f}} \; \lambda_{\mathbf{\Sigma}}(\mathbf{f},t) \tag{P2}$$

$$\text{s.t. } f_c \le f_m \le f_c + \Delta F, \quad \forall m.$$

After the optimal $\mathbf{f}^{\star}$ for (P2) is found, the optimal beamformer $\mathbf{w}^{\star}(t;\mathbf{f}^{\star})$ can be computed in closed form using (13). Therefore, in the subsequent development we focus on solving (P2).

Problem (P2) can be recast into a more amenable form by carefully inspecting the structure of matrix $\mathbf{\Sigma}(\mathbf{f},t)$. Actually, the following result gives a more straightforward way to find the optimal frequency offsets for (P2).

Lemma 2: Problem (P2) *is equivalent to the following problem*

$$\min_{\mathbf{f}} \; |\langle \mathbf{h}_e(\mathbf{f},t),\ \mathbf{h}_u(\mathbf{f},t)\rangle|^2 \tag{P3}$$

$$\text{s.t. } f_c \le f_m \le f_c + \Delta F, \quad \forall m,$$

where $\langle\cdot,\cdot\rangle$ *denotes the inner product. Moreover, the optimal frequency offsets and the maximum principal eigenvalue in* (P2) *are both time independent.*

Proof: See Appendix B. ■

Physically, Lemma 2 reveals two interesting facts. Firstly, since the objective of (P3), i.e., $\langle \mathbf{h}_e(\mathbf{f},t),\ \mathbf{h}_u(\mathbf{f},t)\rangle$, is independent of time t (cf. Eq. (14) and Appendix B), the optimal frequency offsets as well as the maximum secrecy rate keeps constant and does not change with time. This fact helps extend the solution approach of the instantaneous SRM problem (P1) to maximize the average secrecy rate over a given time period.

Secondly, the frequency offsets should be appropriately chosen to turn the channels of LU and Eve as orthogonal as possible, such that the two channels can be maximally decoupled. In the ideal case, we have $\langle \mathbf{h}_e(\mathbf{f},t),\ \mathbf{h}_u(\mathbf{f},t)\rangle = 0$. Unfortunately, owing to the limited dynamic range of frequency offsets, it is generally impossible to make $\mathbf{h}_e(\mathbf{f},t)$ and $\mathbf{h}_u(\mathbf{f},t)$ exactly orthogonal; i.e., the channels of proximal LU and Eve cannot be decoupled completely. Since (P3) is difficult due to the nonconvex objective and tightly coupled variables, we pursue some suboptimal solutions with manageable complexity. In particular, we develop an iterative

algorithm based on BSUM to find a solution with stationary convergence guarantee. Each BSUM iteration admits a closed-form solution, thus giving the algorithm very low complexity.

B. A BSUM Approach to (P3)

According to the FDA channel definition in (1), the inner product of $\mathbf{h}_u(\mathbf{f},t)$ and $\mathbf{h}_e(\mathbf{f},t)$ is given by

$$\begin{aligned}\langle \mathbf{h}_e(\mathbf{f},t),\, \mathbf{h}_u(\mathbf{f},t)\rangle &= \mathbf{h}_e^{\dagger}(\mathbf{f},t)\mathbf{h}_u(\mathbf{f},t)\\ &= a(r_e)a(r_u)\sum_{m=1}^{M} e^{j2\pi f_m \frac{(m-1)d(\sin\theta_e-\sin\theta_u)}{c}}\\ &= a(r_e)a(r_u)\sum_{m=1}^{M} e^{j2\pi f_m \tau_m}, \end{aligned} \tag{14}$$

with $\tau_m = \frac{(m-1)d(\sin\theta_e-\sin\theta_u)}{c}$. Thus, $|\langle \mathbf{h}_e(\mathbf{f},t),\, \mathbf{h}_u(\mathbf{f},t)\rangle|^2$ is expressed as

$$\begin{aligned}&|\langle \mathbf{h}_e(\mathbf{f},t),\, \mathbf{h}_u(\mathbf{f},t)\rangle|^2\\ &= a^2(r_u)a^2(r_e)\left|\sum_{m=1}^{M} e^{j2\pi f_m\tau_m}\right|^2\\ &= a^2(r_u)a^2(r_e)\sum_{m=1}^{M}\sum_{n=1}^{M} e^{j2\pi(f_m\tau_m - f_n\tau_n)}\\ &= a^2(r_u)a^2(r_e)\left\{M + \sum_{m=1}^{M}\sum_{\substack{n=1\\ n\neq m}}^{M}\cos\left[2\pi(f_m\tau_m - f_n\tau_n)\right]\right\}\end{aligned} \tag{15}$$

and then (P3) can be equivalently expressed as

$$\begin{aligned}\min_{\mathbf{f}}\ & \sum_{m=1}^{M}\sum_{\substack{n=1\\ n\neq m}}^{M}\cos\left[2\pi(f_m\tau_m - f_n\tau_n)\right] \qquad \text{(P4)}\\ \text{s.t. }& f_c \le f_m \le f_c + \Delta F, \quad \forall m.\end{aligned}$$

To solve (P4), we resort to the block successive upper-bound minimization (BSUM) method [24]. The BSUM algorithm is a very general framework that can handle a general nonconvex nonsmooth problem with multiple block variables. Since our proposed method relies heavily on BSUM, let us first give a brief review of the BSUM method.

1) A Brief Review of the BSUM Method: Consider the following minimization problem,

$$\begin{aligned}\min_{\mathbf{x}}\ & y(x_1, x_2, \ldots, x_I)\\ \text{s.t. }& x_i \in \mathcal{X}_i, \quad i = 1, 2, \ldots, I,\end{aligned}$$

where $\mathbf{x} = [x_1, x_2, \ldots, x_I]^T \in \mathbb{R}^{I\times 1}$; $\mathcal{X}_i \subseteq \mathbb{R}$ is a closed convex set; $y(\cdot) : \prod_{i=1}^{I}\mathcal{X}_i = \mathcal{X} \to \mathbb{R}$ is a continuous function. A popular approach for solving the above problem is the block coordinate descent (BCD) method [31]. At each iteration of BCD, the function is minimized with respect to a single block while the rest blocks are held fixed. More specifically, in the sth iteration, we update $\mathbf{x}$ as follows

$$\begin{cases} x_i^s = \operatorname{argmin}_{x_i\in\mathcal{X}_i}\ y_i(x_i; \mathbf{x}_{-i}^{s-1})\\ x_l^s = x_l^{s-1},\ \forall\, l \neq i,\end{cases}$$

where $\mathbf{x}_{-i}^{s-1} \triangleq [x_1^{s-1}, \ldots, x_{i-1}^{s-1}, x_{i+1}^{s-1}, \ldots, x_I^{s-1}]^T \in \mathbb{R}^{(I-1)\times 1}$ is the remaining variables in $\mathbf{x}^{s-1}$ after removing x_i^{s-1}, and $y_i(x_i; \mathbf{x}_{-i}^{s-1}) \triangleq y(x_1^{s-1}, \ldots, x_{i-1}^{s-1}, x_i, x_{i+1}^{s-1}, \ldots, x_I^{s-1})$.

However, solving the subproblem may not be easy in the case of nonconvex $y_i(x_i; \mathbf{x}_{-i}^{s-1})$. To circumvent this difficulty, the BSUM method proposes to approximate $y_i(x_i; \mathbf{x}_{-i}^{s-1})$ by $u_i(x_i; \mathbf{x}^{s-1}) \triangleq u_i(x_i; x_1^{s-1}, x_2^{s-1}, \ldots, x_I^{s-1})$, which satisfies

$$\begin{cases} u_i(x_i^{s-1}; \mathbf{x}^{s-1}) = y_i(x_i^{s-1}; \mathbf{x}_{-i}^{s-1}),\\ u_i'(x_i^{s-1}; \mathbf{x}^{s-1}) = y_i'(x_i^{s-1}; \mathbf{x}_{-i}^{s-1}),\\ u_i(x_i; \mathbf{x}^{s-1}) \ge y_i(x_i; \mathbf{x}_{-i}^{s-1}),\\ u_i(x_i; \mathbf{x}^{s-1}) \text{ is continuous,}\end{cases} \tag{16}$$

and then updates x_i as

$$\begin{cases} x_i^s = \operatorname{argmin}_{x_i\in\mathcal{X}_i}\ u_i(x_i; \mathbf{x}^{s-1}),\\ x_l^s = x_l^{s-1},\ \forall\, l \neq i.\end{cases}$$

The convergence of BSUM is summarized below.

Theorem 1 [24, Th. 2]: Suppose that: (i) the BSUM assumption (16) *holds; (ii) the function $u_i(x_i; \mathbf{x}^{s-1})$ is quasi-convex in x_i; (iii) the subproblem in each iteration has a unique solution for any point $\mathbf{x}^{s-1} \in \mathcal{X}$; (iv) the function $y(\cdot)$ is regular*[2] *at every point in the set of stationary points. Then, every limit point of the iterates generated by the BSUM algorithm is a stationary point.*

Next, we show how the BSUM method can be invoked to handle (P4).

2) The BSUM Algorithm for (P4): Without loss of generality, let us consider the update of f_m in the sth iteration by solving the following problem

$$\begin{aligned}\min_{f_m}\ & \sum_{\substack{n=1\\ n\neq m}}^{M}\cos[2\pi(f_m\tau_m - f_n^{s-1}\tau_n)] \qquad \text{(P5)}\\ \text{s.t. }& f_c \le f_m \le f_c + \Delta F. \qquad (17)\end{aligned}$$

Following the BSUM framework, we propose to approximate the nonconvex objective in (P5) by some convex quadratic function. For ease of exposition, let us define the objective in (P5) as

$$y_m(f_m; \mathbf{f}_{-m}^{s-1}) \triangleq \sum_{n=1}^{M}\tilde{y}_{m,n}(f_m; f_n^{s-1}) \tag{18}$$

$$\tilde{y}_{m,n}(f_m; f_n^{s-1}) \triangleq \begin{cases}\cos[2\pi(f_m\tau_m - f_n^{s-1}\tau_n)],\ n\neq m,\\ 0,\ n = m,\end{cases} \tag{19}$$

and then approximate $y_m(f_m; \mathbf{f}_{-m}^{s-1})$ with the convex quadratic function $u_m(f_m; \mathbf{f}^{s-1})$, i.e.,

$$u_m(f_m; \mathbf{f}^{s-1}) \triangleq \sum_{n=1}^{M}\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}), \tag{20}$$

$$\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \triangleq \begin{cases}\kappa_{m,n}(f_m - \zeta_{m,n})^2 + \delta_{m,n},\ n\neq m,\\ 0,\ n = m,\end{cases} \tag{21}$$

[2]If $y(\cdot)$ is smooth, then it is regular automatically.

TABLE I

ALGORITHM 1 FOR FREQUENCY OFFSETTING PROBLEM (P4)

Find a feasible point $\mathbf{f}^0$ and set $s=0$;
repeat
$s=s+1,\ m=(s \bmod M)+1$;
Determine $\{\kappa_{m,n},\zeta_{m,n},\delta_{m,n}\}_{n=1}^{M}$ by (24) and (25);
$f_m^s=\left[\frac{\sum_{n=1}^{M}\kappa_{m,n}\zeta_{m,n}}{\sum_{n=1}^{M}\kappa_{m,n}}\right]_{f_c}^{f_c+\Delta F}$;
$f_n^s=f_n^{s-1},\ \forall\, n\neq m$;
until some stopping criterion is satisfied.

where $\kappa_{m,n}\in\mathbb{R}_+$, $\zeta_{m,n}\in\mathbb{R}$ and $\delta_{m,n}\in\mathbb{R}$, $n\neq m$, are parameters needed to be designed; we will elaborate on this shortly.

Therefore, (P5) is replaced by

$$\min_{f_m}\ \sum_{n=1}^{M}\left[\kappa_{m,n}(f_m-\zeta_{m,n})^2+\delta_{m,n}\right]$$
$$\text{s.t. } f_c\le f_m\le f_c+\Delta F.$$

It is easy to see that the optimal solution of the above problem is given by

$$f_m^s=\left[\frac{\sum_{n=1}^{M}\kappa_{m,n}\zeta_{m,n}}{\sum_{n=1}^{M}\kappa_{m,n}}\right]_{f_c}^{f_c+\Delta F} \tag{22}$$

where $[\cdot]_{f_c}^{f_c+\Delta F}$ denotes the projection onto $[f_c, f_c+\Delta F]$. Algorithm 1 in Table I summarizes the whole procedure to solve (P4), and the convergence of Algorithm 1 is established as follows.

Proposition 1: Every limit point of the iterates generated by Algorithm 1 is a stationary solution of (P4).

The key step in the proof of proposition 1 is to show that the convergence conditions required by BSUM (cf. Theorem 1) are satisfied by Algorithm 1. The detailed proof is relegated to Appendix C. We should also point it out that the stationary convergence is generally not guaranteed if one directly applies BCD method to (P4). This is because convergence of the BCD methods typically requires the uniqueness of the minimizer at each step or the quasi-convexity of the objective function [31]. However, this is not true since $y_m(f_m;\mathbf{f}_{-m}^{s-1})$ may have multiple minimizers or be nonconvex within the range of $f_m\in[f_c, f_c+\Delta F]$.

Now, let us turn back to the design of the BSUM parameters of $\{\kappa_{m,n},\zeta_{m,n},\delta_{m,n}\}$ such that the BSUM assumption (16) is satisfied. Specifically, as shown in Fig. 3, we require that

$$\begin{cases}\tilde{u}_{m,n}(f_m^{s-1};f_m^{s-1},f_n^{s-1})=\tilde{y}_{m,n}(f_m^{s-1};f_n^{s-1})\\ \tilde{u}'_{m,n}(f_m^{s-1};f_m^{s-1},f_n^{s-1})=\tilde{y}'_{m,n}(f_m^{s-1};f_n^{s-1})\\ \tilde{y}_{m,n}(\zeta_{m,n};f_n^{s-1})\le\tilde{y}_{m,n}(f_m^{s-1};f_n^{s-1})\\ \tilde{y}_{m,n}(\zeta_{m,n};f_n^{s-1})\in\{1,-1\},|\zeta_{m,n}-f_m^{s-1}|<\dfrac{1}{2|\tau_m|}\end{cases} \tag{23}$$

and thus solve $\{\kappa_{m,n},\zeta_{m,n},\delta_{m,n}\}$ based on (23) and the sign of $y'_{m,n}(f_m;f_n^{s-1})$ at f_m^{s-1}, i.e,

$$\tilde{y}'_{m,n}(f_m^{s-1};f_n^{s-1})=-2\pi\tau_m\sin[2\pi(f_m^{s-1}\tau_m-f_n^{s-1}\tau_n)].$$

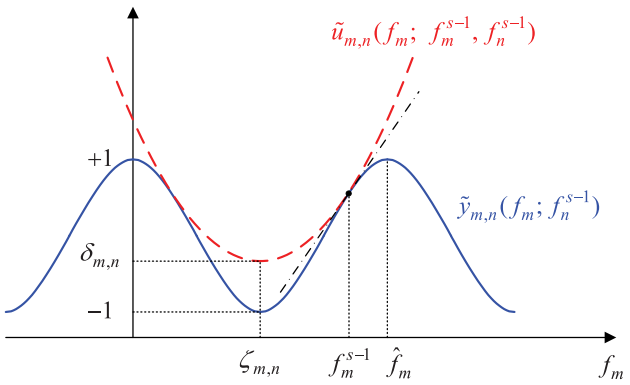


Fig. 3. Approximating the cos(·) function by a convex quadratic function.

TABLE II

TWO-STAGE ALGORITHM FOR INSTANTANEOUS SRM PROBLEM

Initialize the system parameters
[Stage 1] Optimize the frequency offsets
Call Algorithm 1 and output $f_m^\star,\ \forall m$;
[Stage 2] Optimize the beamformer
$\mathbf{w}^\star(t;\mathbf{f}^\star)=\mathrm{sgn}\{\lambda_{\mathbf{\Sigma}}(\mathbf{f}^\star,t)\}\frac{\sqrt{P}\tilde{\mathbf{H}}_e^{-1/2}(\mathbf{f}^\star,t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f}^\star,t)}{\|\tilde{\mathbf{H}}_e^{-1/2}(\mathbf{f}^\star,t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f}^\star,t)\|_2}$,
Output the secrecy rate $R_s^\star(t;\mathbf{f}^\star)=\log\left(1+[\lambda_{\mathbf{\Sigma}}(\mathbf{f}^\star,t)]^+\right)$.

More specifically, if $y'_{m,n}(f_m^{s-1};f_n^{s-1})=0$, we have

$$\begin{cases}\kappa_{m,n}=(1-\delta_{m,n})\pi^2\tau_m^2,\\ \zeta_{m,n}=f_m^{s-1},\\ \delta_{m,n}=\cos[2\pi(f_m^{s-1}\tau_m-f_n^{s-1}\tau_n)]\in\{1,\ -1\}.\end{cases} \tag{24}$$

Otherwise,

$$\begin{cases}\kappa_{m,n}=\dfrac{-\pi\tau_m\sin[2\pi(f_m^{s-1}\tau_m-f_n^{s-1}\tau_n)]}{f_m^{s-1}-\zeta_{m,n}}\\ \zeta_{m,n}=\begin{cases}\dfrac{\lfloor 2(f_m^{s-1}\tau_m-f_n^{s-1}\tau_n)\rfloor}{2\tau_m}+\dfrac{f_n^{s-1}\tau_n}{\tau_m},\\ \qquad\text{if } y'_{m,n}(f_m^{s-1};f_n^{s-1})>0\\ \dfrac{\lceil 2(f_m^{s-1}\tau_m-f_n^{s-1}\tau_n)\rceil}{2\tau_m}+\dfrac{f_n^{s-1}\tau_n}{\tau_m},\\ \qquad\text{if } y'_{m,n}(f_m^{s-1};f_n^{s-1})<0\end{cases}\\ \delta_{m,n}=\cos[2\pi(f_m^{s-1}\tau_m-f_n^{s-1}\tau_n)]-\kappa_{m,n}(f_m^{s-1}-\zeta_{m,n})^2\end{cases} \tag{25}$$

where $\lfloor\cdot\rfloor$ and $\lceil\cdot\rceil$ round the argument to the nearest integer towards $-\infty$ and ∞, respectively.

In Table II, we summarize the two-stage FDA beamforming algorithm for the instantaneous SRM problem. Specifically, in the first stage, we maximize the principal eigenvalue $\lambda_\Sigma(\mathbf{f},t)$ by optimizing the frequency offsets. Then, in the second stage, utilizing the frequency offsets obtained in the first stage, we determine the optimal transmit beamformer as in (13). We should mention that this two-stage algorithm is done in one shot and there is no alternating between the frequency offsets optimization and the transmit beamformer optimization. With each stage being solved analytically, the two-stage algorithm can be efficiently performed.

C. Solution to Average SRM Problem

Since the optimal frequency offsets for (P1), i.e., the instantaneous SRM problem, are independent of time, the proposed two-stage algorithm (cf. Table II) can be directly used to solve the following problem, which maximizes the average secrecy rate within a predefined time period of length T, i.e.,

$$\begin{aligned}\max_{\{\mathbf{f},\ \{\mathbf{w}(t)\}_{t\in[0,T]}\}}\ & \frac{1}{T}\int_0^T R_s(t)dt \\ \text{s.t. } & \|\mathbf{w}(t)\|_2^2 \le P, \quad \forall\ t\in[0,T], \\ & f_c \le f_m \le f_c + \Delta F, \quad \forall m.\end{aligned} \tag{P6}$$

To solve (P6), we employ a time-varying FDA beamforming approach. Specifically, we first optimize $\mathbf{f}$ based on θ_e and θ_u, and then calculate $\mathbf{w}(t)$ according to the frequency offsets in real time as (13). From Lemma 2, we konw that besides the optimal frequency offsets, the maximum principal eigenvalue $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$ is also time independent, indicating that (P1) has constant optimal secrecy rate for arbitrary time instant. Therefore, (P1) and (P6) have same optimal objective value. In this sense, the instantaneous and average SRM problems are equivalent.

We discuss how to implement the time-varying FDA beamforming in practice before closing this section. It is generally impractical to continuously update the beamformer as in (13). As a compromise, we define some time interval $\Delta T_w = \frac{T}{L}$, and a series of beamformer refreshing time points, i.e., $t_l^w = (l-1)\Delta T_w, l = 1,2,\ldots,L$. That is, we update beamformer at t_l^w and then use $\mathbf{w}(t_l^w)$ as the transmit beamformer within $t_l^w \le t < t_{l+1}^w$. Thus, the objective of (P6) is approximated by

$$\frac{1}{T}\int_0^T R_s(t)dt \simeq \frac{1}{T}\sum_{l=1}^{L}\int_{t_l^w}^{t_{l+1}^w}\log\left[\frac{1+\mathbf{w}^\dagger(t_l^w)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t_l^w)}{1+\mathbf{w}^\dagger(t_l^w)\mathbf{H}_e(\mathbf{f},t)\mathbf{w}(t_l^w)}\right]dt. \tag{26}$$

Obviously, there is a trade off between secrecy performance and implementation cost in practice. Higher beamformer refreshing frequency (BRF $= \frac{1}{\Delta T_w}$) leads to better approximation in (26), yet higher implementation cost. Nevertheless, as shown later in simulations (cf. Fig. 9), BRF = 50MHz already yields very accurate approximation. Such a BRF can be easily implemented in current hardware platforms, e.g., [33].

IV. Some Extensions

In the previous discussion, we have made some assumptions to simplify the formulation, e.g., perfect Eve CSI and single antenna Eve. In this section, we extend the FDA beamforming approach and the two-stage algorithm to more practical cases, such as imperfect Eve CSI and multi-antenna Eve.

A. Robust FDA Beamforming for Imperfect Eve CSI

In practice, there is always some uncertainty in the CSI of Eve. Actually, so far the robust SRM problem with imperfect Eve CSI has been intensively researched. For instance, [7] tries to achieve secure transmission by limiting the worst-case (maximum) Eve rate in a bounded-sphere CSI uncertainty set. By applying semidefinite relaxation (SDR) and *S-Lemma*, the worst-case Eve rate constraint is recast as a convex linear matrix inequality (LMI) constraint. An outage-constrained SRM problem is studied in [8], where no specific Eve channel information is available at the transmitter except for the Rayleigh distribution. With the help of some inverse cumulative distribution function, the probabilistic outage constraint is transformed to a deterministic convex LMI constraint. Hu *et al.* [26] considered the case where the Eve's location is unknown, and examine the average performance of an AN-aided FDA secure transmission scheme. Departing from the existing studies, we bypass the troublesome CSI uncertainty distribution modeling problem, and deal with the robust FDA beamforming design under a *moment-based* random CSI model, where only some roughly estimated first and second-order statistics of Eve CSI are available, while the exact distribution or other high-order statistics are unknown.

In particular, we denote the actual Eve CSI as $\mathbf{h}_e(\mathbf{f},t) = \hat{\mathbf{h}}_e(\mathbf{f},t) + \Delta\mathbf{h}_e(\mathbf{f},t)$, where $\hat{\mathbf{h}}_e(\mathbf{f},t)$ is the Eve CSI estimate and $\Delta\mathbf{h}_e(\mathbf{f},t)$ is the CSI error, which is known to be randomly distributed with mean $\boldsymbol{\xi}_e(\mathbf{f},t)$ and covariance matrix $\mathbf{\Omega}_e$, while its exact distribution is not available. We further assume that the CSI errors with different antennas are independent with each other and have equal variance of γ, i.e., $\mathbf{\Omega}_e = \gamma\mathbf{I}$. Let $\mathcal{S}(\boldsymbol{\xi}_e(\mathbf{f},t),\mathbf{\Omega}_e)$ denote the set of all possible distributions having mean $\boldsymbol{\xi}_e(\mathbf{f},t)$ and covariance $\mathbf{\Omega}_e$. The outage-constrained instantaneous SRM problem based on FDA beamforming is formulated as

$$\begin{aligned}\max_{\{\mathbf{f},\mathbf{w}(t)\}}\ & R_s \\ \text{s.t. } & \min_{\mathcal{D}_e\in\mathcal{S}(\boldsymbol{\xi}_e(\mathbf{f},t),\mathbf{\Omega}_e)}\ \operatorname{Prob}_{\Delta\mathbf{h}_e(\mathbf{f},t)\sim\mathcal{D}_e}\{R_u(t)-R_e(t)\ge R_s\} \\ & \qquad \ge 1-\epsilon, \\ & \|\mathbf{w}(t)\|_2^2 \le P, \quad f_c \le f_m \le f_c+\Delta F, \quad \forall m,\end{aligned} \tag{P7}$$

where $0 \le \epsilon \le 1$ is the outage probability, indicating the probability of the secrecy rate falling below R_s. Due to the unavailability of the exact distribution of $\Delta\mathbf{h}_e(\mathbf{f},t)$, we keep the outage probability below ϵ strictly for arbitrary distribution $\mathcal{D}_e \in \mathcal{S}(\boldsymbol{\xi}_e(\mathbf{f},t),\mathbf{\Omega}_e)$.

Introducing an intermediate variable τ_e, (27) is equivalently expressed as

$$\begin{aligned}\max_{\{\mathbf{f},\mathbf{w}(t),\tau_e\}}\ & \log\left[\frac{1+\mathbf{w}^\dagger(t)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t)}{1+\tau_e}\right] \\ \text{s.t. } & \min_{\mathcal{D}_e\in\mathcal{S}(\boldsymbol{\xi}_e(\mathbf{f},t),\mathbf{\Omega}_e)}\ \operatorname{Prob}_{\Delta\mathbf{h}_e(\mathbf{f},t)\sim\mathcal{D}_e}\left\{\frac{|\mathbf{w}^\dagger(t)\mathbf{h}_e(\mathbf{f},t)|^2}{\sigma_e^2}\le\tau_e\right\} \\ & \qquad \ge 1-\epsilon, \\ & \|\mathbf{w}(t)\|_2^2 \le P, \quad f_c \le f_m \le f_c+\Delta F, \quad \forall m.\end{aligned} \tag{P8}$$

This problem is challenging due to the outage constraint (28), that consists of infinite number of probabilistic constraints. As a compromise, we replace the outage probability with its lower bound, which can be expressed in a deterministic form based on Markov's inequality, i.e.,

$$\begin{aligned}&\min_{D_e\in\mathcal{S}(\boldsymbol{\xi}_e(\mathbf{f},t),\mathbf{\Omega}_e)}\ \operatorname{Prob}_{\Delta\mathbf{h}_e(\mathbf{f},t)\sim D_e}\left\{\frac{|\mathbf{w}^\dagger(t)\mathbf{h}_e(\mathbf{f},t)|^2}{\sigma_e^2}\le\tau_e\right\} \\ &\qquad \ge 1-\frac{\mathsf{E}\{|\mathbf{w}^\dagger(t)\mathbf{h}_e(\mathbf{f},t)|^2\}}{\tau_e\sigma_e^2} \\ &\qquad = 1-\frac{\mathbf{w}^\dagger(t)\hat{\mathbf{\Theta}}_e(\mathbf{f},t)\mathbf{w}(t)}{\tau_e\sigma_e^2}\end{aligned} \tag{29}$$

where $\mathsf{E}\{\cdot\}$ denotes expectation, and

$$\begin{aligned}\hat{\boldsymbol{\Theta}}_e(\mathbf{f},t) &= \mathsf{E}\left\{\mathbf{h}_e(\mathbf{f},t)\mathbf{h}_e^{\dagger}(\mathbf{f},t)\right\} \\ &= [\hat{\mathbf{h}}_e(\mathbf{f},t)+\boldsymbol{\xi}_e(\mathbf{f},t)][\hat{\mathbf{h}}_e(\mathbf{f},t)+\boldsymbol{\xi}_e(\mathbf{f},t)]^{\dagger}+\gamma\mathbf{I}. \end{aligned} \tag{30}$$

Then, the outage-constrained SRM problem is conservatively approximated as a deterministic problem, i.e.,

$$\max_{\{\mathbf{f},\mathbf{w}(t),\tau_e\}} \log\left[\frac{1+\mathbf{w}^{\dagger}(t)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t)}{1+\tau_e}\right] \tag{P9}$$

$$\text{s.t. } \mathbf{w}^{\dagger}(t)\hat{\boldsymbol{\Theta}}_e(\mathbf{f},t)\mathbf{w}(t) \le \epsilon\sigma_e^2\tau_e,$$

$$\|\mathbf{w}(t)\|_2^2 \le P, \quad f_c \le f_m \le f_c+\Delta F, \ \forall m. \tag{31}$$

One can easily verify that (31) holds for equality when the optimality of (31) is achieved, i.e., $\tau_e = \mathbf{w}^{\dagger}(t)\boldsymbol{\Theta}_e(\mathbf{f},t)\mathbf{w}(t)$ with $\boldsymbol{\Theta}_e(\mathbf{f},t) = \epsilon^{-1}\sigma_e^{-2}\hat{\boldsymbol{\Theta}}_e(\mathbf{f},t)$. Then, (31) takes a similar form as (P1), and can be solved by the two-stage algorithm.

In particular, we optimize the frequency offsets in the first stage by solving the following problem,

$$\min_{\mathbf{f}} \ |\langle[\hat{\mathbf{h}}_e(\mathbf{f},t)+\boldsymbol{\xi}_e(\mathbf{f},t)],\ \mathbf{h}_u(\mathbf{f},t)\rangle|^2 \tag{P10}$$

$$\text{s.t. } f_c \le f_m \le f_c+\Delta F, \quad \forall m,$$

which can be solved with stationary convergence guarantee by the BSUM algorithm developed in Sec. III-B. In the second stage, we compute the optimal beamformer as in (13).

B. FDA Beamforming for Multi-Antenna Eve

In practice, Eve is usually equipped with multiple antennas to wiretap the confidential signal from the transmitter. In this subsection, we extend the FDA beamforming approach to the case of multi-antenna Eve.

Assuming that the Eve is equipped with $N > 1$ antennas, the perfect channel matrix between the transmit array and Eve is then denoted by

$$\mathbf{G}_e(\mathbf{f},t) = [\mathbf{h}_e^1(\mathbf{f},t), \mathbf{h}_e^2(\mathbf{f},t), \ldots, \mathbf{h}_e^N(\mathbf{f},t)] \in \mathbb{C}^{M\times N}, \tag{32}$$

where $\mathbf{h}_e^n \in \mathbb{C}^{M\times 1}$ is the channel between transmit array and the nth Eve antenna, for $n = 1, 2, \ldots, N$. Using the results in [27]–[29], the SRM problem for multi-input, single-output, multi-eavesdropper (MISOME) wiretap channel is given by

$$\max_{\{\mathbf{f},\mathbf{w}(t)\}} \log\left[\frac{1+\mathbf{w}^{\dagger}(t)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t)}{1+\mathbf{w}^{\dagger}(t)\boldsymbol{\Gamma}_e(\mathbf{f},t)\mathbf{w}(t)}\right] \tag{P11}$$

$$\text{s.t.} \quad \|\mathbf{w}(t)\|_2^2 \le P, \ f_c \le f_m \le f_c+\Delta F, \quad \forall m,$$

where $\boldsymbol{\Gamma}_e(\mathbf{f},t) = \sigma_e^{-2}\mathbf{G}_e(\mathbf{f},t)\mathbf{G}_e^{\dagger}(\mathbf{f},t)$.

Obviously, the frequency offsets can be obtained by minimizing the inner product of $\mathbf{h}_e^n(\mathbf{f},t)$ and the range space of $\mathbf{G}_e(\mathbf{f},t)$, i.e.,

$$\min_{\mathbf{f}} \ \sum_{n=1}^{N} |\langle[\mathbf{h}_e^n(\mathbf{f},t),\ \mathbf{h}_u(\mathbf{f},t)\rangle|^2 \tag{P12}$$

$$\text{s.t. } f_c \le f_m \le f_c+\Delta F, \quad \forall m.$$

Generally speaking, (33) is difficult and the BSUM algorithm can be used to find a stationary solution. However, in the case of highly directional LOS mmWave transmission, (33) can be simplified. In particular, we consider the case where the Eve employs the N-antenna uniform linear receive array with d_e being the uniform antenna spacing, and then under the far-field assumption (i.e., parallel wavefront), we have

$$\mathbf{h}_e^n(\mathbf{f},t) = e^{j2\pi f_m\frac{(n-1)d_e\sin\theta_e}{c}}\cdot\mathbf{h}_e^1(\mathbf{f},t), \quad \forall\ n, \tag{33}$$

with $\mathbf{h}_e^1(\mathbf{f},t) = \mathbf{h}_e(\mathbf{f},t)$. Thus, $\boldsymbol{\Gamma}_e(\mathbf{f},t)$ reduces to a rank-one matrix, i.e., $\boldsymbol{\Gamma}_e(\mathbf{f},t) = N\cdot\mathbf{H}_e(\mathbf{f},t)$. In consequence, (P12) is the same as (P1), except for a slight difference in objectives; that is, the objective changes from $\log\left[\frac{1+\mathbf{w}^{\dagger}(t)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t)}{1+\mathbf{w}^{\dagger}(t)\mathbf{H}_e(\mathbf{f},t)\mathbf{w}(t)}\right]$ to $\log\left[\frac{1+\mathbf{w}^{\dagger}(t)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t)}{1+N\cdot\mathbf{w}^{\dagger}(t)\mathbf{H}_e(\mathbf{f},t)\mathbf{w}(t)}\right]$.

Therefore, we can employ the two-stage algorithm (cf. Table II) to solve (P12). We remark that if the optimal frequency offsets can be obtained, then the channels of LU and Eve can be turned exactly orthogonal and the secure performance of FDA beamforming is independent of the Eve antenna number N; otherwise, the secrecy rate decreases with N due to the information leakage to Eve.

V. Numerical Examples

We consider an LOS mmWave communication system operating at $f_c = 60$GHz. The system consists of an M-antenna transmit array, a single-antenna LU and a single-antenna Eve. We fix the LU's coordinate as $(r_u, \theta_u) = (1000\text{m}, 30^{\text{o}})$, and change the Eve's coordinate (r_e, θ_e), the antenna number M, the transmit power budget P, and the frequency offset upper bound ΔF to test the proposed algorithm's performance in different aspects. We assume -100dBm receive noise power for both LU and Eve, i.e., $10\log(\sigma_u^2) = 10\log(\sigma_e^2) = -100$dBm. The signal attenuation factor $a(r)$ is determined by the free-space path loss formula of radio wave propagation [34], i.e.,

$$\begin{aligned}\text{Lfs (dB)} &= -20\log[a(r)] \\ &= 32.5+20\log[F(\text{MHz})]+20\log[r(\text{Km})] \end{aligned} \tag{34}$$

where $F \simeq f_c$ is transmit frequency in megahertz (MHz), and r is the range in kilometer (Km).

A. FDA Beamforming with Perfect Eve CSI

In Fig. 4, we show the converging behaviour of the BSUM algorithm (cf. Table I), with each trace starting from a randomly selected initial point. Typically, in the case of $M = 12$, $r_u = r_e = 1000$m, $\theta_u = 30^{\text{o}}$, $\theta_e = 32^{\text{o}}$ and $\Delta F = 10^{-1}f_c$, the BSUM algorithm converges in about 80 iterations.

In the next simulation, we fix $r_u = r_e = 1000$m, $\theta_u = 30^{\text{o}}$, and compare the secrecy rates of the proposed FDA beamforming approach and the conventional beamforming approach ($\Delta f_m = 0$, $\forall\ m$) for different values of θ_e. The results are shown in Fig. 5, where we also plot the theoretic secrecy rate upper bound; i.e., the maximum LU channel capacity (without Eve) which is given by $\log[1+\frac{a^2(r_u)PM}{\sigma_u^2}]$ since

$$\begin{aligned}R_u(t) &= \log(1+\sigma_u^{-2}|\mathbf{w}^{\dagger}(t)\mathbf{h}_u(\mathbf{f},t)|^2) \\ &\le \log(1+\sigma_u^{-2}P\|\mathbf{h}_u(\mathbf{f},t)\|^2) \\ &= \log(1+\sigma_u^{-2}a^2(r_u)PM), \end{aligned} \tag{35}$$

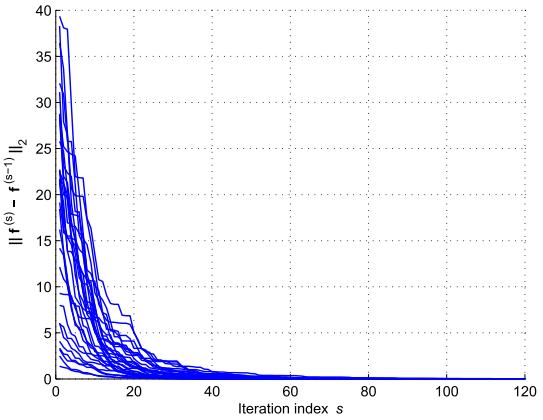


Fig. 4. Typical converging traces of BSUM iterations for $M = 12$, $r_u = r_e = 1000$m, $\theta_u = 30^o$, and $\theta_e = 32^o$.

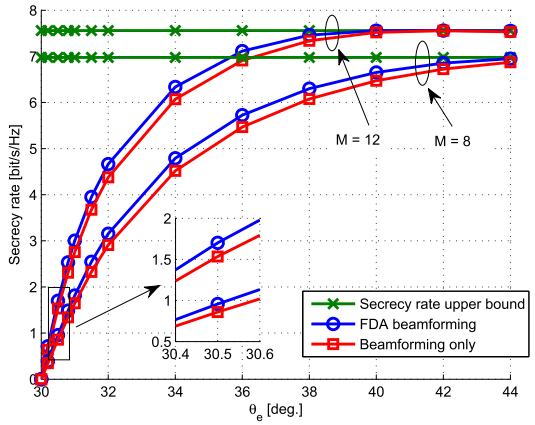


Fig. 5. Secrecy rate comparison for different Eve angle θ_e at $r_u = r_e = 1000$m, $\theta_u = 30^o$, $P = 10$dBW and $\Delta F = 10^{-1} f_c$.

where the inequality is due to the Cauchy-Schwartz inequality, and the equality holds at $\mathbf{w}(t) = \frac{\sqrt{P}\mathbf{h}_u(\mathbf{f},t)}{\|\mathbf{h}_u(\mathbf{f},t)\|_2}$.

When $\theta_e = \theta_u = 30^o$, $\mathbf{h}_u(\mathbf{f},t)$ and $\mathbf{h}_e(\mathbf{f},t)$ are linearly correlated despite the value of $\mathbf{f}$. Thus, both FDA beamforming and conventional beamforming fail to provide PHY security. As θ_e departs from θ_u, the two approaches begin to work gradually. Specifically, the FDA beamforming outperforms the conventional beamforming in the case of $\theta_e \neq \theta_u$. The reason is that we optimize the frequency offsets in FDA which helps decouple the channels of LU and Eve, even when they are close located, thus improving the secrecy rate.

In Fig. 6, we compare the secrecy rates of the two approaches for different antenna number M. As is well-known in array signal processing, increasing the antenna number M improves the array's capability in angle discrimination, and thus higher secrecy rate can be achieved. Again, the FDA beamforming approach outperforms the conventional beamforming approach, despite the value of M. This is expected since the carefully selected frequency offsets help decouple the channels of LU and Eve.

Figs. 7 and 8 illustrate how the value of frequency offsetting range ΔF influences the performance of FDA beamforming in PHY security. The absolute secrecy rates at different ΔF and θ_e are shown in Fig. 7. As expected, larger ΔF provides more flexibilities to choose f_m, $\forall$ m, and thus

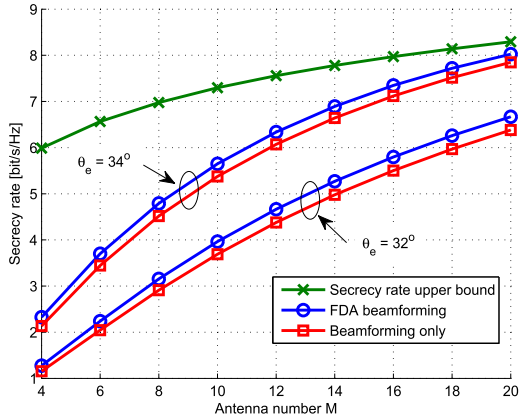


Fig. 6. Secrecy rate comparison for different antenna number M at $r_u = r_e = 1000$m, $\theta_u = 30^o$, $P = 10$dBW and $\Delta F = 10^{-1} f_c$.

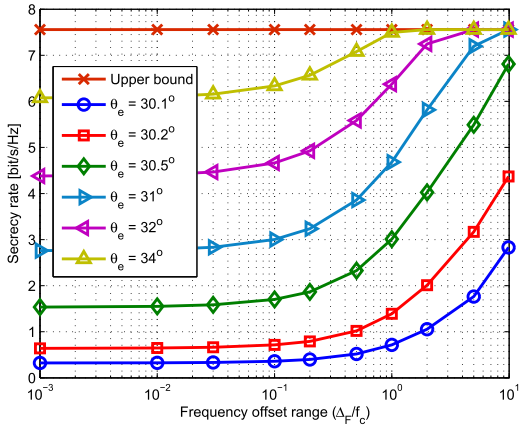


Fig. 7. Secrecy rate comparison for different frequency offsetting range ΔF at $r_u = r_e = 1000$m, $\theta_u = 30^o$, $P = 10$dBW and $M = 12$.

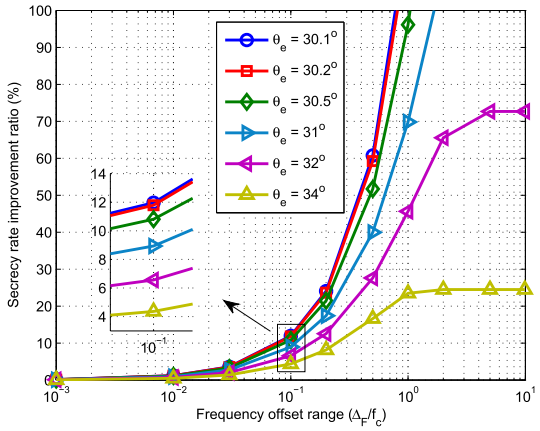


Fig. 8. Secrecy rate improvement ratio for different frequency offsetting range ΔF at $r_u = r_e = 1000$m, $\theta_u = 30^o$, $P = 10$dBW and $M = 12$.

improves the secrecy rate. Specifically, when ΔF is large enough, the channels of LU and Eve can be turned orthogonal, and the proposed FDA beamforming approach can achieve the theoretic secrecy rate upper bound.

The secrecy rate improvement rate is shown in Fig. 8, which is defined as

$$\text{ratio} \triangleq \frac{R_{s,\text{FB}} - R_{s,\text{CB}}}{R_{s,\text{CB}}} \times 100\%,$$

where $R_{s,\text{FB}}$ and $R_{s,\text{CB}}$ denote the respective secrecy rates of FDA beamforming and conventional beamforming.

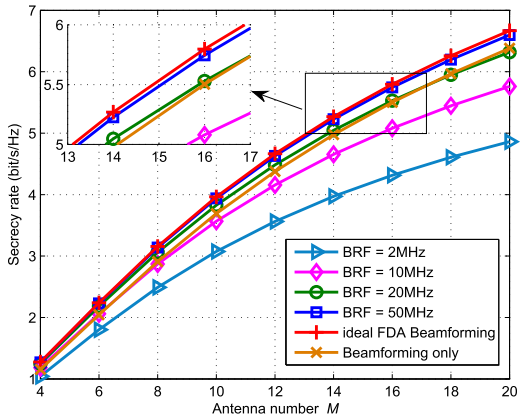


Fig. 9. Secrecy rate comparison for different BRFs at $r_u = r_e = 1000m$, $\theta_u = 30^o$, $\theta_e = 32^o$, and $P = 10$dBW.

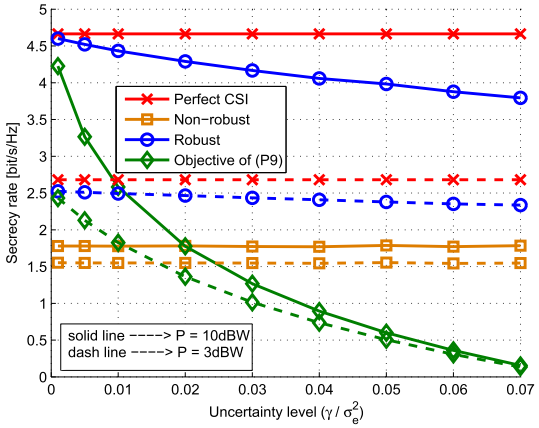


Fig. 10. Secrecy rate comparison for different Eve CSI uncertainty levels at $r_e = 1000$m, $\theta_e = 32^o$, $\hat{r}_e = 1000$m, $\hat{\theta}_e = 34^o$, and $\epsilon = 0.05$.

Consistent with the results in Fig. 7, larger ΔF yields higher secrecy rate improvement. In addition, the FDA beamforming outperforms the conventional beamforming more apparently as θ_e is closer to θ_u; that is, the proposed approach is especially useful in achieving PHY security for proximal LU and Eve.

We should mention that the FDA beamforming approach improves the secrecy rate at the cost of more frequency. Actually, introducing the frequency offsets renders some transmit bandwidth expansion. That is, the FDA beamforming requires wider transmit band than the conventional beamforming. On the other hand, ΔF is required to be far less than the carrier frequency and the transmit bandwidth in practice [35]. Therefore, we should balance the performance improvement and the bandwidth expansion. In this paper, we set $\Delta F = 10^{-1} f_c$ and more than 10% secrecy rate improvement is achievable as $\theta_e - \theta_u \leq 0.5^o$.

To show the behaviour of time-varying FDA beamforming in practice, we list the performance of FDA beamforming with different beamformer refreshing frequencies (BRFs) in Fig. 9. To this end, we define two refreshing time intervals — ΔT_w for beamformer and ΔT_h for channel ($\Delta T_h = \frac{\Delta T_w}{K}$, $K \gg 1$). The beamformer refreshing time point is $t_l^w = (l-1)\Delta T_w$ and the channel refreshing time point is $t_{l,k}^h = t_l^w + (k-1)\Delta T_h$ for $l = 1, 2, \ldots, L$; $k = 1, 2, \ldots, K$. Thus, the average secrecy rate is approximated by

$$\begin{aligned}
&\frac{1}{T}\int_{t=0}^{T} R_s(t)\,dt \\
&\simeq \frac{1}{T}\sum_{l=1}^{L}\int_{t_l^w}^{t_{l+1}^w} \log\left[\frac{1+\mathbf{w}^\dagger(t_l^w)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t_l^w)}{1+\mathbf{w}^\dagger(t_l^w)\mathbf{H}_e(\mathbf{f},t)\mathbf{w}(t_l^w)}\right]dt \\
&\simeq \frac{1}{T}\sum_{l=1}^{L}\sum_{k=1}^{K}\Delta T_h \cdot \log\left[\frac{1+\mathbf{w}^\dagger(t_l^w)\mathbf{H}_u(\mathbf{f},t_{l,k}^h)\mathbf{w}(t_l^w)}{1+\mathbf{w}^\dagger(t_l^w)\mathbf{H}_e(\mathbf{f},t_{l,k}^h)\mathbf{w}(t_l^w)}\right]. \qquad (36)
\end{aligned}$$

In Fig. 9, we choose $T = 20\mu$s, and the channel refreshing frequency (CRF) = $1/\Delta T_h = 200$GHz[3]. As expected, higher BRF yields more precise approximation. The results in Fig. 9 indicate that BRF = 50MHz is sufficient, and the resultant average secrecy rate is very close to that of the ideal time-varying FDA beamforming. It should be mentioned that for current hardware platforms, the 50MHz BRF can be easily implemented [33].

B. Robust FDA Beamforming for Imperfect Eve CSI

Next, we consider the case of imperfect Eve CSI. The LU is located at ($r_u = 1000$m, $\theta_u = 30^o$). Assume that the estimate and actual Eve coordinates are ($\hat{r}_e = 1000$m, $\hat{\theta}_e = 34^o$) and ($r_e = 1000$m, $\theta_e = 32^o$), respectively. Besides the location estimation error, the Eve CSI suffers from other uncertainties, which are modeled as randomly distributed errors with zero mean and covariance $\gamma\,\mathbf{I}$, while the exact distribution is not known. In this simulation, we test three widely used distributions — Gaussian, uniform and Laplacian distributions.

The average secrecy rate comparison of the non-robust and robust algorithms over 3×10^6 randomly generated Eve CSI samples (10^6 samples for each distribution) is shown in Fig. 10 with $M = 12$ and $\epsilon = 0.05$. Due to the Eve CSI uncertainty, the non-robust algorithm cannot obtain the optimal frequency offsets, and hence has a very low secrecy rate even when γ is small. As a contrast, the robust algorithm achieves much higher average secrecy rate. As the uncertainty level increases, the performance of the robust algorithm degrades. Specifically, as $\frac{\gamma}{a^2(r_e)} > 0.07$, the secrecy rate threshold, i.e., the objective value of (P9), approaches zero and the robust algorithm stops working, because $\mathbf{w} = \mathbf{0}$ is always an optimal solution.

To show whether the outage probability constraint can be satisfied, we list the empirical outage probabilities for different values of ϵ in Fig. 11 at $M = 12$ and $\frac{\gamma}{a^2(r_e)} = 0.01$, where each point is obtained over 10^6 random CSI errors. The non-robust algorithm has an average secrecy outage probability very close to 1, while for the three tested CSI error distributions, the proposed robust algorithm always satisfies the outage probability requirement as ϵ varies. In particular, as $\epsilon < 0.05$, the outage probabilities of the these distributions are all below 10^{-6}; i.e., no outage occurs during our simulations. This is expected since we optimize the lower bound of the outage

[3]We use CRF in simulation only. In practice, the channel changes automatically as in (1) and we only update beamformer at some given time points. In other words, the real average secrecy rate in practical digital implementation is given by (26), which is approximated by (36) in simulation.

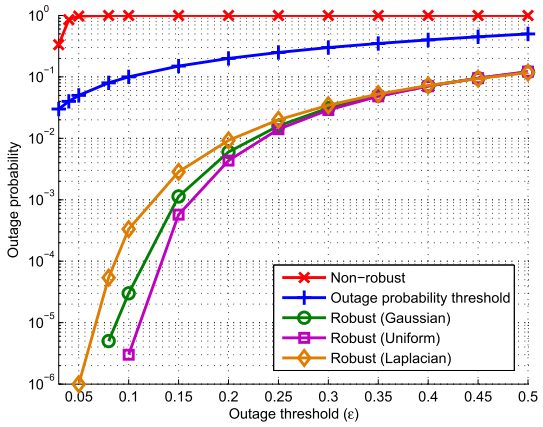


Fig. 11. Empirical outage probabilities for different values of ϵ at $M = 12$, $r_e = 1000$m, $\theta_e = 32^{\rm o}$, $\hat{r}_e = 1000$m, $\hat{\theta}_e = 34^{\rm o}$, $\frac{\gamma}{a^2(r_e)} = 0.01$, and $P = 10$dBW.

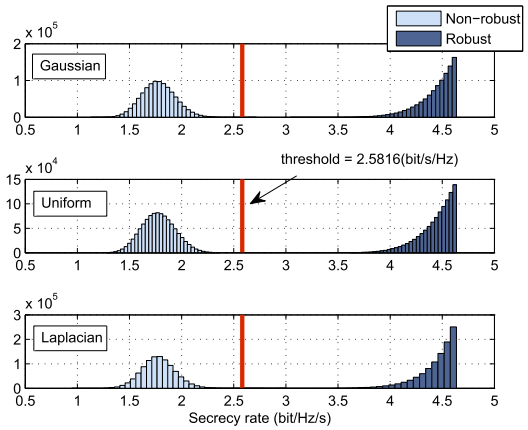


Fig. 12. Secrecy rate histograms under different distributions at $M = 12$, $r_e = 1000$m, $\theta_e = 32^{\rm o}$, $\hat{r}_e = 1000$m, $\hat{\theta}_e = 34^{\rm o}$, $\frac{\gamma}{a^2(r_e)} = 0.01$, $\epsilon = 0.05$, and $P = 10$dBW.

probability for arbitrary Eve CSI error distribution in the set of $\mathcal{S}(\boldsymbol{\xi}_e(\mathbf{f}, t), \boldsymbol{\Omega}_e)$. That is, the robust design provides a worst-case secrecy outage probability guarantee. This is particularly important for PHY security, where the information leakage should be stringently controlled in a worst-case sense.

To show the result more clearly, we further plot the secrecy rates histograms of non-robust and robust algorithms in Fig. 12 at $M = 12$, $\epsilon = 0.05$ and $\frac{\gamma}{a^2(r_e)} = 0.01$. From this figure, we see that for most channel realizations, the empirical secrecy rate of the robust algorithm is above the secrecy rate threshold obtained from (P9). Obviously, the outage probability is far below 5% for all the three tested distributions. On the other hand, almost all the empirical secrecy rates of the non-robust algorithm are below the secrecy rate threshold; that is, the non-robust design suffers from severe secrecy outage, and cannot provide satisfactory transmission security because of ignoring the Eve CSI imperfection.

C. FDA Beamforming for Multi-Antenna Eve

In the last simulation, we show the performance of FDA beamforming for different Eve antenna numbers. In Fig. 13, we let the Eve approach LU from $\theta_e = 40^{\rm o}$ to $\theta_e = 30.1^{\rm o}$ gradually, and see how the number of Eve antennas, i.e., N, influences the secrecy rate. Consistent with previous analysis, as Eve is far from LU, the orthogonality between $\mathbf{h}_u(\mathbf{f}, t)$ and $\mathbf{h}_e(\mathbf{f}, t)$ can be easily achieved (cf. Fig. 5), and hence the performance of FDA beamforming is independent of N. As Eve is close to LU, usually only a stationary solution to the frequency offsets can be obtained, yielding some information leakage. Thus, the secrecy rate degrades with N. Moreover, due to the marginal effect of logarithmic function, the secrecy rate decreases rapidly with N when N is small, and the falling speed slows down as N increases.

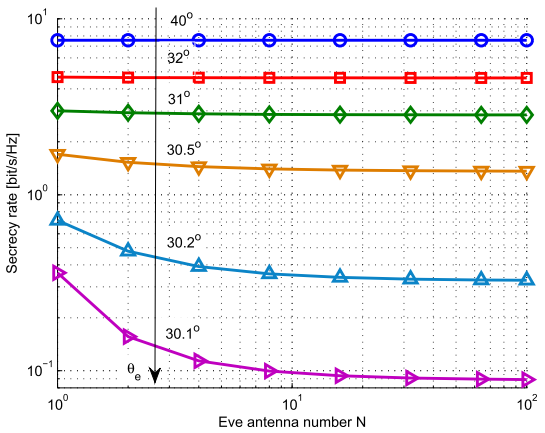


Fig. 13. Secrecy rate for different numbers of Eve antennas at $M = 12$, $r_e = 1000$m, $r_u = 1000m$, $\theta_u = 30^{\rm o}$, and $P = 10$dBW.

VI. Conclusion

In this paper, we consider the PHY security problem for proximal LU and Eve, under which many conventional PHY security approaches fail to provide satisfactory secrecy performance due to the highly correlated LU and Eve channels. To tackle this, we introduce some frequency offsets across the array antennas to decouple the channels, and then propose an innovative FDA beamforming approach. Specifically, we integrate beamforming into FDA, and then aim to maximize the secrecy rate by jointly optimizing the frequency offsets and the array transmit beamformer. To solve this challenging problem, we first provide some insights to the solution of FDA beamforming. Then, we develop a two-stage algorithm which optimizes the frequency offsets and the transmit beamformer successively. With each step being calculated in closed form, the proposed algorithm can be efficiently implemented. Moreover, we show that the proposed two-stage algorithm can be easily extended to the cases of imperfect Eve CSI and multi-antenna Eve. Finally, the effectiveness of FDA beamforming in PHY security has been demonstrated via extensive numerical simulations.

Appendix A
Proof of Lemma 1

Utilizing (4), (5), (8) and (9), we rewrite the instantaneous secrecy rate as

$$R_s(t) = \log\left[\frac{1+\mathbf{w}^\dagger(t)\mathbf{H}_u(\mathbf{f},t)\mathbf{w}(t)}{1+\mathbf{w}^\dagger(t)\mathbf{H}_e(\mathbf{f},t)\mathbf{w}(t)}\right] = \log\left[1 + \frac{\mathbf{w}^\dagger(t)[\mathbf{H}_u(\mathbf{f},t)-\mathbf{H}_e(\mathbf{f},t)]\mathbf{w}(t)}{1+\mathbf{w}^\dagger(t)\mathbf{H}_e(\mathbf{f},t)\mathbf{w}(t)}\right]. \quad (37)$$

Therefore, with given $\mathbf{f}$, the SRM problem is equivalent to

$$\max_{\|\mathbf{w}(t)\|_2^2 \le P} \frac{\mathbf{w}^\dagger(t)[\mathbf{H}_u(\mathbf{f},t)-\mathbf{H}_e(\mathbf{f},t)]\mathbf{w}(t)}{1+\mathbf{w}^\dagger(t)\mathbf{H}_e(\mathbf{f},t)\mathbf{w}(t)} \tag{P-A1}$$

Clearly, in the case of $[\mathbf{H}_u(\mathbf{f},t)-\mathbf{H}_e(\mathbf{f},t)] \preceq \mathbf{0}$, $\mathbf{w}(t)=\mathbf{0}$ is optimal, and the resultant secrecy rate is zero. For the positive secrecy rate case, the array must transmit at full power, namely, $\|\mathbf{w}(t)\|_2^2 = \mathbf{w}^\dagger(t)\mathbf{w}(t) = P$. By making a change of variable $\hat{\mathbf{w}}(t) = \frac{1}{\sqrt{P}}\mathbf{w}(t)$, we can rewrite (38) as

$$\max_{\|\hat{\mathbf{w}}(t)\|_2^2=1} \frac{\hat{\mathbf{w}}^\dagger(t)[\mathbf{H}_u(\mathbf{f},t)-\mathbf{H}_e(\mathbf{f},t)]\mathbf{w}(\hat{t})}{\hat{\mathbf{w}}^\dagger(t)\tilde{\mathbf{H}}_e(\mathbf{f},t)\hat{\mathbf{w}}(t)} \tag{P-A2}$$

with $\tilde{\mathbf{H}}_e(\mathbf{f},t) = \mathbf{H}_e(\mathbf{f},t) + \frac{1}{P}\mathbf{I}$. Actually, problem (38) is a Rayleigh quotient and the optimal solution is given by $\hat{\mathbf{w}}(t) = \frac{\tilde{\mathbf{H}}_e^{-1/2}(\mathbf{f},t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f},t)}{\|\tilde{\mathbf{H}}_e^{-1/2}(\mathbf{f},t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f},t)\|_2}$, with the maximal objective value being $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$. Equivalently, the optimal secrecy rate and the transmit beamformer of (P1) with given $\mathbf{f}$ are given by

$$R_s^\star(t;\mathbf{f}) = \log(1+[\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)]^+),$$
$$\mathbf{w}^\star(t;\mathbf{f}) = \mathrm{sgn}\{\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)\}\cdot\frac{\sqrt{P}\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f},t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f},t)}{\|\tilde{\mathbf{H}}_e^{-\frac{1}{2}}(\mathbf{f},t)\mathbf{v}_{\mathbf{\Sigma}}(\mathbf{f},t)\|_2}.$$

Appendix B
Proof of Lemma 2

For two matrices $\mathbf{A}$ and $\mathbf{B}$ with proper dimensions, we have $\mathrm{eig}(\mathbf{AB}) = \mathrm{eig}(\mathbf{BA})$. Hence, $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$ is actually the principal eigenvalue of $\tilde{\mathbf{H}}_e^{-1}(\mathbf{f},t)[\mathbf{H}_u(\mathbf{f},t)-\mathbf{H}_e(\mathbf{f},t)]$. Applying matrix inverse lemma [30], we obtain

$$\begin{aligned}
&\tilde{\mathbf{H}}_e^{-1}(\mathbf{f},t)[\mathbf{H}_u(\mathbf{f},t)-\mathbf{H}_e(\mathbf{f},t)]\\
&= P\left[\mathbf{I}-\frac{P\tilde{\mathbf{h}}_e(\mathbf{f},t)\tilde{\mathbf{h}}_e^\dagger(\mathbf{f},t)}{1+P\|\tilde{\mathbf{h}}_e(\mathbf{f},t)\|_2^2}\right]\left[\tilde{\mathbf{h}}_u(\mathbf{f},t)\tilde{\mathbf{h}}_u^\dagger(\mathbf{f},t)-\tilde{\mathbf{h}}_e(\mathbf{f},t)\tilde{\mathbf{h}}_e^\dagger(\mathbf{f},t)\right]\\
&= P\Bigg[\tilde{\mathbf{h}}_u(\mathbf{f},t)\tilde{\mathbf{h}}_u^\dagger(\mathbf{f},t)\\
&\qquad -\frac{P\langle\tilde{\mathbf{h}}_e(\mathbf{f},t),\tilde{\mathbf{h}}_u(\mathbf{f},t)\rangle\tilde{\mathbf{h}}_e(\mathbf{f},t)\tilde{\mathbf{h}}_u^\dagger(\mathbf{f},t)}{1+P\|\tilde{\mathbf{h}}_e(\mathbf{f},t)\|_2^2}-\frac{\tilde{\mathbf{h}}_e(\mathbf{f},t)\tilde{\mathbf{h}}_e^\dagger(\mathbf{f},t)}{1+P\|\tilde{\mathbf{h}}_e(\mathbf{f},t)\|_2^2}\Bigg]
\end{aligned} \tag{38}$$

For notational simplicity, we drop the arguments of $(\mathbf{f},t)$ in $\tilde{\mathbf{h}}_u$, $\tilde{\mathbf{h}}_e$, $\mathbf{H}_u$, $\mathbf{H}_e$, and $\tilde{\mathbf{H}}_e$, when there is no ambiguity. Let us consider decomposing vectors $\tilde{\mathbf{h}}_u$ and $\tilde{\mathbf{h}}_e$ into two orthogonal components, i.e.,

$$\tilde{\mathbf{h}}_u = \beta\vec{\mathbf{h}}_e + \gamma\vec{\mathbf{h}}_{e^\perp}, \quad \tilde{\mathbf{h}}_e = \|\tilde{\mathbf{h}}_e\|_2\vec{\mathbf{h}}_e + 0\cdot\vec{\mathbf{h}}_{e^\perp} \tag{39}$$

where $\vec{\mathbf{h}}_e$ and $\vec{\mathbf{h}}_{e^\perp}$ are unit vectors parallel and orthogonal to $\tilde{\mathbf{h}}_e$, respectively; β and γ are scalar numbers satisfying $\beta^2+\gamma^2 = \|\tilde{\mathbf{h}}_u\|_2^2$.

Inserting (39) into (38), we obtain

$$\begin{aligned}
&\tfrac{1+P\|\tilde{\mathbf{h}}_e\|_2^2}{P}\cdot\tilde{\mathbf{H}}_e^{-1}(\mathbf{H}_u-\mathbf{H}_e)\\
&= \gamma^2(1+P\|\tilde{\mathbf{h}}_e\|_2^2)\vec{\mathbf{h}}_{e^\perp}\vec{\mathbf{h}}_{e^\perp}^\dagger+\beta\gamma(1+P\|\tilde{\mathbf{h}}_e\|_2^2)\vec{\mathbf{h}}_{e^\perp}\vec{\mathbf{h}}_e^\dagger\\
&\quad+\beta\gamma\vec{\mathbf{h}}_e\vec{\mathbf{h}}_{e^\perp}^\dagger+(\beta^2-\|\tilde{\mathbf{h}}_e\|_2^2)\vec{\mathbf{h}}_e\vec{\mathbf{h}}_e^\dagger\\
&= [\vec{\mathbf{h}}_{e^\perp},\vec{\mathbf{h}}_e]\begin{bmatrix}\gamma^2(1+P\|\tilde{\mathbf{h}}_e\|_2^2), & \beta\gamma(1+P\|\tilde{\mathbf{h}}_e\|_2^2)\\ \beta\gamma, & \beta^2-\|\tilde{\mathbf{h}}_e\|_2^2\end{bmatrix}[\vec{\mathbf{h}}_{e^\perp},\vec{\mathbf{h}}_e]^\dagger
\end{aligned} \tag{40}$$

which implies that $\tilde{\mathbf{H}}_e^{-1}(\mathbf{H}_u-\mathbf{H}_e)$ has at most two nonzero eigenvalues, with $\vec{\mathbf{h}}_{e^\perp}$ and $\vec{\mathbf{h}}_e$ being the associated eigenvectors. More specifically, the two possible nonzero eigenvalues are the roots of the following equation for $\beta^2\in[0,\|\tilde{\mathbf{h}}_u\|_2^2]$, (see [30, Ch. 1] for details)

$$\begin{aligned}
&\left[\lambda-\left(\|\tilde{\mathbf{h}}_u\|_2^2-\beta^2\right)\left(1+P\|\tilde{\mathbf{h}}_e\|_2^2\right)\right]\left[\lambda-\left(\beta^2-\|\tilde{\mathbf{h}}_e\|_2^2\right)\right]\\
&\qquad-\beta^2\left(\|\tilde{\mathbf{h}}_u\|_2^2-\beta^2\right)\left(1+P\|\tilde{\mathbf{h}}_e\|_2^2\right)=0,
\end{aligned} \tag{41}$$

where we use the fact $\gamma^2 = \|\tilde{\mathbf{h}}_u\|_2^2-\beta^2$. Solving the Eq. (41) gives the principal eigenvalue of $\mathbf{\Sigma}$:

$$\lambda_{\mathbf{\Sigma}} = \frac{P}{1+P\|\tilde{\mathbf{h}}_e\|_2^2}\cdot\frac{g(\beta^2)+\sqrt{g^2(\beta^2)+4q(\beta^2)}}{2} \tag{42}$$
$$g(\beta^2) = \|\tilde{\mathbf{h}}_u\|_2^2(1+P\|\tilde{\mathbf{h}}_e\|_2^2)-\|\tilde{\mathbf{h}}_e\|_2^2-P\|\tilde{\mathbf{h}}_e\|_2^2\beta^2 \tag{43}$$
$$q(\beta^2) = \|\tilde{\mathbf{h}}_e\|_2^2(1+P\|\tilde{\mathbf{h}}_e\|_2^2)(\|\tilde{\mathbf{h}}_u\|_2^2-\beta^2) \tag{44}$$

One can easily verify that $\lambda_{\mathbf{\Sigma}}$ is monotonically decreasing with β^2 for $\beta^2\in[0,\|\tilde{\mathbf{h}}_u\|_2^2]$. Therefore, maximizing $\lambda_{\mathbf{\Sigma}}$ is equivalent to minimizing β^2. Since $|\langle\mathbf{h}_e,\mathbf{h}_u\rangle|^2 = \beta^2\|\mathbf{h}_e\|_2^2 = Ma^2(r_e)\cdot\beta^2$, we establish the equivalence between (P2) and (P3).

Based on the definition of $\mathbf{h}_u(\mathbf{f},t)$ and $\mathbf{h}_e(\mathbf{f},t)$, we observe that the objective of (P3) is actually

$$|\langle\mathbf{h}_e(\mathbf{f},t),\mathbf{h}_u(\mathbf{f},t)\rangle|^2 = \left|a(r_u)a(r_e)\sum_{m=1}^{M}e^{j2\pi f_m\frac{(m-1)d(\sin\theta_e-\sin\theta_u)}{c}}\right|^2, \tag{45}$$

indicating that the optimal frequency offsets are independent of t, which keep constant as the locations of LU and Eve are fixed. Furthermore, we know that $\|\tilde{\mathbf{h}}_u(\mathbf{f},t)\|_2^2$, $\|\tilde{\mathbf{h}}_e(\mathbf{f},t)\|_2^2$, and β^2 are all independent of t, since

$$\|\tilde{\mathbf{h}}_u(\mathbf{f},t)\|_2^2 = \tfrac{a^2(r_e)M}{\sigma_u^2}, \tag{46}$$
$$\|\tilde{\mathbf{h}}_e(\mathbf{f},t)\|_2^2 = \tfrac{a^2(r_e)M}{\sigma_e^2}, \tag{47}$$
$$\beta^2 = \tfrac{|\langle\mathbf{h}_e(\mathbf{f},t),\mathbf{h}_u(\mathbf{f},t)\rangle|^2}{\|\tilde{\mathbf{h}}_e(\mathbf{f},t)\|_2^2}. \tag{48}$$

Then, we claim the maximum principal eigenvalue $\lambda_{\mathbf{\Sigma}}(\mathbf{f},t)$ is also time independent for given LU and Eve locations (cf. Eq. (42) – (44)).

Appendix C
Proof of Proposition 1

We establish the convergence of Algorithm 1 by showing that the assumptions in Theorem 1 are all fulfilled. Clearly, the tightness assumption, the identical derivative assumption and the continuity assumption in (16) hold automatically. In addition, $y_m(f_m;\mathbf{f}_{-m}^{s-1})$ is smooth and thus regular. Moreover, the unique solution of each subproblem is given as (22). Hence, we only need to check that the upper bound assumption holds. Since both $\tilde{u}(\cdot)$ and $\tilde{y}(\cdot)$ are symmetrical along $f_m=\zeta_{m,n}$, it is sufficient to show $\tilde{u}_{m,n}(f_m;f_m^{s-1},f_n^{s-1})\ge\tilde{y}_{m,n}(f_m;f_n^{s-1})$ for $f_m\ge\zeta_{m,n}$.

As $\tilde{y}'_{m,n}(f_m^{s-1};f_n^{s-1})=0$, we have $\tilde{y}_{m,n}(f_m^{s-1};f_n^{s-1})\in\{1,-1\}$. If $\tilde{y}_{m,n}(f_m^{s-1};f_n^{s-1})=1$, we directly have

$\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) = 1 \geq \tilde{y}_{m,n}(f_m; f_n^{s-1})$; otherwise, we show $u'_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \geq y'_{m,n}(f_m; f_n^{s-1})$ for $f_m \geq \zeta_{m,n} = f_m^{s-1}$. Basically, we have

$$\begin{aligned}
&\tilde{y}_{m,n}(f_m^{s-1}; f_n^{s-1}) = -1 \\
&\Rightarrow\ 2\pi(f_m^{s-1}\tau_m - f_n^{s-1}\tau_n) = (2k+1)\pi \\
&\Rightarrow\ y'_{m,n}(f_m; f_n^{s-1}) = -2\pi\tau_m \sin[2\pi(f_m\tau_m - f_n^{s-1}\tau_n)] \\
&\qquad = 2\pi\tau_m \sin[2\pi(f_m - \zeta_{m,n})\tau_m] \\
&\Rightarrow\ \tfrac{y'_{m,n}(f_m; f_n^{s-1})}{2(f_m-\zeta_{m,n})} = 2\pi^2\tau_m^2 \tfrac{\sin[2\pi(f_m-\zeta_{m,n})\tau_m]}{2\pi(f_m-\zeta_{m,n})\tau_m} \\
&\qquad \leq 2\pi^2\tau_m^2 = \kappa_{m,n} \\
&\Rightarrow\ y'_{m,n}(f_m; f_n^{s-1}) \leq 2\kappa_{m,n}(f_m - \zeta_{m,n}) \\
&\quad = u'_{m,n}(f_m; f_m^{s-1}, f_n^{s-1})
\end{aligned}$$

where k is an integer. We thus claim $\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \geq \tilde{y}_{m,n}(f_m; f_n^{s-1})$ in the case of $\tilde{y}'_{m,n}(f_m^{s-1}; f_n^{s-1}) = 0$.

As $\tilde{y}'_{m,n}(f_m^{s-1}; f_n^{s-1}) \neq 0$, without loss of generality, we focus on the case of $\tilde{y}'_{m,n}(f_m^{s-1}; f_n^{s-1}) > 0$. Considering that $\tilde{u}_{m,n}(f_m^{s-1}; f_m^{s-1}, f_n^{s-1}) = \tilde{y}_{m,n}(f_m^{s-1}; f_n^{s-1})$, we show $\tilde{u}'_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \leq \tilde{y}'_{m,n}(f_m; f_n^{s-1})$ for $f_m \in [\zeta_{m,n}, f_m^{s-1}]$ and $\tilde{u}'_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \geq \tilde{y}'_{m,n}(f_m; f_n^{s-1})$ for $f_m > f_m^{s-1}$, to validate the upper bound assumption. Since $\tilde{y}_{m,n}(\zeta_{m,n}; f_n^{s-1}) = -1$, we have

$$2\pi(\zeta_{m,n}\tau_m - f_n^{s-1}\tau_n) = (2k+1)\pi \tag{49}$$

where k is an integer. This leads to

$$\begin{aligned}
&\tilde{u}'_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \\
&\quad = -2\pi\tau_m \sin[2\pi(f_m^{s-1}\tau_m - f_n^{s-1}\tau_n)] \tfrac{f_m-\zeta_{m,n}}{f_m^{s-1}-\zeta_{m,n}} \\
&\quad = 2\pi\tau_m \sin[2\pi(f_m^{s-1} - \zeta_{m,n})\tau_m] \tfrac{f_m-\zeta_{m,n}}{f_m^{s-1}-\zeta_{m,n}} \qquad (50) \\
&\qquad \times \tilde{y}'_{m,n}(f_m; f_n^{s-1}) \\
&\quad = -2\pi\tau_m \sin[2\pi(f_m\tau_m - f_n^{s-1}\tau_n)] \\
&\quad = 2\pi\tau_m \sin[2\pi(f_m - \zeta_{m,n})\tau_m] \qquad (51)
\end{aligned}$$

In the case of $f_m \in [\zeta_{m,n}, f_m^{s-1}]$, since $2\pi(f_m^{s-1} - \zeta_{m,n})\tau_m \leq \pi$, see Fig. 3 or (23), we get

$$\begin{aligned}
&2\pi^2\tau_m^2 \tfrac{\sin[2\pi(f_m-\zeta_{m,n})\tau_m]}{2\pi(f_m-\zeta_{m,n})\tau_m} \geq 2\pi^2\tau_m^2 \tfrac{\sin[2\pi(f_m^{s-1}-\zeta_{m,n})\tau_m]}{2\pi(f_m^{s-1}-\zeta_{m,n})\tau_m} \\
&\Rightarrow\ 2\pi\tau_m \tfrac{\sin[2\pi(f_m-\zeta_{m,n})\tau_m]}{f_m-\zeta_{m,n}} \geq 2\pi\tau_m \tfrac{\sin[2\pi(f_m^{s-1}-\zeta_{m,n})\tau_m]}{f_m^{s-1}-\zeta_{m,n}} \\
&\Rightarrow\ \tilde{y}'_{m,n}(f_m; f_n^{s-1}) \geq \tilde{u}'_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}). \qquad (52)
\end{aligned}$$

In the case of $f_m > f_m^{s-1}$, we focus on the range of $f_m \in (f_m^{s-1}, \hat{f}_m]$, where $\hat{f}_m$ is the smallest frequency satisfying $\hat{f}_m \geq f_m^{s-1}$ and $\tilde{y}_{m,n}(\hat{f}_m; f_n^{s-1}) = 1$, as shown in Fig. 3. Equivalently, we have $[2\pi(\hat{f}_m - \zeta_{m,n})\tau_m] = \pi$, and

$$\begin{aligned}
&2\pi^2\tau_m^2 \tfrac{\sin[2\pi(f_m-\zeta_{m,n})\tau_m]}{2\pi(f_m-\zeta_{m,n})\tau_m} \leq 2\pi^2\tau_m^2 \tfrac{\sin[2\pi(f_m^{s-1}-\zeta_{m,n})\tau_m]}{2\pi(f_m^{s-1}-\zeta_{m,n})\tau_m} \\
&\Rightarrow\ 2\pi\tau_m \tfrac{\sin[2\pi(f_m-\zeta_{m,n})\tau_m]}{f_m-\zeta_{m,n}} \leq 2\pi\tau_m \tfrac{\sin[2\pi(f_m^{s-1}-\zeta_{m,n})\tau_m]}{f_m^{s-1}-\zeta_{m,n}} \\
&\Rightarrow\ \tilde{y}'_{m,n}(f_m; f_n^{s-1}) \leq \tilde{u}'_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}). \qquad (53)
\end{aligned}$$

Based on (52), (53) and the fact $\tilde{u}_{m,n}(f_m^{s-1}; f_m^{s-1}, f_n^{s-1}) = \tilde{y}_{m,n}(f_m^{s-1}; f_n^{s-1})$, we claim that $\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \geq \tilde{y}_{m,n}(f_m; f_n^{s-1})$ for $f_m \in [\zeta_{m,n}, \hat{f}_m]$. Furthermore, considering that $\tilde{u}_{m,n}(\hat{f}_m; f_m^{s-1}, f_n^{s-1}) \geq \tilde{y}_{m,n}(\hat{f}_m; f_n^{s-1}) = 1$ and $\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1})$ is monotonically increasing as $f_m \geq \zeta_{m,n}$, we have $\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) > \tilde{y}_{m,n}(f_m; f_n^{s-1})$ for $f_m > \hat{f}_m$. Since the two functions are both symmetrical along $f_m = \zeta_{m,n}$, we conclude that $\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \geq \tilde{y}_{m,n}(f_m; f_n^{s-1})$ in the case of $\tilde{y}'_{m,n}(f_m^{s-1}; f_n^{s-1}) > 0$.

In the case of $\tilde{y}'_{m,n}(f_m^{s-1}; f_n^{s-1}) < 0$, we can similarly show that $\tilde{u}_{m,n}(f_m; f_m^{s-1}, f_n^{s-1}) \geq \tilde{y}_{m,n}(f_m; f_n^{s-1})$.

Therefore, all the BSUM assumptions in Theorem 1 are satisfied, indicating that every accumulation point of the iterates generated by Algorithm 1 is a stationary solution of (P4).

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their helpful comments and suggestions.

REFERENCES

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

[2] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, nos. 4–5, pp. 355–580, 2009.

[3] C. Jeong, I.-M. Kim, and D. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.

[4] X. Wang, K. Wang, and X.-D. Zhang, "Secure relay beamforming with imperfect channel side information," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2140–2155, Jun. 2013.

[5] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[6] S. Ma, M. Hong, E. Song, X. Wang, and D. Sun, "Outage constrained robust secure transmission for MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 10, pp. 5558–5570, Oct. 2014.

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

[8] V.-D. Nguyen, T. Q. Duong, O. A. Dobre, and O.-S. Shin, "Joint information and jamming beamforming for secrecy rate maximization in cognitive radio networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2609–2623, Nov. 2016.

[9] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf. (VTC)*, Sep. 2005, pp. 1906–1910.

[10] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[11] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, "Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks," *IEEE Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.

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

[13] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

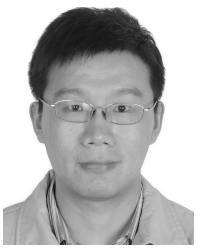
[14] A. Maltsev *et al.*, "Millimetre-wave evolution for backhaul and access," MiWEBA, Germany, Tech. Rep. FP7-ICT 368721/D5.1, Jun. 2014.

[15] S. Rangan, T. S. Rappaport, and E. Erkip, "Millimeter-wave cellular wireless networks: Potentials and challenges," *Proc. IEEE*, vol. 102, no. 3, pp. 366–385, Mar. 2014.

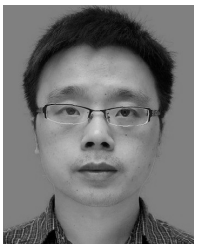
[16] X. Liu, Z. Xiao, L. Bai, J. Choi, P. Xia, and X.-G. Xia, "Beamforming based full-duplex for millimeter-wave communication," *Sensors*, vol. 16, no. 7, pp. 1–22, Jul. 2016.

[17] P. Antonik, M. C. Wicks, H. D. Griffiths, and C. J. Baker, "Frequency diverse array radars," in *Proc. IEEE Radar Conf.*, Apr. 2006, pp. 215–217.

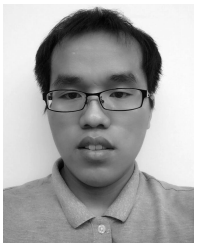
[18] P. Antonik, "An investigation of a frequency diverse array," Ph.D. dissertation, Dept. Electron. Elect. Eng., Univ. College London, London, U.K., 2009.
[19] W.-Q. Wang, "Overview of frequency diverse array in radar and navigation applications," *IET Radar, Sonar Navigat.*, vol. 10, no. 6, pp. 1001–1012, 2016.
[20] S. Mustafa, D. Simsek, and H. A. E. Taylan, "Frequency diverse array antenna with periodic time modulated pattern in range and angle," in *Proc. IEEE Radar Conf.*, Apr. 2007, pp. 427–430.
[21] W.-Q. Wang and H. C. So, "Transmit subaperturing for range and angle estimation in frequency diverse array radar," *IEEE Trans. Signal Process.*, vol. 62, no. 8, pp. 2000–2011, Apr. 2014.
[22] S. Huang, K. F. Tong, and C. J. Baker, "Frequency diverse array with beam scanning feature," in *Proc. IEEE Antennas Propag. Conf.*, San Diego, CA, USA, Jul. 2008, pp. 1–4.
[23] P. F. Sammartino, C. J. Baker, and H. D. Griffiths, "Frequency diverse MIMO techniques for radar," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 1, pp. 201–222, Jan. 2013.
[24] M. Razaviyayn, M. Hong, and Z.-Q. Luo, "A unified convergence analysis of block successive minimization methods for nonsmooth optimization," *SIAM J. Optim.*, vol. 23, no. 2, pp. 1126–1153, 2013.
[25] Y. Ding, J. Zhang, and V. Fusco, "Frequency diverse array OFDM transmitter for secure wireless communication," *Electron. Lett.*, vol. 51, no. 17, pp. 1374–1376, Aug. 2015.
[26] J. Hu, S. Yan, F. Shu, J. Wang, and Y. Zhang, "Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays," *IEEE Access*, vol. 5, pp. 1658–1667, Jan. 2017.
[27] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[28] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the MIMO Gaussian wiretap channel with an average power constraint," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2620–2631, May 2013.
[29] Q. Shi, E. Song, and G. Chen, "Signaling strategy optimization for Gaussian MIMO wiretap channel," in *Proc. IEEE ICC*, Jun. 2012, pp. 3611–3615.
[30] R. A. Horn and C. A. Johnson, *Matrix Analysis*. Cambridge, U.K.: Cambridge Univ. Press, 1985.
[31] P. Tseng, "Convergene of a block coordinate descent method for nondifferentiable minimization," *J. Optim. Theory Appl.*, vol. 109, no. 3, pp. 475–494, Jun. 2001.
[32] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, "Optimization of code rates in SISOME wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015.
[33] "Introduction to the NI mmWave transceiver system hardware," Nat. Instrum., Austin, TX, USA, White Paper, Apr. 2016. [Online]. Available: http://www.ni.com/white-paper/53095/en/
[34] A. Glodsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[35] C. Cetintepe and S. Demir, "Multipath characteristics of frequency diverse arrays over a ground plane," *IEEE Trans. Antennas Propag.*, vol. 62, no. 7, pp. 3567–3574, Jul. 2014.



Jingran Lin (M'14) received the B.S. degree in computer communication from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2001, and the M.S. and Ph.D. degrees in signal and information processing from UESTC in 2005 and 2007, respectively. In 2007, he joined the School of Communication and Information Engineering, UESTC, where he is currently an Associate Professor. From 2012 to 2013, he was a Visiting Scholar with the University of Minnesota (Twin Cities), Minneapolis, MN, USA. His research interests include the design and analysis of efficient optimization algorithms for the signal processing problems arising from modern communication systems.

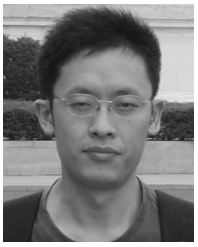


Qiang Li (M'13) received the B.Eng. and M.Phil. degrees in communication and information engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, and the Ph.D. degree in electronic engineering from The Chinese University of Hong Kong (CUHK), Hong Kong, in 2005, 2008, and 2012, respectively. From 2011 to 2012, he was a Visiting Scholar with the University of Minnesota, Minneapolis, MN, USA. From 2012 to 2013, he was a Research Associate with the Department of Electronic Engineering and the Department of Systems Engineering and Engineering Management, CUHK. Since 2013, he has been with the School of Communication and Information Engineering, UESTC, where he is currently an Associate Professor. His research interests include convex optimization and its application in signal processing with an emphasis on the physical-layer security and full-duplex communications. He received the First Prize Paper Award from the IEEE Signal Processing Society Postgraduate Forum Hong Kong Chapter in 2010, the Best Paper Award of the IEEE PIMRC 2016, and the Best Paper Award of the IEEE Signal Processing Letters 2016.



Jintai Yang received the B.S. degree in electronic and information engineering from Zhejiang Sci-Tech University, Hangzhou, China, in 2016. He is currently pursuing the M.S. degree in communication and information systems with the University of Electronic Science and Technology of China. He is currently a Visiting Student with The Chinese University of Hong Kong, Shenzhen. His research interests include signal processing, wireless communications, machine learning, and large-scale optimization theory.

Huaizong Shao (M'15) received the M.S. degree in electrical engineering from Sichuan University, Chengdu, China, in 1998, and the Ph.D. degree in information and communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, in 2003. Since 2003, he has been with the School of Communication and Information Engineering, UESTC, where he is currently a Professor. From 2014 to 2015, he was a Visiting Scholar with The University of Sheffield, Sheffield, U.K. His research interests include communication and radar signal processing.



Wen-Qin Wang (M'08–SM'16) received the B.E. degree in electrical engineering from Shandong University, Jinan, China, in 2002, and the M.E. and Ph.D. degrees in information and communication engineering from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 2005 and 2010, respectively. From 2005 to 2007, he was with the National Key Laboratory of Microwave Imaging Technology, Chinese Academy of Sciences, Beijing, China. Since 2007, he has been with the School of Communication and Information Engineering, UESTC, where he is currently a Professor. From 2011 to 2012, he was a Visiting Scholar with the Stevens Institute of Technology, Hoboken, NJ, USA. From 2012 to 2013, he was a Hong Kong Scholar with the City University of Hong Kong, Hong Kong. From 2014 to 2016, he was a Marie Curie Fellow with Imperial College London, U.K. His research interests include communication and radar signal processing, and microwave imaging techniques. He was a recipient of the National Young Top-Notch Talent of the Ten-Thousand Talent Program Award, the Marie Curie International Incoming Fellowship, and the Hong Kong Scholar Fellowship. He is an editorial board member of four international journals.