AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

PLEASE NOTE: We cannot accept new source files as corrections for your article. If possible, please annotate the PDF proof we have sent you with your corrections and upload it via the Author Gateway. Alternatively, you may send us your corrections in list format. You may also upload revised graphics via the Author Gateway.

AQ:1 = Please confirm or add details for any funding or financial support for the research of this article.

AQ:2 = Please provide the department name for Queen's University Belfast where the authors Tiep M. Hoang and Trung Q. Duong are currently affiliated with.

AQ:3 = Please confirm the postal code for University of Technology Sydney.

AQ:4 = Please provide the department name for University of Liverpool where the author Alan Marshall is currently affiliated with.

AQ:5 = Note that if you require corrections/changes to tables or figures, you must supply the revised files, as these items are not edited for you.

AQ:6 = Please provide the publisher location for Ref. [28].

Security and Energy Harvesting for MIMO-OFDM Networks

Tiep M. Hoang, Ahmed El Shafie, *Senior Member, IEEE*, Daniel Benevides da Costa, *Senior Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, Hoang Duong Tuan, and Alan Marshall, *Senior Member, IEEE*

***Abstract*— We consider a multiple-input multiple-output (MIMO) orthogonal frequency-division multiplexing (OFDM) network in which a source node, Alice, communicates with an energy-harvesting destination node, Bob, in the presence of a passive eavesdropper. To secure the wireless transmission, Alice generates a hybrid artificial noise (AN) in both frequency and time domains. Moreover, in order to collect more energy, Bob splits the received signal power of the cyclic prefix of each OFDM block. We then propose two non-convex optimization problems to balance both the need for security and the need for harvesting energy at Bob. While one considers maximizing the secrecy rate, the other approach aims at maximizing the harvested energy. Path-following algorithms of low computational complexity are developed and evaluated. Our numerical results show the gain of our proposed scheme and the effectiveness of our proposed algorithms.**

***Index Terms*— MIMO, OFDM, SWIPT, security, energy harvesting, hybrid artificial noise, path-following algorithms.**

I. Introduction

OVER the past decade, wireless security has been widely investigated since wireless networks are vulnerable to passive eavesdropping [2]–[5]. Harvesting energy in secure wireless networks has also drawn the research community's attention recently [6]–[8]. Obviously, considering wireless security and energy-harvesting is generally more challenging than considering each problem separately [7], [9], [10].

Many works have examined the impact of secrecy parameters on the harvested energy and clarified the role of energy-harvesting parameters on the physical-layer security performance. For example, [11] considered a relaying network and then designed beamforming vector and time-switching (TS) coefficient to maximize secrecy rate subject to energy-related constraints. Moreover, [12] focused on minimizing the transmit power subject to rate-related constraints and considered power-splitting (PS) protocol instead of TS protocol. Using the TS protocol for energy-harvesting and using game theory to cope with jamming attacks, the authors of [13] evaluated the secure performance of a wireless secret key generation system. The results in [14] indicated that the secure performance of a relaying network would be improved by using a TS-based relaying protocol (instead of merely processing information). Both the TS and PS protocols were discussed in [15] with the emphasis on protecting a relaying network. Furthermore, security and energy-harvesting for orthogonal frequency-division multiplexing (OFDM) systems were also simultaneously studied in previous works [16]–[18]. However, the proposed systems in [16] and [18] were single-input single-output (SISO) systems, while [17] had to invoke a jammer to cope with information leakage. Moreover, the methodologies used in these works might not be extended to more general cases such as multiple-input multiple-output (MIMO). Having said that, the idea of using OFDM to simultaneously improve security level and received energy in these works is worth our consideration. For instance, [18] took advantage of cyclic prefix, which is one of the most characteristics of the OFDM technique, to improve the energy harvested at the intended energy-harvesting user. Apart from the linear energy-harvesting (EH) model, several non-linear EH models are studied in [19]–[21]. In [19], the authors maximize the sum throughput and the minimum individual throughput based on the constraints of time and power allocation. From a hardware design perspective, the authors in [20] and [21] consider power conversion/transmission efficiency in connection with EH circuits. Especially, the EH model in [21] includes the sensitivity and saturation threshold of EH circuits. Such non-linear EH models are relatively practical, but applying them to secure wireless systems is really challenging. To simplify the

AQ:1 Manuscript received May 3, 2019; revised September 18, 2019 and November 11, 2019; accepted December 21, 2019. This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22. This article was presented in part at the IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, Italy, 2018. The associate editor coordinating the review of this article and approving it for publication was L. Xiao. *(Corresponding author: Trung Q. Duong.)*

AQ:2 Tiep M. Hoang and Trung Q. Duong are with Queen's University Belfast, Belfast BT7 1NN, U.K. (e-mail: mhoang02@qub.ac.uk; trung.q.duong@qub.ac.uk).

Ahmed El Shafie is with Qualcomm Inc., San Diego, CA 92121 USA (e-mail: ahmed.salahelshafie@gmail.com).

Daniel Benevides da Costa is with the Department of Computer Engineering, Federal University of Ceara (UFC), Sobral 62010-560, Brazil (e-mail: danielbcosta@ieee.org).

AQ:3 Hoang Duong Tuan is with the School of Electrical and Data Engineering, University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: tuan.hoang@uts.edu.au).

AQ:4 Alan Marshall is with the University of Liverpool, Liverpool L69 3GJ, U.K. (e-mail: alan.marshall@liverpool.ac.uk).

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

Digital Object Identifier 10.1109/TCOMM.2019.2962436

analysis, we choose to use a linear EH model as in most of the existing works. Hence, the topic of non-linear EH models is out of the scope of our paper.

Among the aforementioned works, our paper is closely related to [18]. In [18], the authors considered a SISO-OFDM simultaneous wireless information and power transfer (SWIPT) in the presence of a passive eavesdropper. As an extension of [18] to the MIMO case, this work considers a MIMO-OFDM SWPIT system. Noticeably, [18] suggests a non-convex problem for the trade-off between information security and energy-harvesting, but cannot solve it through any analytical methodology. In other words, the approach in [18] is unable to apply to similar works. In contrast, this paper provides a computational framework for resolving non-convex problems relating to the trade-off between security and energy-harvesting. Following that, we face the challenges in transforming non-convex problems into convex approximation ones[1]. More specifically, to address these non-convex optimization problems, we develop path-following iterative algorithms, which iteratively improve feasible points for the original non-convex problems. Thereby, we obtain at least a sub-optimal solution to each of the proposed problems. It should also be noted that this paper simultaneously discusses the frequency-domain artificial noise (freq. AN) design and the time-domain artificial noise (temporal AN) design. This type of hybrid AN was out of the scope of [11], [12], [14], [16]–[18], [22]. Although the hybrid AN design was proposed in [23], the topic of energy-harvesting was not considered. On the contrary, we take into account security and energy-harvesting, then resolving the trade-off problem between these two aspects. Our contributions can be summarized as follows:

- We propose a secure MIMO-OFDM SWIPT scheme in which the source node, Alice, employs a hybrid AN strategy to guarantee secure transmissions. In addition, a legitimate destination employs energy-harvesting circuitry to gather energy (see Fig. 1). We turn the process of removing the cyclic prefix into the process of harvesting energy, thereby improving the amount of achievable energy at the intended user.
- We consider two different optimization approaches. First, we maximize the secrecy rate of the system subject to the constraints of energy. Second, we maximize the harvested-energy rate at the legitimate energy-harvesting receiver subject to security constraints. As previously mentioned, we handle non-convex optimization problems by developing path-following algorithms to reach at least sub-optimal solutions.
- We quantitatively evaluate the system performance in terms of security and energy-harvesting, respectively. Through numerical results, the impact of system parameters is evaluated.

The remainder of this paper is organized as follows: Section II presents the system model and the specific setups at transceivers. Section III presents achievable secrecy rate and its lower bound. In Section IV, the total amount of harvested energy and its lower bound are derived. The two different maximization problems (i.e., maximizing the achievable secrecy rate and maximizing the harvested energy) are suggested in Section V. The numerical results and conclusions are provided in Sections VI and VII, respectively.

[1]As aforementioned, the SISO-OFDM in [18] does not provide any framework to transform non-convex problems into convex programming problems and thus, its approach fails to deal with the MIMO-OFDM case.

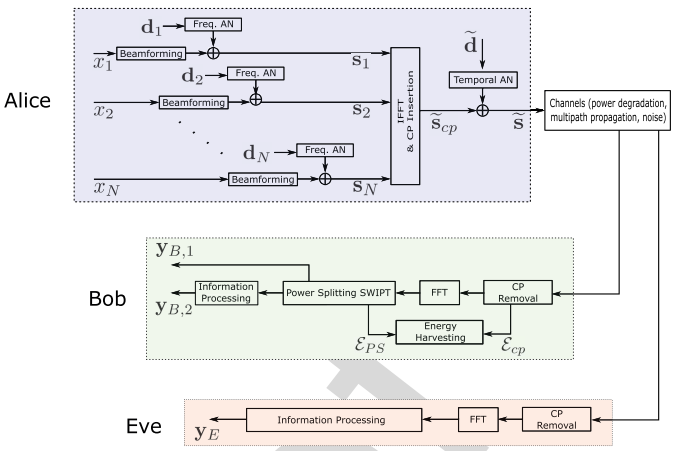

Fig. 1. System model.

Notation: $\mathbb{C}^{m\times n}$ denotes the set of all complex matrices of size m-by-n. $\Re\{\cdot\}$ and $\Im\{\cdot\}$ denote the real and imaginary parts of a complex number. $[\cdot]_{m,n}$ denotes the (m,n)th entry of a matrix. $(\cdot)^*$, $(\cdot)^\top$ and $(\cdot)^\dagger$ denote the conjugate, transpose and Hermitian operators, respectively. $\mathrm{trace}\{\cdot\}$ denotes the sum of the diagonal entries of a matrix. $(\mathbf{A})^\perp$ is an orthonormal basis for the null space of some matrix $\mathbf{A}$, i.e., $\mathbf{A}(\mathbf{A})^\perp = \mathbf{0}$. $\|.\|$ denotes the Euclidean norm of a vector. The expectation is denoted by $\mathbb{E}\{\cdot\}$. $\mathbf{z} \sim \mathcal{CN}_n(\mathbf{0}, \mathbf{\Sigma})$ denotes a complex Gaussian random vector $\mathbf{z} \in \mathbb{C}^{n\times 1}$ with mean $\mathbf{0}$ and covariance matrix $\mathbf{\Sigma} \in \mathbb{C}^{n\times n}$. Moreover, $z \sim \mathcal{CN}(0, \sigma^2)$ denotes a complex Gaussian random variable with zero-mean and covariance σ^2. $\mathrm{blkdiag}\{\cdot\}$ denotes a block diagonal matrix with its diagonal elements being matrices. The operator $\mathrm{resize}ij\{\mathbf{a}\}$ resizes the vector $\mathbf{a} = [a_1, \ldots, a_i, \ldots, a_j, \ldots, a_M]$ to the vector $\mathbf{a}' = [a_i, \ldots, a_j]$.

II. System Model

In this section, we respectively present the system model and the specific setups at all nodes. The considered system consists of one source node (Alice), one energy-harvesting node (Bob), and one eavesdropper (Eve). Alice first converts the frequency-domain signals into the time-domain signals using an N-point *inverse fast Fourier transform* (IFFT), and then inserts a cyclic prefix (CP) of N_{cp} length into the beginning of each OFDM block. Let N_{A}, N_{B} and N_{E} be the number of antennas at Alice, Bob and Eve, respectively.

A. The Injection of Freq. AN and Temporal AN at Alice

Let $\mathbf{a}_n \in \mathbb{C}^{N_{\mathrm{A}}\times 1}$ and $\mathbf{B}_n$ be, respectively, the beamforming vector of subcarrier n and the frequency-domain AN precoding matrix of subcarrier n. The frequency-domain symbol vector, corresponding to the nth subcarrier, can be written as

$$\mathbf{s}_n = \mathbf{a}_n x_n + \mathbf{B}_n \mathbf{d}_n,$$

where $x_n \in \mathbb{C}$ is the frequency-domain symbol and $\mathbf{d}_n$ is the injected *freq.* AN vector. To maximize the interference at Eve, $\mathbf{d}_n$ is generated to be independent of $\mathbf{d}_m$ if $n \neq m$. Moreover, each entry in $\mathbf{d}_n$ is a complex Gaussian random variable with zero mean and covariance σ^2. The size of $\mathbf{B}_n$ and that of $\mathbf{d}_n$ will be determined later in Section II-D; however, the product $\mathbf{B}_n\mathbf{d}_n$ must be a vector, which lies in $\mathbb{C}^{N_{\mathrm{A}}\times 1}$.

As such, the frequency-domain symbol vector over all subcarriers can be written as

$$\mathbf{s} \triangleq \left[\mathbf{s}_1^\top, \mathbf{s}_2^\top, \ldots, \mathbf{s}_N^\top\right]^\top = \mathbf{X}\mathbf{a} + \mathbf{B}\mathbf{d} \tag{1}$$

where

$$\mathbf{X} = \mathrm{blkdiag}\left\{\mathbf{I}_{N_{\mathrm{A}}}x_1, \mathbf{I}_{N_{\mathrm{A}}}x_2, \ldots, \mathbf{I}_{N_{\mathrm{A}}}x_N\right\},$$
$$\mathbf{a} = \left[\mathbf{a}_1^\top, \mathbf{a}_2^\top, \ldots, \mathbf{a}_N^\top\right]^\top$$
$$\mathbf{B} = \mathrm{blkdiag}\left\{\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_N\right\}, \tag{2}$$
$$\mathbf{d} = \left[\mathbf{d}_1^\top, \mathbf{d}_2^\top, \ldots, \mathbf{d}_N^\top\right]^\top. \tag{3}$$

Remark 1: The covariance matrix of $\mathbf{s}$ *can be calculated as*:

$$\begin{aligned}\mathbb{E}\left\{\mathbf{s}\mathbf{s}^\dagger\right\} &= \mathbb{E}\left\{\mathbf{X}\mathbf{a}\mathbf{a}^\dagger\mathbf{X}^\dagger\right\} + \mathbb{E}\left\{\mathbf{B}\mathbf{d}\mathbf{d}^\dagger\mathbf{B}^\dagger\right\} \\ &= \sigma_0^2 \mathrm{blkdiag}\left\{\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_N\right\} + \sigma^2\mathbf{B}\mathbf{B}^\dagger \end{aligned} \tag{4}$$

where $\mathbf{W}_n \triangleq \mathbf{w}_n\mathbf{w}_n^\dagger$, $\mathbf{w}_n \triangleq \sqrt{\frac{p_n}{\sigma_0^2}}\mathbf{a}_n$ *and* $p_n \triangleq \mathbb{E}\left\{|x_n|^2\right\}$. *Note that* σ_0^2 *is a constant, which is used to adjust the range of the ratio* (p_n/σ_0^2).

In order to convert the array $\{\mathbf{s}_n\}_{n=1,\ldots,N}$ into the time-domain signal, Alice uses the IFFT matrix $\mathbf{F}_{\mathrm{A}}^\dagger = \left(\mathbf{F}^\dagger \otimes \mathbf{I}_{N_{\mathrm{A}}}\right) \in \mathbb{C}^{N_{\mathrm{A}}N\times N_{\mathrm{A}}N}$ with $\mathbf{F} \in \mathbb{C}^{N\times N}$. Note that the (p,q)th element of $\mathbf{F} \in \mathbb{C}^{N\times N}$ takes the value of $[\mathbf{F}]_{p,q} = \sqrt{(1/N)}\exp\left(-j2\pi pq/N\right)$. After the conversion, Alice inserts a CP of N_{cp} samples into the beginning of that IFFT signal by using the following CP insertion matrix:

$$\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}} = \left[\left[\mathbf{0}_{N_{\mathrm{A}}N_{\mathrm{cp}}\times N_{\mathrm{A}}(N-N_{\mathrm{cp}})}, \mathbf{I}_{N_{\mathrm{A}}N_{\mathrm{cp}}}\right]^\top, \mathbf{I}_{N_{\mathrm{A}}N}\right]^\top.$$

As such, the transmitted signal in the time domain can be expressed as:

$$\widetilde{\mathbf{s}}^{\mathrm{cp}} = \mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{s}. \tag{5}$$

Let $\widetilde{\mathbf{d}}$ be the injected *temporal* AN vector, and let $\mathbf{Q}$ be the temporal AN precoding matrix. By adding $\widetilde{\mathbf{s}}^{\mathrm{cp}}$ and $\mathbf{Q}\widetilde{\mathbf{d}}$, we obtain the transmitted signal in the time domain, i.e.,

$$\widetilde{\mathbf{s}} = \widetilde{\mathbf{s}}^{\mathrm{cp}} + \mathbf{Q}\widetilde{\mathbf{d}} = \mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{s} + \mathbf{Q}\widetilde{\mathbf{d}}. \tag{6}$$

Note that the size of $\mathbf{Q}$ and the size of $\widetilde{\mathbf{d}}$ will be determined later in Section II-D. However, each entry of the vector $\widetilde{\mathbf{d}}$ will be assumed to obey $\mathcal{CN}\left(0, \widetilde{\sigma}^2\right)$.

Remark 2: The covariance matrix of the time-domain signal $\widetilde{\mathbf{s}}$ *can be calculated as*:

$$\begin{aligned}\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\} &= \mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\left(\sigma_0^2\mathbf{w}\mathbf{w}^\dagger + \sigma^2\mathbf{B}\mathbf{B}^\dagger\right)\mathbf{F}_A(\mathbf{T}_A^{cp})^\dagger + \widetilde{\sigma}^2\mathbf{Q}\mathbf{Q}^\dagger \\ &= \sigma_0^2\left[\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\mathbf{w}^\dagger\mathbf{F}_A(\mathbf{T}_A^{cp})^\dagger + \mathbf{\Lambda}\right] \end{aligned} \tag{7}$$

where

$$\mathbf{\Lambda} = \left(\sigma^2/\sigma_0^2\right)\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{B}\mathbf{B}^\dagger\mathbf{F}_A(\mathbf{T}_A^{cp})^\dagger + \left(\widetilde{\sigma}^2/\sigma_0^2\right)\mathbf{Q}\mathbf{Q}^\dagger$$

and

$$\mathbf{w} \triangleq \left[\mathbf{w}_1^\top, \ldots, \mathbf{w}_N^\top\right]^\top.$$

Then, the average power of the time-domain signal $\widetilde{\mathbf{s}}$ *is*

$$\begin{aligned}\mathbb{E}\left\{\|\widetilde{\mathbf{s}}\|^2\right\} &= \mathrm{trace}\left\{\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\}\right\} \\ &= \sigma_0^2\ \mathrm{trace}\left\{\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\mathbf{w}^\dagger\mathbf{F}_A\left(\mathbf{T}_A^{cp}\right)^\dagger + \mathbf{\Lambda}\right\} \\ &= \sigma_0^2\left[\left\|\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\right\|^2 + \mathrm{trace}\left\{\mathbf{\Lambda}\right\}\right]. \end{aligned} \tag{8}$$

Denote P_A *as the power budget of Alice. A power constraint is imposed on the signal* $\widetilde{\mathbf{s}}$ *as follows*:

$$\mathbb{E}\left\{\|\widetilde{\mathbf{s}}\|^2\right\} \leq P_A \Leftrightarrow \left\|\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\right\|^2 \leq \tfrac{P_A}{\sigma_0^2} - \mathrm{trace}\left\{\mathbf{\Lambda}\right\}. \tag{9}$$

B. Information Processing at Eve

Eve first removes the CP from her received time-domain OFDM signal by multiplying by the following CP removal matrix:

$$\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}} = \left[\mathbf{0}_{N_{\mathrm{E}}N\times N_{\mathrm{E}}N_{\mathrm{cp}}}, \mathbf{I}_{N_{\mathrm{E}}N}\right].$$

Then, a FFT algorithm is applied to convert the time-domain signals to the frequency-domain signals. This FFT algorithm is performed by multiplying the FFT matrix $\mathbf{F}_{\mathrm{E}} = (\mathbf{F} \otimes \mathbf{I}_{N_{\mathrm{E}}}) \in \mathbb{C}^{N_{\mathrm{E}}N\times N_{\mathrm{E}}N}$. As such, the frequency-domain received signal at Eve can be given by

$$\begin{aligned}\mathbf{y}_E &= \mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{EA}}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}} + \mathbf{F}_{\mathrm{E}}\widetilde{\mathbf{z}}_E \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{s} \\ &\quad + \sqrt{\beta_{\mathrm{EA}}}\mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \mathbf{F}_{\mathrm{E}}\widetilde{\mathbf{z}}_E \end{aligned} \tag{10}$$

where β_{EA} represents the impact of the large-scale fading, $\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}} \in \mathbb{C}^{N_{\mathrm{E}}(N+N_{\mathrm{cp}})\times N_{\mathrm{A}}(N+N_{\mathrm{cp}})}$ represents the small-scale fading, and $\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}$ represents the time-domain *channel impulse response* (CIR) matrix of the Eve-Alice link. Meanwhile, $\widetilde{\mathbf{z}}_E \in \mathbb{C}^{N_{\mathrm{E}}N\times 1}$ is the additive white Gaussian noise (AWGN) vector with each element distributed as $\mathcal{CN}\left(0, \sigma_0^2\right)$.

We assume that there are $L_{\mathrm{EA}} = L$ paths between Eve and Alice. Note that the multi-path delay spread is equal to $(L-1)$. In order to avoid inter-block interference at a legitimate user, it is required that the CP length is larger or equal to the multi-path delay spread, i.e., $N_{\mathrm{cp}} \geq L-1$. Also note that Alice is not aware of the Eve's presence; thus, the setting $N_{\mathrm{cp}} \geq L-1$ is not originally intended for Eve, but rather for Bob. In practice, N_{cp} is often assigned some fairly large number so that it will be able to cover most channels.

For the lth ($l \in \{0, 2, \ldots, L-1\}$) path between Eve and Alice, we denote $\mathbf{G}_{\mathrm{EA}_l} \in \mathbb{C}^{N_{\mathrm{E}}\times N_{\mathrm{A}}}$ be the time-domain fading channel matrix. According to [24], [25], $\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}$ is a block *circulant* matrix and takes the following form:

$$\begin{bmatrix} \mathbf{G}_{\mathrm{EA}_1} & \ldots & \mathcal{O}_{\mathrm{EA}} & \mathcal{O}_{\mathrm{EA}} & \ldots & \mathbf{G}_{\mathrm{EA}_2} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{G}_{\mathrm{EA}_L} & \ldots & \mathbf{G}_{\mathrm{EA}_1} & \mathcal{O}_{\mathrm{EA}} & \ldots & \mathcal{O}_{\mathrm{EA}} \\ \mathcal{O}_{\mathrm{EA}} & \ldots & \mathbf{G}_{\mathrm{EA}_2} & \mathbf{G}_{\mathrm{EA}_1} & \ldots & \mathcal{O}_{\mathrm{EA}} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathcal{O}_{\mathrm{EA}} & \ldots & \mathcal{O}_{\mathrm{EA}} & \mathcal{O}_{\mathrm{EA}} & \ldots & \mathbf{G}_{\mathrm{EA}_1} \end{bmatrix}$$

where $\mathcal{O}_{\mathrm{EA}} \triangleq \mathbf{0}_{N_{\mathrm{E}}\times N_{\mathrm{A}}}$.

Defining $\mathbf{H}_{\mathrm{EA}} \triangleq \mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^{\dagger}$ and using the property of a circulant matrix,[2] we can express $\mathbf{H}_{\mathrm{EA}} \in \mathbb{C}^{N_{\mathrm{E}}N \times N_{\mathrm{A}}N}$ as a block-diagonal matrix, i.e.,

$$\mathbf{H}_{\mathrm{EA}} = \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{EA}_1}, \ldots, \mathbf{H}_{\mathrm{EA}_n}, \ldots, \mathbf{H}_{\mathrm{EA}_N}\right\} \quad (11)$$

where $\mathbf{H}_{\mathrm{EA}_n} = \sum_{l=1}^{L} \mathbf{G}_{\mathrm{EA}_l} e^{-j2\pi n(l-1)/N}$ represents the *frequency response* of the Eve-Alice link at the nth subcarrier. Finally, (10) is rewritten as:

$$\begin{aligned}\mathbf{y}_E &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\mathbf{s} + \mathbf{F}_{\mathrm{E}}\left[\sqrt{\beta_{\mathrm{EA}}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_E\right] \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\ \mathrm{diag}(\mathbf{a})\,[\,\underbrace{x_1, \ldots, x_1}_{N_{\mathrm{A}}\text{ elements}}, \ldots, \underbrace{x_N, \ldots, x_N}_{N_{\mathrm{A}}\text{ elements}}\,]^{\top} \\ &\quad + \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\mathbf{B}\mathbf{d} + \mathbf{F}_{\mathrm{E}}\left[\sqrt{\beta_{\mathrm{EA}}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_E\right].\end{aligned} \quad (12)$$

Let $\mathbf{y}_{\mathrm{E}_n}$ be the nth subcarrier received signal. The elements in $\mathbf{y}_{\mathrm{E}_n}$ are also the entries in $\mathbf{y}_E$, beginning at index $(n-1)N_{\mathrm{E}}+1$ and ending at index nN_{E}. We have

$$\begin{aligned}\mathbf{y}_{\mathrm{E}_n} &= \mathrm{resize}(n-1)N_{\mathrm{E}} + 1nN_{\mathrm{E}}\{\mathbf{y}_E\} \\ &= \underbrace{\left[\mathbf{0}_{N_{\mathrm{E}}\times(n-1)N_{\mathrm{E}}}\ \mathbf{I}_{N_{\mathrm{E}}}\ \mathbf{0}_{N_{\mathrm{E}}\times(N-n)N_{\mathrm{E}}}\right]}_{\triangleq \mathbf{C}_{\mathrm{E}_n}}\mathbf{y}_E \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{C}_{\mathrm{E}_n}\mathbf{H}_{\mathrm{EA}}\left(\mathbf{X}\mathbf{a} + \mathbf{B}\mathbf{d}\right) \\ &\quad + \mathbf{C}_{\mathrm{E}_n}\mathbf{F}_{\mathrm{E}}\left[\sqrt{\beta_{\mathrm{EA}}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_E\right] \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}_n}\mathbf{a}_n x_n + \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}_n}\mathbf{B}_n\mathbf{d}_n \\ &\quad + \sqrt{\beta_{\mathrm{EA}}}\mathbf{C}_{\mathrm{E}_n}\mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \mathbf{C}_{\mathrm{E}_n}\mathbf{F}_{\mathrm{E}}\widetilde{\mathbf{z}}_E\end{aligned} \quad (13)$$

where the last equality is obtained by using block matrix multiplication to shorten the first term $\mathbf{C}_{\mathrm{E}_n}\mathbf{H}_{\mathrm{EA}}\mathbf{X}\mathbf{a}$ and the second term $\mathbf{C}_{\mathrm{E}_n}\mathbf{H}_{\mathrm{EA}}\mathbf{B}\mathbf{d}$.

C. Information Processing and Energy Harvesting at Bob

Similar to the previous sub-section, the channel between Alice and Bob is a MIMO frequency selective fading channel with L_{BA} paths. For simplicity, we also assume $L_{\mathrm{BA}} = L$. For the lth path between Bob and Alice, $\mathbf{G}_{\mathrm{BA}_l} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{A}}}$ is the time-domain fading channel matrix.

The employment of OFDM at Alice leads to the fact that each MIMO-OFDM transmission block can be viewed as N parallel frequency-domain MIMO channels. If Bob does not adopt any energy-harvesting scheme, the received frequency-domain signal at Bob (say $\mathbf{y}_{B,\varnothing}$) would be formulated exactly the same way we attained (10)–(12), i.e.,

$$\begin{aligned}\mathbf{y}_{B,\varnothing} &= \mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^{\dagger}\mathbf{s} \\ &\quad + \mathbf{F}_{\mathrm{B}}\left[\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},\varnothing}\right] \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\mathbf{s} + \mathbf{F}_{\mathrm{B}}\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},\varnothing}\right]\end{aligned} \quad (14)$$

where β_{BA} represents the impact of the large-scale fading, $\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}} \in \mathbb{C}^{N_{\mathrm{B}}(N+N_{\mathrm{cp}})\times N_{\mathrm{A}}(N+N_{\mathrm{cp}})}$ represents the small-scale fading, and $\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}$ represents the time-domain CIR matrix of the Bob-Alice link. In (14), $\widetilde{\mathbf{z}}_{\mathrm{B},\varnothing} \in \mathbb{C}^{N_{\mathrm{B}}N\times 1}$ is the AWGN vector with each element distributed as $\mathcal{CN}\left(0, \sigma_0^2\right)$, the CP removal matrix at Bob is $\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}} = \left[\mathbf{0}_{N_{\mathrm{B}}N\times N_{\mathrm{B}}N_{\mathrm{cp}}}, \mathbf{I}_{N_{\mathrm{B}}N}\right]$, and $\mathbf{H}_{\mathrm{BA}}$ is defined as

$$\begin{aligned}\mathbf{H}_{\mathrm{BA}} &\triangleq \mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^{\dagger} \\ &= \mathrm{blkdiag}\Big\{\mathbf{H}_{\mathrm{BA}_1}, \ldots, \mathbf{H}_{\mathrm{BA}_n}, \ldots, \mathbf{H}_{\mathrm{BA}_N}\Big\}\end{aligned} \quad (15)$$

with $\mathbf{H}_{\mathrm{BA}_n} = \sum_{l=1}^{L}\mathbf{G}_{\mathrm{BA}_l}e^{-j2\pi n(l-1)/N}$.

Bob is assumed to adopt the PS SWIPT scheme, the received signal $\mathbf{y}_{\mathrm{B}}$ will be derived in a slightly different way. Obviously, we have $\mathbf{y}_{\mathrm{B}} \neq \mathbf{y}_{B,\varnothing}$. A detailed description of information processing and energy-harvesting at Bob will be presented below.[3]

- The time duration of an OFDM block is divided into three smaller portions: the first portion is from 0 to $\tau^{\mathrm{cp}} = N_{\mathrm{cp}}\tau_s$, the second portion is from τ^{cp} to $\tau^{\mathrm{cp}} + K\tau_s$ (with $K \in \{1, \ldots, N\}$), and the remaining part is from $\tau^{\mathrm{cp}} + K\tau_s$ to the end of the OFDM block duration (i.e., $N\tau_s$). Herein, τ_s represents the sampling time (the sampling rate is thus equal to $1/\tau_s$).
- The first portion is to remove the CP from the received time-domain OFDM signal at Bob. In other words, the first $N_{\mathrm{B}}N_{\mathrm{cp}}$ elements of the vector $\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}}$ are not be treated as information elements and will not go through any information processing. Instead, these elements are employed for the purpose of harvesting energy. Thus, the energy harvested by Bob can be calculated as follows:

$$\mathcal{E}_{\mathrm{cp}} = \eta\tau^{\mathrm{cp}}\,\mathbb{E}\left\{\left\|\mathrm{resize}1N_{\mathrm{B}}N_{\mathrm{cp}}\left\{\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}}\right\}\right\|^2\right\} \quad (16)$$

  where $\eta \in [0,1]$ is the energy conversion efficiency of the energy-harvester circuit, and $\mathbf{C}^{\mathrm{cp}} \triangleq \left[\mathbf{I}_{N_{\mathrm{B}}N_{\mathrm{cp}}}\ \mathbf{0}_{N_{\mathrm{B}}N_{\mathrm{cp}}\times N_{\mathrm{B}}N}\right]$
- During the second portion, Bob uses the PS SWIPT scheme to decode information and harvest energy simultaneously. More specifically, the obtained signal is divided into two streams based on a PS coefficient $\rho \in (0,1]$. For information processing, the received power of one stream will be multiplied by the coefficient ρ. Given that the multiplication of the received power by ρ is equivalent to the multiplication of noise by $1/\rho$, we can express the received signal in the frequency domain (after the FFT operation) as follows:

$$\begin{aligned}&\mathbf{y}_{\mathrm{B},1} \\ &= \mathrm{resize}1N_{\mathrm{B}}K\left\{\mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}} + \frac{1}{\sqrt{\rho}}\mathbf{F}_{\mathrm{B}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\right\} \\ &= \mathbf{C}_1\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}} + \frac{1}{\sqrt{\rho}}\mathbf{F}_{\mathrm{B}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\right] \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{C}_1\mathbf{H}_{\mathrm{BA}}\mathbf{s} \\ &\quad + \mathbf{C}_1\mathbf{F}_{\mathrm{B}}\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \frac{1}{\sqrt{\rho}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\right]\end{aligned} \quad (17)$$

[2] If a square matrix $\mathbf{C}$ is circulant, then it can be diagonalized by the FFT matrix $\mathbf{F}$ and the IFFT matrix $\mathbf{F}^{\dagger}$, i.e., $\mathbf{F}\mathbf{C}\mathbf{F}^{\dagger}$ is a diagonal matrix [25].

[3] In [18], only SISO channels and temporal AN were discussed. In contrast, our work extends SISO channels to MIMO channels and yet, the injection of additional frequency-domain AN is also taken into account.

where $\mathbf{C}_1 \triangleq \left[\mathbf{I}_{N_\mathrm{B}K} \ \mathbf{0}_{N_\mathrm{B}K\times N_\mathrm{B}(N-K)}\right]$ and $\widetilde{\mathbf{z}}_{\mathrm{B},1} \in \mathbb{C}^{N_\mathrm{B}N\times 1}$ is the AWGN vector with each element distributed as $\mathcal{CN}\left(0,\sigma_0^2\right)$. In parallel, for energy-harvesting, the remaining stream will be transformed into energy. The harvested energy during this portion is given by

$$\mathcal{E}_{\mathrm{PS}} = \eta\left(K\tau_s\right)\left(1-\rho\right) \times \mathbb{E}\left\{\left\|\mathrm{resize}1N_\mathrm{B}K\left\{\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}}\right\}\right\|^2\right\}. \tag{18}$$

Different from $\mathbf{y}_{\mathrm{B},1}$ in (17), the term $\mathrm{resize}1N_\mathrm{B}K\left\{\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}}\right\}$ in (18) is the signal which does not go through information processing (thus, there is no noise term) as well as FFT operation.

- During the third/last portion, Bob processes the signal in the same way as Eve does. Given that there are $N_\mathrm{B}(N-K)$ samples left for this portion, the received signal from time $\tau_s + K\tau_s$ to time $N\tau_s$ can be written as:

$$\begin{aligned}\mathbf{y}_{\mathrm{B},2} &= \mathrm{resize}N_\mathrm{B}(K+1)N_\mathrm{B}N\Bigg\{\sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\mathbf{s} \\ &\quad + \mathbf{F}_\mathrm{B}\left(\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},2}\right)\Bigg\} \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{C}_2\mathbf{H}_{\mathrm{BA}}\mathbf{s} \\ &\quad + \mathbf{C}_2\mathbf{F}_\mathrm{B}\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},2}\right]\end{aligned} \tag{19}$$

where $\mathbf{C}_2 \triangleq \left[\mathbf{0}_{N_\mathrm{B}(N-K)\times N_\mathrm{B}K} \ \mathbf{I}_{N_\mathrm{B}(N-K)}\right]$ and $\widetilde{\mathbf{z}}_{\mathrm{B},2} \in \mathbb{C}^{N_\mathrm{B}N\times 1}$ is the AWGN vector with each element distributed as $\mathcal{CN}\left(0,\sigma_0^2\right)$.

In short, the received signal $\mathbf{y}_\mathrm{B} = \left[\mathbf{y}_{\mathrm{B},1}^\top, \mathbf{y}_{\mathrm{B},2}^\top\right]^\top$ at Bob can be given by

$$\begin{aligned}\mathbf{y}_\mathrm{B} &= \begin{bmatrix}\mathbf{C}_1\\ \mathbf{C}_2\end{bmatrix}\sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\left(\mathbf{X}\mathbf{a}+\mathbf{B}\mathbf{d}\right) \\ &\quad + \begin{bmatrix}\mathbf{C}_1\\ \mathbf{C}_2\end{bmatrix}\mathbf{F}_\mathrm{B}\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{Q}\widetilde{\mathbf{d}} \\ &\quad + \begin{bmatrix}\mathbf{C}_1\mathbf{F}_\mathrm{B} & \mathbf{0}_{N_\mathrm{B}K\times N_\mathrm{B}N}\\ \mathbf{0}_{N_\mathrm{B}(N-K)\times N_\mathrm{B}N} & \mathbf{C}_2\mathbf{F}_\mathrm{B}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{\rho}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\\ \widetilde{\mathbf{z}}_{\mathrm{B},2}\end{bmatrix} \\ &\overset{(a)}{=} \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\left(\mathbf{X}\mathbf{a}+\mathbf{B}\mathbf{d}\right) \\ &\quad + \sqrt{\beta_{\mathrm{BA}}}\mathbf{F}_\mathrm{B}\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B}\end{aligned} \tag{20}$$

where (a) is obtained by defining

$$\mathbf{C}_{\mathrm{BA}} \triangleq \begin{bmatrix}\mathbf{C}_1\mathbf{F}_\mathrm{B} & \mathbf{0}_{N_\mathrm{B}K\times N_\mathrm{B}N}\\ \mathbf{0}_{N_\mathrm{B}(N-K)\times N_\mathrm{B}N} & \mathbf{C}_2\mathbf{F}_\mathrm{B}\end{bmatrix},$$

$$\widetilde{\mathbf{z}}_\mathrm{B} \triangleq \begin{bmatrix}\frac{1}{\sqrt{\rho}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\\ \widetilde{\mathbf{z}}_{\mathrm{B},2}\end{bmatrix} \sim \mathcal{CN}_{2\ N_\mathrm{B}N}\left(\mathbf{0},\mathbf{J}\right)$$

$$\text{with } \mathbf{J} = \begin{bmatrix}(1/\rho)\sigma_0^2\mathbf{I}_{N_\mathrm{B}N} & \mathbf{0}_{N_\mathrm{B}N}\\ \mathbf{0}_{N_\mathrm{B}N} & \sigma_0^2\mathbf{I}_{N_\mathrm{B}N}\end{bmatrix},$$

and using the fact that $\begin{bmatrix}\mathbf{C}_1\\ \mathbf{C}_2\end{bmatrix} \equiv \mathbf{I}_{N_\mathrm{B}N}$. The covariance matrix of $\mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B}$ can be calculated as follows:

$$\begin{aligned}\mathbf{C}_{\mathrm{BA}}\mathbf{J}\mathbf{C}_{\mathrm{BA}}^\dagger &= \begin{bmatrix}(1/\rho)\sigma_0^2\mathbf{C}_1\mathbf{F}_\mathrm{B}\mathbf{F}_\mathrm{B}^\dagger\mathbf{C}_1^\dagger & \mathbf{0}\\ \mathbf{0} & \sigma_0^2\mathbf{C}_2\mathbf{F}_\mathrm{B}\mathbf{F}_\mathrm{B}^\dagger\mathbf{C}_2^\dagger\end{bmatrix} \\ &= \begin{bmatrix}(1/\rho)\sigma_0^2\mathbf{I}_{N_\mathrm{B}K} & \mathbf{0}\\ \mathbf{0} & \sigma_0^2\mathbf{I}_{N_\mathrm{B}(N-K)}\end{bmatrix}\end{aligned} \tag{21}$$

where the last equality follows that $\mathbf{F}_\mathrm{B}\mathbf{F}_\mathrm{B}^\dagger = \mathbf{I}_{N_\mathrm{B}N}$, $\mathbf{C}_1\mathbf{C}_1^\dagger = \mathbf{I}_{N_\mathrm{B}K}$ and $\mathbf{C}_2\mathbf{C}_2^\dagger = \mathbf{I}_{N_\mathrm{B}(N-K)}$.

Let $\mathbf{y}_{\mathrm{B}_n}$ be the nth subcarrier received signal. We have

$$\begin{aligned}\mathbf{y}_{\mathrm{B}_n} &= \mathrm{resize}(n-1)N_\mathrm{B} + 1nN_\mathrm{B}\left\{\mathbf{y}_\mathrm{B}\right\} \\ &= \underbrace{\left[\mathbf{0}_{N_\mathrm{B}\times(n-1)N_\mathrm{B}} \ \mathbf{I}_{N_\mathrm{B}} \ \mathbf{0}_{N_\mathrm{B}\times(N-n)N_\mathrm{B}}\right]}_{\triangleq\mathbf{C}_{\mathrm{B}_n}}\mathbf{y}_\mathrm{B} \\ &= \mathbf{C}_{\mathrm{B}_n}\mathbf{y}_\mathrm{B}.\end{aligned} \tag{22}$$

D. AN Design at Alice to Cancel Interference at Bob

As seen in (20), the presence of AN terms $\mathbf{d}$ and $\widetilde{\mathbf{d}}$ causes interference at Bob. To cancel the interference, Alice can design $\mathbf{B}$ and $\mathbf{Q}$ subject to

$$\begin{cases}\mathbf{H}_{\mathrm{BA}}\mathbf{B} &= \mathbf{0}\\ \mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q} &= \mathbf{0}.\end{cases} \tag{23}$$

Using (2) and (15), we can find out the solution $\mathbf{B}$ to the equation $\mathbf{H}_{\mathrm{BA}}\mathbf{B} = \mathbf{0}$ as follows:

$$\begin{aligned}\mathbf{H}_{\mathrm{BA}}\mathbf{B} = \mathbf{0} &\Leftrightarrow \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{BA}_1}\mathbf{B}_1,\ldots,\mathbf{H}_{\mathrm{BA}_N}\mathbf{B}_N\right\} = \mathbf{0} \\ &\Leftrightarrow \mathbf{B}_n = \mathbf{H}_{\mathrm{BA}_n}^\perp,\ \forall n\in\{1,\ldots,N\}.\end{aligned} \tag{24}$$

Now it is obvious that $\mathbf{B} = \mathrm{blkdiag}\left\{\mathbf{B}_1,\ldots,\mathbf{B}_N\right\} = \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{BA}_1}^\perp,\ldots,\mathbf{H}_{\mathrm{BA}_N}^\perp\right\}$ is a matrix with $N_\mathrm{A}N$ rows and $(N_\mathrm{A}-N_\mathrm{B})N$ columns due to $\mathbf{B}_n \in \mathbb{C}^{N_\mathrm{A}\times(N_\mathrm{A}-N_\mathrm{B})}$. The existence of $\mathbf{B}$, in general, depends on the existence of all elements $\{\mathbf{B}_n\}_{n=1}^N$. Each $\mathbf{B}_n$ exists if and only if its second dimension is positive, i.e.,

$$N_\mathrm{A} - N_\mathrm{B} > 0 \Leftrightarrow N_\mathrm{B} < N_\mathrm{A}. \tag{25}$$

Likewise, we deduce $\mathbf{Q} \in \mathbb{C}^{N_\mathrm{A}(N+N_{\mathrm{cp}})\times(N_\mathrm{A}(N+N_{\mathrm{cp}})-r)}$ with $r = \mathrm{rank}\left(\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right) = \min\{N_\mathrm{B}N, N_\mathrm{A}(N+N_{\mathrm{cp}})\}$. For the existence of $\mathbf{Q}$, it is required to have the condition $N_\mathrm{A}(N+N_{\mathrm{cp}})-r>0$, which leads to

$$r = N_\mathrm{B}N \Leftrightarrow N_\mathrm{B}N < N_\mathrm{A}(N+N_{\mathrm{cp}}). \tag{26}$$

Note that once (25) has been satisfied, (26) will be satisfied as well. Thus, the case of $N_\mathrm{A} > N_\mathrm{B}$ is taken into account in this paper. Then, we will be able to design $\mathbf{B}_n \in \mathbb{C}^{N_\mathrm{A}\times(N_\mathrm{A}-N_\mathrm{B})}$, $\mathbf{d}_n \in \mathbb{C}^{(N_\mathrm{A}-N_\mathrm{B})\times 1}$, $\mathbf{Q} \in \mathbb{C}^{N_\mathrm{A}(N+N_{\mathrm{cp}})\times(N_\mathrm{A}(N+N_{\mathrm{cp}})-N_\mathrm{B}N)}$ and $\widetilde{\mathbf{d}} \in \mathbb{C}^{(N_\mathrm{A}(N+N_{\mathrm{cp}})-N_\mathrm{B}N)\times 1}$.

Substituting (23) into (20) and (22), we can rewrite

$$\begin{aligned}\mathbf{y}_\mathrm{B} &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\mathbf{X}\mathbf{a} + \mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B} \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\ \mathrm{diag}\left(\mathbf{a}\right)\big[\underbrace{x_1,\ldots,x_1}_{N_\mathrm{A}\text{ elements}},\ldots,\underbrace{x_N,\ldots,x_N}_{N_\mathrm{A}\text{ elements}}\big]^\top \\ &\quad + \mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B}\end{aligned} \tag{27}$$

TABLE I
A TABLE OF FREQUENTLY-USED SYMBOLS

Parameters	Physical Meanings
$\mathbf{G}_{\mathrm{BA}_{l_\mathrm{B}}} \in \mathbb{C}^{N_\mathrm{B}\times N_\mathrm{A}}$	The *time-domain* fading channel matrix corresponding to the l_Bth path between Bob and Alice, for given $l_\mathrm{B} \in \{1,\ldots,L_\mathrm{BA}\}$.
$\mathbf{G}_{\mathrm{EA}_{l_\mathrm{E}}} \in \mathbb{C}^{N_\mathrm{E}\times N_\mathrm{A}}$	The *time-domain* fading channel matrix corresponding to the lth path between Eve and Alice, for given $l_\mathrm{E} \in \{1,\ldots,L_\mathrm{EA}\}$.
$\mathbf{H}_{\mathrm{BA}_n} = \sum_{l=0}^{L_\mathrm{BA}} \mathbf{G}_{\mathrm{BA}_l} e^{-j2\pi\frac{nl}{N}}$	The *frequency response* of the Bob-Alice link at the nth subcarrier, for given $n \in \{1,\ldots,N\}$.
$\mathbf{H}_{\mathrm{EA}_n} = \sum_{l=0}^{L_\mathrm{EA}} \mathbf{G}_{\mathrm{EA}_l} e^{-j2\pi\frac{nl}{N}}$	The *frequency response* of the Eve-Alice link at the nth subcarrier, for given $n \in \{1,\ldots,N\}$.
N_cp	The CP length. To prevent Bob from being affected by inter-block interference, it is required to have $N_\mathrm{cp} \geq L_\mathrm{BA}-1$.
$\mathbf{T}_\mathrm{A}^\mathrm{cp}$	The CP insertion matrix at Alice.
$\mathbf{R}_\mathrm{B}^\mathrm{cp}$ and $\mathbf{R}_\mathrm{E}^\mathrm{cp}$	The CP removal matrices at Bob and at Eve, respectively.
$\mathbf{F}_\mathrm{A}^\dagger = \left(\mathbf{F}^\dagger \otimes \mathbf{I}_{N_\mathrm{A}}\right)$	The N-point IFFT matrix at Alice.
$\mathbf{F}_\mathrm{B} = \left(\mathbf{F} \otimes \mathbf{I}_{N_\mathrm{B}}\right)$	The N-point FFT matrix at Bob.
$\mathbf{F}_\mathrm{E} = \left(\mathbf{F} \otimes \mathbf{I}_{N_\mathrm{E}}\right)$	The N-point FFT matrix at Eve.
$\mathbf{a}_n \in \mathbb{C}^{N_\mathrm{A}\times 1}$	The beamforming vector corresponding to subcarrier n.
$\mathbf{B}_n = \mathbf{H}_{\mathrm{BA}_n}^\perp$	The frequency-domain AN precoding matrix corresponding to subcarrier n.
$\mathbf{d}_n \in \mathbb{C}^{(N_\mathrm{A}-N_\mathrm{B})\times 1}$	The injected frequency-domain AN vector corresponding to subcarrier n. Each entry obeys $\mathcal{CN}\left(0,\sigma^2\right)$.
$\mathbf{Q} = \left(\mathbf{R}_\mathrm{B}^\mathrm{cp}\widetilde{\mathbf{H}}_\mathrm{BA}^\mathrm{cp}\right)^\perp$	The temporal AN precoding matrix.
$\widetilde{\mathbf{d}} \in \mathbb{C}^{(N_\mathrm{A}(N+N_\mathrm{cp})-N_\mathrm{B}N)\times 1}$	The temporal AN vector. Each entry obeys $\mathcal{CN}\left(0,\widetilde{\sigma}^2\right)$.

and

$$\begin{aligned}\mathbf{y}_{\mathrm{B}_n} &= \sqrt{\beta_\mathrm{BA}}\mathbf{C}_{\mathrm{B}_n}\mathbf{H}_\mathrm{BA}\mathbf{X}\mathbf{a} + \mathbf{C}_{\mathrm{B}_n}\mathbf{C}_\mathrm{BA}\widetilde{\mathbf{z}}_\mathrm{B}\\ &\overset{(a)}{=} \sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\mathbf{a}_n x_n + \mathbf{C}_{\mathrm{B}_n}\mathbf{C}_\mathrm{BA}\widetilde{\mathbf{z}}_\mathrm{B} \qquad (28)\end{aligned}$$

where (a) is obtained by using block matrix multiplication to calculate the product $\mathbf{C}_{\mathrm{B}_n}\mathbf{H}_\mathrm{BA}\mathbf{X}\mathbf{a}$. The covariance matrix of $\mathbf{C}_{\mathrm{B}_n}\mathbf{C}_\mathrm{BA}\widetilde{\mathbf{z}}_\mathrm{B}$ can be calculated as:

$$\begin{aligned}&\mathbf{C}_{\mathrm{B}_n}\left(\mathbf{C}_\mathrm{BA}\mathbf{J}\mathbf{C}_\mathrm{BA}^\dagger\right)\mathbf{C}_{\mathrm{B}_n}^\dagger = (1/\varrho_n)\sigma_0^2\mathbf{I}_{N_\mathrm{B}}\\ &\text{where } \varrho_n = \begin{cases}\rho & \text{if } 1\leq n\leq K\\ 1 & \text{if } K+1\leq n\leq N\end{cases}. \qquad (29)\end{aligned}$$

For readability, we present a table of symbols, Table I, at the top of the next page.

III. ACHIEVABLE SECRECY RATE

In this section, we formulate the achievable secrecy rate, which is the lower-bound of the capacity difference between the Bob-Alice link and the Eve-Alice link.

A. Mutual Information Between Bob and Alice

Let $\mathcal{I}_{\mathrm{BA}_n}\left(\mathbf{y}_{\mathrm{B}_n};x_n\right)$ (or simply $\mathcal{I}_{\mathrm{BA}_n}$) be the mutual information of the nth MIMO-OFDM subcarrier between Bob and Alice. From (28), $\mathcal{I}_{\mathrm{BA}_n}\left(\mathbf{y}_{\mathrm{B}_n};x_n\right)$ (in nats/OFDM block) can be expressed as [26]:

$$\begin{aligned}&\mathcal{I}_{\mathrm{BA}_n}\left(\mathbf{y}_{\mathrm{B}_n};x_n\right) \equiv \mathcal{I}_{\mathrm{BA}_n}\\ &= \ln\det\Bigg(\mathbf{I}_{N_\mathrm{B}} + \left(\sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\right)\mathbf{a}_n\,\mathbb{E}\left\{|x_n|^2\right\}\mathbf{a}_n^\dagger\\ &\quad\times\left(\sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\right)^\dagger\left(\frac{\sigma_0^2}{\varrho_n}\mathbf{I}_{N_\mathrm{B}}\right)^{-1}\Bigg)\\ &= \ln\left(1+\frac{\left\|\sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\mathbf{w}_n\right\|^2}{(1/\varrho_n)}\right) \qquad (30)\end{aligned}$$

where $\mathbf{w}_n \triangleq \sqrt{\frac{\mathbb{E}\{|x_n|^2\}}{\sigma_0^2}}\,\mathbf{a}_n = \sqrt{\frac{p_n}{\sigma_0^2}}\,\mathbf{a}_n$.

Let $\mathcal{I}_\mathrm{BA}\left(\mathbf{y}_\mathrm{B};\{x_n\}_{n=1,\ldots,N}\right)$ (or simply $\mathcal{I}_\mathrm{BA}$) be the total mutual information of the MIMO-OFDM subcarriers between Bob and Alice. From (27), we have [27]

$$\begin{aligned}\mathcal{I}_\mathrm{BA} &= \ln\det\Big(\mathbf{I}_{N_\mathrm{B}N} + \sqrt{\beta_\mathrm{BA}}\mathbf{H}_\mathrm{BA}\,\mathrm{diag}\left(\mathbf{a}\right)\\ &\quad\times\mathrm{diag}\big(\underbrace{p_1,\ldots,p_1}_{N_\mathrm{A}\text{ elements}},\ldots,\underbrace{p_N,\ldots,p_N}_{N_\mathrm{A}\text{ elements}}\big)\\ &\quad\times\left(\sqrt{\beta_\mathrm{BA}}\mathbf{H}_\mathrm{BA}\,\mathrm{diag}\left(\mathbf{a}\right)\right)^\dagger\left(\mathbf{C}_\mathrm{BA}\mathbf{J}\mathbf{C}_\mathrm{BA}^\dagger\right)^{-1}\Big)\\ &\overset{(a)}{=} \ln\det\Big(\mathbf{I}_{N_\mathrm{B}N} + \mathrm{blkdiag}\Big(\varrho_1\beta_\mathrm{BA}\mathbf{H}_{\mathrm{BA}_1}\mathbf{W}_1{\mathbf{H}_{\mathrm{BA}_1}}^\dagger,\\ &\quad\ldots,\ \varrho_N\beta_\mathrm{BA}\mathbf{H}_{\mathrm{BA}_N}\mathbf{W}_N{\mathbf{H}_{\mathrm{BA}_N}}^\dagger\Big)\Big)\\ &= \sum_{n=1}^{N}\mathcal{I}_{\mathrm{BA}_n} \qquad (31)\end{aligned}$$

where (a) is obtained by using (21) and the substitutions of $\mathbf{H}_\mathrm{BA} = \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{BA}_1},\ldots,\mathbf{H}_{\mathrm{BA}_N}\right\}$ and $\mathbf{W}_n = (p_n/\sigma_0^2)\mathbf{a}_n\mathbf{a}_n^\dagger$.

B. Mutual Information Between Eve and Alice

From (13), the mutual information (in nats/OFDM block) of the nth MIMO-OFDM subcarrier between Eve and Alice can be expressed as follows:

$$\begin{aligned}&\mathcal{I}_{\mathrm{EA}_n}\left(\mathbf{y}_{\mathrm{E}_n};x_n\right) = \mathcal{I}_{\mathrm{EA}_n}\\ &= \ln\det\Big(\mathbf{I}_{N_\mathrm{E}} + \left(\sqrt{\beta_\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_n}\right)\mathbf{a}_n\,\mathbb{E}\left\{|x_n|^2\right\}\mathbf{a}_n^\dagger\\ &\quad\times\left(\sqrt{\beta_\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_n}\right)^\dagger\left(\sigma_0^2\Xi_n\right)^{-1}\Big)\\ &= \ln\Big(1+\beta_\mathrm{EA}\mathbf{w}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}^\dagger\,\Xi_n^{-1}\mathbf{H}_{\mathrm{EA}_n}\mathbf{w}_n\Big) \qquad (32)\end{aligned}$$

where

$$\begin{aligned}\Xi_n &\triangleq (\sigma^2/\sigma_0^2)\beta_\mathrm{EA}\mathbf{H}_{\mathrm{EA}_n}\mathbf{B}_n\mathbf{B}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}^\dagger\\ &\quad+\mathbf{C}_{\mathrm{E}_n}\left[(\widetilde{\sigma}^2/\sigma_0^2)\beta_\mathrm{EA}\mathbf{E}\mathbf{E}^\dagger+\mathbf{I}_{N_\mathrm{E}N}\right]\mathbf{C}_{\mathrm{E}_n}^\dagger,\\ \mathbf{E} &\triangleq \mathbf{F}_\mathrm{E}\mathbf{R}_\mathrm{E}^\mathrm{cp}\widetilde{\mathbf{H}}_\mathrm{EA}^\mathrm{cp}\mathbf{Q}.\end{aligned}$$

Note that Ξ_n is a positive definite matrix we can make singular value decomposition $\Xi_n = \mathbf{V}_n\mathbf{D}_n\mathbf{V}_n^\dagger$ with a nonegative diagonal matrix $\mathbf{D}_n$ and unitary matrix $\mathbf{V}_n$. Then

$$\Xi_n^{-1} = \mathbf{V}_n\mathbf{D}_n^{-1/2}\left(\mathbf{V}_n\mathbf{D}_n^{-1/2}\right)^\dagger$$

and $\mathcal{I}_{\mathrm{EA}_n}$ in (32) is expressed as

$$\begin{aligned}\mathcal{I}_{\mathrm{EA}_n} &= \ln\Big(1+\beta_{\mathrm{EA}}\mathbf{w}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}^\dagger\mathbf{V}_n\mathbf{D}_n^{-1/2}\\ &\quad\times\left(\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}\mathbf{w}_n\right)\Big)\\ &= \ln\left(1+\left\|\sqrt{\beta_{\mathrm{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}\mathbf{w}_n\right\|^2\right). \quad (33)\end{aligned}$$

Meanwhile, the total mutual information $\mathcal{I}_{\mathrm{EA}}$ (in nats/OFDM block) of all MIMO-OFDM subcarriers between Eve and Alice can be deduced from (12) as follows:

$$\begin{aligned}\mathcal{I}_{\mathrm{EA}} &= \ln\det\Big(\mathbf{I}_{N_{\mathrm{E}}N}+\sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\ \mathrm{diag}(\mathbf{a})\\ &\quad\times\mathrm{diag}\big(\underbrace{p_1,\ldots,p_1}_{N_{\mathrm{A}}\text{ elements}},\ldots,\underbrace{p_N,\ldots,p_N}_{N_{\mathrm{A}}\text{ elements}}\big)\\ &\quad\times\left(\sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\ \mathrm{diag}(\mathbf{a})\right)^\dagger\left(\sigma_0^2\Xi\right)^{-1}\Big)\\ &\overset{(a)}{=}\ln\det\Big(\mathbf{I}_{N_{\mathrm{E}}N}+\mathrm{blkdiag}\Big\{\beta_{\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_1}\mathbf{W}_1\mathbf{H}_{\mathrm{EA}_1}^\dagger\Xi_1^{-1},\\ &\quad\ldots,\beta_{\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_N}\mathbf{W}_N\mathbf{H}_{\mathrm{EA}_N}^\dagger\Xi_N^{-1}\Big\}\Big)\\ &=\sum_{n=1}^{N}\mathcal{I}_{\mathrm{EA}_n} \quad (34)\end{aligned}$$

where

$$\begin{aligned}\Xi &= \frac{\sigma^2}{\sigma_0^2}\beta_{\mathrm{EA}}\mathbf{H}_{\mathrm{EA}}\mathbf{B}\mathbf{B}^\dagger\mathbf{H}_{\mathrm{EA}}^\dagger+\frac{\widetilde{\sigma}^2}{\sigma_0^2}\beta_{\mathrm{EA}}\mathbf{E}\mathbf{E}^\dagger+\mathbf{I}_{N_{\mathrm{E}}N}\\ &= (\sigma^2/\sigma_0^2)\beta_{\mathrm{EA}}\mathrm{blkdiag}\Big\{\mathbf{H}_{\mathrm{EA}_1}\mathbf{B}_1\mathbf{B}_1^\dagger\mathbf{H}_{\mathrm{EA}_1}^\dagger,\\ &\quad\ldots,\mathbf{H}_{\mathrm{EA}_N}\mathbf{B}_N\mathbf{B}_N^\dagger\mathbf{H}_{\mathrm{EA}_N}^\dagger\Big\}\\ &\quad+(\widetilde{\sigma}^2/\sigma_0^2)\beta_{\mathrm{EA}}\mathbf{E}\mathbf{E}^\dagger+\mathbf{I}_{N_{\mathrm{E}}N}\\ &= \mathrm{blkdiag}\left\{\Xi_1,\ldots,\Xi_N\right\}.\end{aligned}$$

The equality (a) is obtained by using the fact that $\Xi^{-1}=\mathrm{blkdiag}\left\{\Xi_1^{-1},\ldots,\Xi_N^{-1}\right\}$.

IV. Harvested Energy

In this section, we present the total energy that Bob harvests during the first and second portions.

Firstly, the harvested energy during the first portion can be calculated from (16) as follows:

$$\begin{aligned}\mathcal{E}_{\mathrm{cp}} &= \eta\tau^{\mathrm{cp}}\beta_{\mathrm{BA}}\ \mathrm{trace}\left\{\mathbf{C}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\,\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\}\left(\mathbf{C}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)^\dagger\right\}\\ &= \eta\tau^{\mathrm{cp}}\sigma_0^2\Big[\left\|\sqrt{\beta_{\mathrm{BA}}}\boldsymbol{\Upsilon}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{w}\right\|^2\\ &\quad+\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{cp}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{cp}}\right)^\dagger\right\}\Big] \quad (35)\end{aligned}$$

where $\boldsymbol{\Upsilon}^{\mathrm{cp}}=\mathbf{C}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}$. Secondly, from (18) we can also calculate the harvested energy during the second portion as follows:

$$\begin{aligned}\mathcal{E}_{\mathrm{PS}} &= \eta(K\tau_s)(1-\rho)\beta_{\mathrm{BA}}\mathbb{E}\left\{\left\|\mathrm{resize}1N_{\mathrm{B}}K\left\{\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}}\right\}\right\|^2\right\}\\ &= \eta K\tau_s(1-\rho)\beta_{\mathrm{BA}}\\ &\quad\times\mathrm{trace}\left\{\mathbf{C}_1\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\,\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\}\left(\mathbf{C}_1\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)^\dagger\right\}\\ &= \eta\left(K\tau_s\right)\left(1-\rho\right)\\ &\quad\times\sigma_0^2\Big[\left\|\sqrt{\beta_{\mathrm{BA}}}\boldsymbol{\Upsilon}^{\mathrm{PS}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{w}\right\|^2\\ &\quad+\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{PS}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{PS}}\right)^\dagger\right\}\Big] \quad (36)\end{aligned}$$

where $\boldsymbol{\Upsilon}^{\mathrm{PS}}=\mathbf{C}_1\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}$. Then, the total harvested energy can be given by

$$\begin{aligned}\mathcal{E}_{\mathrm{total}}\left(\rho,\mathbf{w}\right) &= \mathcal{E}_{\mathrm{cp}}+\mathcal{E}_{\mathrm{PS}}\\ &= \sigma_0^2\Big[-\rho\mathcal{E}_1+\mathcal{E}_2+\left\|\sqrt{\beta_{\mathrm{BA}}}\Gamma_1\mathbf{w}\right\|^2\\ &\quad+(1-\rho)\left\|\sqrt{\beta_{\mathrm{BA}}}\Gamma_2\mathbf{w}\right\|^2\Big]\\ &= \sigma_0^2\Big[-\rho\mathcal{E}_1+\mathcal{E}_2+\left\|\sqrt{\beta_{\mathrm{BA}}}\mathbf{M}\mathbf{w}\right\|^2\\ &\quad-\rho\left\|\sqrt{\beta_{\mathrm{BA}}}\Gamma_2\mathbf{w}\right\|^2\Big] \quad (37)\end{aligned}$$

where

$$2\mathcal{E}_1 = \eta K\tau_s\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{PS}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{PS}}\right)^\dagger\right\}, \quad (38a)$$

$$\mathcal{E}_2 = \mathcal{E}_1+\eta\tau^{\mathrm{cp}}\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{cp}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{cp}}\right)^\dagger\right\}, \quad (38b)$$

$$\Gamma_1 = \sqrt{\eta\tau^{\mathrm{cp}}}\ \boldsymbol{\Upsilon}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger, \quad (38c)$$

$$\Gamma_2 = \sqrt{\eta K\tau_s}\ \boldsymbol{\Upsilon}^{\mathrm{PS}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger, \quad (38d)$$

$$\mathbf{M}=\mathbf{M}^\dagger=\left(\Gamma_1^\dagger\Gamma_1+\Gamma_2^\dagger\Gamma_2\right)^{1/2}. \quad (38e)$$

V. Trade-off Problem Formulation

This section tackles the trade-off problems between the secure performance and the total harvested energy. Such trade-off problems will be presented in terms of optimization problems. For the purpose of comparing the performance of the system, we propose the following two maximization problems:

- Maximizing the difference

$$\Delta\left(\rho,\mathbf{w}\right)=\mathcal{I}_{\mathrm{BA}}-\mathcal{I}_{\mathrm{EA}}=\textstyle\sum_{n=1}^{N}\mathcal{I}_{\mathrm{BA}_n}-\sum_{n=1}^{N}\mathcal{I}_{\mathrm{EA}_n} \quad (39)$$

subject to $\mathcal{E}_{\mathrm{total}}$-based and power-based constraints. Herein, it must be noted that the achievable secrecy rate R_{sec} will be calculated as

$$R_{\mathrm{sec}}=\max\{0,\Delta\left(\rho,\mathbf{w}\right)\}. \quad (40)$$

Due to this relation, we only need to focus on $\Delta\left(\rho,\mathbf{w}\right)$ rather than R_{sec}. In short, our first problem is to

$$\begin{aligned}\underset{\rho,\mathbf{w}}{\text{maximize}}\quad & \Delta\left(\rho,\mathbf{w}\right) && (41a)\\ \text{subject to}\quad & \mathcal{E}_{\mathrm{total}}\left(\rho,\mathbf{w}\right)\geq\mathcal{E}_0, && (41b)\\ & \text{and (9).} && (41c)\end{aligned}$$

- Maximizing the total harvested energy $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ subject to Δ-based and power-based constraints. In particular, our second problem is to

$$\begin{aligned} 2 \quad \underset{\rho, \mathbf{w}}{\text{maximize}} \quad & \mathcal{E}_{\text{total}}(\rho, \mathbf{w}) && \text{(42a)} \\ \text{subject to} \quad & \Delta(\rho, \mathbf{w}) \geq \Delta_0, && \text{(42b)} \\ & \text{and (9).} && \text{(42c)} \end{aligned}$$

Note that $\mathcal{E}_0$ in (41b) and Δ_0 in (42b) are the desired energy and the desired secrecy rate, respectively. These two quantities reflect the quality-of-service of our secure scheme, and their values are pre-determined.

A. Inner Convex Approximations for Non-Convex Problems

The optimization problems (41) and (42) are non-convex because both the objective function $\Delta(\rho, \mathbf{w})$ in (39) and the objective function $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ in (37) are not concave, while both constraint (41b) and constraint (42b) are not convex. To address (41) and (42) we will employ inner convex approximation at each iteration. Let $(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)})$ be a feasible point for (41) or (42), which is found at the $(\kappa-1)$th iteration. At the κth iteration, we will

- Approximate $\Delta(\rho, \mathbf{w})$ in (39) by a lower bounding concave function $\Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w})$, which matches with $\Delta(\rho, \mathbf{w})$ at $\left(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}\right)$, i.e.

$$\Delta(\rho, \mathbf{w}) \geq \Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \quad \forall\ (\rho, \mathbf{w}) \tag{43}$$

and

$$\Delta(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}) = \Delta_{\text{lower}}^{(\kappa)}(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}). \tag{44}$$

- Approximate $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ in (37) by a lower bounding concave function $\mathcal{E}_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w})$, which matches with $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ at $\left(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}\right)$, i.e.

$$\mathcal{E}_{\text{total}}(\rho, \mathbf{w}) \geq \mathcal{E}_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \quad \forall\ (\rho, \mathbf{w}), \tag{45}$$

and

$$\mathcal{E}_{\text{total}}(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}) = \mathcal{E}_{\text{lower}}^{(\kappa)}(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}). \tag{46}$$

- Innerly approximate the nonconvex constraints (41b) and (42b) by the convex constraint

$$\mathcal{E}_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \geq \mathcal{E}_0, \tag{47}$$

and

$$\Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \geq \Delta_0, \tag{48}$$

respectively. Indeed, it follows from (43) and (45) that any feasible point for the convex constraint (47) ((48), resp.) is also feasible for the nonconvex constraint (41b) ((42b), resp.).

Proposition 1: Let $x \in \mathbb{C}$, $\bar{x} \in \mathbb{C}$, $y > 0$ and $\bar{y} > 0$. The inequality

$$\begin{aligned} \ln\left(1 + \frac{|x|^2}{y}\right) \geq \ln\left(1 + \frac{|\bar{x}|^2}{\bar{y}}\right) - \frac{|\bar{x}|^2}{\bar{y}} \\ + 2\frac{\Re\{\bar{x}^* x\}}{\bar{y}} - \frac{|\bar{x}|^2}{\bar{y}\left(\bar{y} + |\bar{x}|^2\right)}\left(y + |x|^2\right) \end{aligned} \tag{49}$$

holds true [9]. The RHS of (49) *is a concave function [28].*

Proposition 2: For $x > 0$ and $\bar{x} > 0$, the inequality

$$\ln(1 + x) \leq \ln(1 + \bar{x}) - \frac{\bar{x}}{1 + \bar{x}} + \frac{x}{1 + \bar{x}} \tag{50}$$

always holds true. The RHS of (50) *is a convex function of x.* Note that (50) holds true because its RHS is the first-order Taylor approximation of its left hand side (LHS), which is a concave function [28].

1) Obtaining $\Delta_{lower}^{(\kappa)}(\rho, \mathbf{w})$: Applying Proposition 1 to $\mathcal{I}_{\text{BA}_n}$ in (30) yields

$$\begin{aligned} \mathcal{I}_{\text{BA}_n} \geq \ln & \left(1 + \frac{\left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2}{1\Big/\varrho_n^{(\kappa)}}\right) \\ & - \frac{\left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2}{1\Big/\varrho_n^{(\kappa)}} \\ & - \frac{\left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2 \left(\frac{1}{\varrho_n} + \left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n\right\|^2\right)}{1\Big/\varrho_n^{(\kappa)}\left(1\Big/\varrho_n^{(\kappa)} + \left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2\right)} \\ \triangleq\ & f^{(\kappa)}(\mathbf{w}_n, \varrho_n) \\ =\ & \begin{cases} f^{(\kappa)}(\mathbf{w}_n, \rho) & \text{if } 1 \leq n \leq K \\ f^{(\kappa)}(\mathbf{w}_n, 1) & \text{if } K+1 \leq n \leq N \end{cases} \end{aligned} \tag{51}$$

At the same time, applying Proposition 2 yields

$$\begin{aligned} \mathcal{I}_{\text{EA}_n} \leq & \ln\left(1 + \left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2\right) \\ & - \frac{\left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2}{1 + \left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2} \\ & + \frac{\left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n\right\|^2}{1 + \left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2} \\ \triangleq\ & g^{(\kappa+1)}(\mathbf{w}_n). \end{aligned} \tag{52}$$

Using (39), (51) and (52), the concave function

$$\begin{aligned} \Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) = & \sum_{n=1}^{K} f^{(\kappa)}(\mathbf{w}_n, \rho) + \sum_{n=K+1}^{N} f^{(\kappa)}(\mathbf{w}_n, 1) \\ & - \sum_{n=1}^{N} g^{(\kappa)}(\mathbf{w}_n) \end{aligned} \tag{53}$$

satisfies (43) and (44) and thus is qualified as a lower bounding approximation of $\Delta_{\text{lower}}(\rho, \mathbf{w})$.

2) Obtaining $\mathcal{E}_{lower}^{(\kappa)}(\rho, \mathbf{w})$: Let $\mathbf{M} = [\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{N_{\text{A}}N}]$ with $\mathbf{m}_i$ being the ith column of $\mathbf{M}$. One can derive the following inequality:

$$\begin{aligned} \|\mathbf{M}\mathbf{w}\|^2 = \|\mathbf{M}^\dagger\mathbf{w}\|^2 &= \sum_{i=1}^{N_{\text{A}}N} \left|\mathbf{m}_i^\dagger\mathbf{w}\right|^2 \\ &\geq 2\sum_{i=1}^{N_{\text{A}}N} \Re\left\{(\mathbf{m}_i^\dagger\mathbf{w}^{(\kappa)})^*(\mathbf{m}_i^\dagger\mathbf{w})\right\} - \left\|\mathbf{M}^\dagger\mathbf{w}^{(\kappa)}\right\|^2 \\ &\triangleq (1/\beta_{\text{BA}})\,\eth^{(\kappa+1)}(\mathbf{w}) \end{aligned} \tag{54}$$

over the trust region

$$2\Re\left\{(\mathbf{m}_i^\dagger \mathbf{w}^{(\kappa)})^*(\mathbf{m}_i^\dagger \mathbf{w})\right\} - |\mathbf{m}_i^\dagger \mathbf{w}^{(\kappa)}|^2 > 0, i = 1, \ldots, N_{\mathrm{A}}N. \tag{55}$$

Substituting (54) into (37), we can obtain

$$\begin{aligned}
&\mathcal{E}_{\text{total}}(\rho, \mathbf{w}) \\
&\geq \sigma_0^2 \left[-\rho\mathcal{E}_1 + \mathcal{E}_2 + \eth^{(\kappa+1)}(\mathbf{w}) - \rho \left\| \sqrt{\beta_{\text{BA}}}\Gamma_2 \mathbf{w} \right\|^2 \right] \\
&= \sigma_0^2 \left[\mathcal{E}_2 + \eth^{(\kappa+1)}(\mathbf{w}) - \left\| \begin{bmatrix} \sqrt{\mathcal{E}_1} \\ \sqrt{\beta_{\text{BA}}}\,\Gamma_2 \mathbf{w} \end{bmatrix} \right\|^2 \Big/ \rho_{\text{inv}} \right] \\
&\triangleq \mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w})
\end{aligned} \tag{56}$$

where

$$\rho_{\text{inv}} \triangleq \frac{1}{\rho} \geq 1, \tag{57}$$

verifying (45) and (46), making $\mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w})$ qualified as a lower bounding approximation of $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$.

3) Algorithms and Convergence: At the κ-th the iteration we solve the following convex optimization problems to generate the next feasible point $\left(\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}\right)$ for (41) and (42), respectively:

$$\begin{aligned}
2 \quad \underset{\rho_{\text{inv}}, \mathbf{w}}{\text{maximize}} \quad & \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w}) && \text{(58a)} \\
\text{subject to} \quad & \mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \mathcal{E}_0, && \text{(58b)} \\
& (9), (55), (57) && \text{(58c)}
\end{aligned}$$

and

$$\begin{aligned}
2\text{maximize} \quad \underset{\rho_{\text{inv}}, \mathbf{w}}{} \quad & \mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w}) && \text{(59a)} \\
\text{subject to} \quad & \Delta_{\text{lower}}^{(\kappa+1)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \Delta_0, && \text{(59b)} \\
& (9), (55), (57). && \text{(59c)}
\end{aligned}$$

Note that the convex constraints (58b) and (59b) correspond to the convex constraints (47) and (48), respectively. Furthermore, we have

$$\Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}) > \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)}) \tag{60}$$

where $(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)})$ is the optimal solution of (58) and $(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)})$ is a feasible point for (58), which together with (43) and (44) yield

$$\begin{aligned}
\Delta_{\text{lower}}(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}) &\geq \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}) \\
&> \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)}),
\end{aligned} \tag{61}$$

i.e. $(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)})$ is a better feasible point than $(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)})$ for (41). Therefore, Algorithm 1, which generates the sequence $\{(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)})\}$, at least converges to a locally optimal solution of (41) [9, Proposition 2]).

Analogously, Algorithm 2 at least converges to a locally optimal solution of (42). Once initialized from an initial feasible point, both algorithms converge after a few iterations for a given error tolerance.

Convergence: The problem (58) includes two variables ρ and $\mathbf{w}$. Given that $\mathbf{w}$ is a vector of $N_{\mathrm{A}}N$ complex elements,

Algorithm 1 Path-Following Algorithm for (41)

1: **Initialization**: Set $\kappa = 0$ with an initial feasible point $\left\{\rho_{\text{inv}}^{(0)}, \mathbf{w}^{(0)}\right\}$ for (41) (see Appendix A).
2: **repeat**
3: At the $(\kappa+1)$th iteration, solve the inner convex approximation problem (58) to obtain the optimal values $\rho_{\text{inv}}^{(\kappa+1)}$ and $\mathbf{w}^{(\kappa+1)}$ of variables ρ_{inv} and $\mathbf{w}$, respectively.
4: Reset $\kappa := \kappa + 1$.
5: **until** $\left|\Delta_{\text{lower}}^{(\kappa+1)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa+1)}}, \mathbf{w}^{(\kappa+1)}\right) - \Delta_{\text{lower}}^{(\kappa)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa)}}, \mathbf{w}^{(\kappa)}\right)\right|$ converges.
6: **return** $(\rho^*, \mathbf{w}^*) = \left(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}\right)$ as the desired feasible point for (41).

Algorithm 2 Path-Following Algorithm for (42)

1: **Initialization**: Set $\kappa = 0$ with an initial feasible point $\left\{\rho_{\text{inv}}^{(0)\text{th}}, \mathbf{w}^{(0)\text{th}}\right\}$ for (42) (see Appendix B).
2: **repeat**
3: At the $(\kappa+1)$th iteration, solve the inner convex approximation problem (59) to obtain the optimal values $\rho_{\text{inv}}^{(\kappa+1)}$ and $\mathbf{w}^{(\kappa+1)}$ of variables ρ_{inv} and $\mathbf{w}$, respectively.
4: Reset $\kappa := \kappa + 1$.
5: **until** $\left|\mathcal{E}_{\text{lower}}^{(\kappa+1)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa+1)}}, \mathbf{w}^{(\kappa+1)}\right) - \mathcal{E}_{\text{lower}}^{(\kappa)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa)}}, \mathbf{w}^{(\kappa)}\right)\right|$ converges.
6: **return** $(\rho^*, \mathbf{w}^*) = \left(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}\right)$ as the desired feasible point for (42).

the total number of scalar variables is equal to $2\ N_{\mathrm{A}}N + 1$. Herein, the real part and the imaginary part of each complex element in $\mathbf{w}$ are considered as independent variables. The number of quadratic constraints is equal to $\epsilon_1 = 2$. Thus, the per-iteration computational complexity of Algorithm 1 is $\mathcal{O}\left((2\ N_{\mathrm{A}}N + 1)^2\epsilon_1^{2.5} + \epsilon_1^{3.5}\right)$ [29, Ch. 10]. Likewise, Algorithm 2 is also invoked to resolve (59). With $2N_{\mathrm{A}}N+1$ distinct variables and $\epsilon_2 = 2$ quadratic constraints, the per-iteration cost is $\mathcal{O}\left((2\ N_{\mathrm{A}}N + 1)^2\epsilon_2^{2.5} + \epsilon_2^{3.5}\right)$.

VI. Numerical Results

In this section, we provide numerical results to evaluate the performance of proposed maximization problems. More particularly, we draw the *average* curves of the achievable secrecy rate $R_{\text{sec}}(\rho, \mathbf{w}) = \max\{0, \Delta(\rho, \mathbf{w})\}$ and the total harvested energy $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ over numerous realizations of $\beta_{\text{BA}}, \beta_{\text{EA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N$ and $\{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N$.

While the realization of $\left\{\beta_{\text{BA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N\right\}$ implies the *instantaneous* observation of the channel between Alice and Bob, the realization of $\left\{\beta_{\text{EA}}, \{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N\right\}$ corresponds to *instantaneous* observation of the Alice-Eve channel at the time of measurement. Note that Algorithm 1 and Algorithm 2 are conducted in the case that $\beta_{\text{BA}}, \beta_{\text{EA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N$ and $\{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N$ are given. Let $\{\rho^\star, \mathbf{w}^\star\}$ be one of the feasible solutions after running Algorithm 1 (or Algorithm 2). Then, our goals are to evaluate

$$\begin{aligned}
R_{\text{sec}}^{\text{avr}} &= \mathbb{E}_{\{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N, \{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N}\left\{R_{\text{sec}}(\rho^*, \mathbf{w}^*)\right\}, \\
\mathcal{E}_{\text{total}}^{\text{avr}} &= \mathbb{E}_{\{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N, \{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N}\left\{\mathcal{E}_{\text{total}}(\rho^*, \mathbf{w}^*)\right\}.
\end{aligned}$$

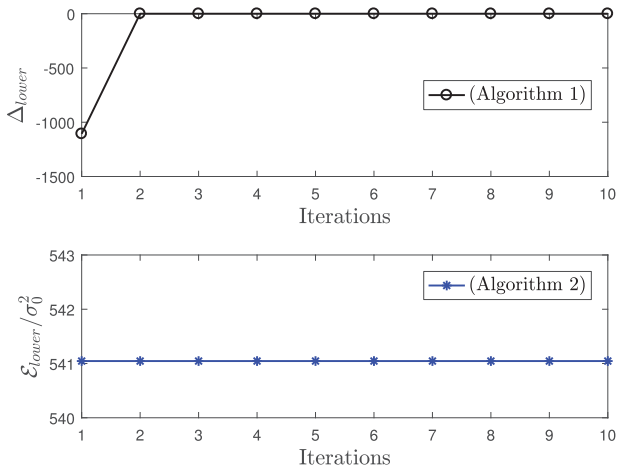

Fig. 2. The convergence rate of the proposed algorithms. Other parameters: $N = 10$, $K = 2$, and $\{P_A, \sigma^2, \bar{\sigma}^2\} = \{30, 10, 10\}$ dBm.

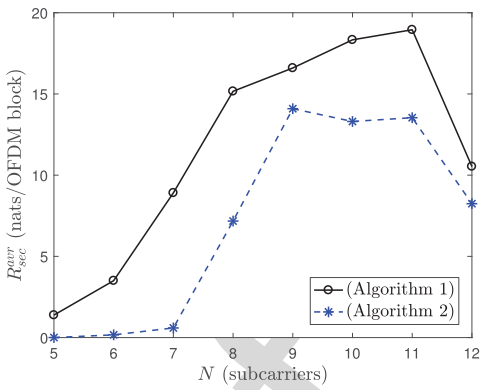

Fig. 3. The achievable secrecy rate R_{sec} as a function of the number of subcarriers N. Other system parameters: $K = 2$ and $\{P_A, \sigma^2, \bar{\sigma}^2\} = \{30, 10, 10\}$ dBm.

In short, the use of Algorithm 1 (or Algorithm 2, respectively) to solve (58) (or (59), respectively) yields a certain point $\{\rho^\star, \mathbf{w}^\star\}$. Then, the substitution $\rho = \rho^\star, \mathbf{w} = \mathbf{w}^\star$ into the expressions of R_{sec} and $\mathcal{E}$ will yield the instantaneous values at the time of measurement. Generating sufficiently large number of realizations of $\beta_{\text{BA}}, \beta_{\text{EA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N$ and $\{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N$, we can calculate the average values for the secrecy rate and harvested energy.

In simulation, the time-domain fading channel matrices $\mathbf{G}_{\text{BA}_l}$ and $\mathbf{G}_{\text{EA}_l}$ can be assumed to be symmetric complex Gaussian random variables. More particularly, we assume $\mathbf{G}_{\text{BA}_l} \sim \mathcal{CN}(0,1)$ and $\mathbf{G}_{\text{EA}_l} \sim \mathcal{CN}(0,1)$ for $\forall l \in \{1, \ldots, L\}$. The values of β_{BA} and β_{EA} rely on the rule of power degradation and the shadowing fading effect. For instance, if the distance between two transceivers is below 50 meters, the path loss can be around -90 dB. That may lead to $\beta_{\text{BA}} = 10^{(-90+\mathcal{S}_{\text{BA}})/10}$, and $\beta_{\text{EA}} = 10^{(-90+\mathcal{S}_{\text{EA}})/10}$ where $\mathcal{S}_{\text{BA}}$ and $\mathcal{S}_{\text{EA}}$ represent the shadowing. For simplicity, let us set $\mathcal{S}_{\text{BA}} = \mathcal{S}_{\text{EA}} = 10$. Other simulation parameters are as follows: $N_{\text{cp}} = 3$, $N_{\text{A}} = 6$, $N_{\text{B}} = 3$, $N_{\text{E}} = 4$, $L = 3$, $\sigma_0^2 = -80$ dBm, $\tau_s = 0.1$ s, $\eta = 80\%$, $\Delta_0 = 0$, and $\mathcal{E}_0 = 20\ \sigma_0^2$.

Fig. 2 illustrates the convergence rate for each of the proposed algorithms. It is not surprising that Algorithm 1 and Algorithm 2 converge within only 2 iterations because of the fact that (58) and (59) contain only quadratic and linear constraints.

Fig. 3 shows the relation between $R_{\text{sec}}^{\text{avr}}$ and N. The largest value of $R_{\text{sec}}^{\text{avr}}$ is obtained at $N = 11$ in the case of Algorithm 1. Meanwhile, $R_{\text{sec}}^{\text{avr}}$ takes the largest value at $N = 9$ subcarriers in the case of Algorithm 2. The curve of Algorithm 1 shows an uptrend with $N \in \{5, \ldots, 11\}$ but start a strong downtrend at $N = 12$. While the curve of Algorithm 2 is in an uptrend with $N \in \{5, \ldots, 9\}$, then slightly reducing at $N = 10$, increasing at $N = 11$ before reducing again at $N = 12$. Lastly, on average, Algorithm 1 provides higher secrecy rate than Algorithm 2.

In Fig. 4, the relation between $\mathcal{E}_{\text{total}}^{\text{avr}}$ and N is illustrated. We can see that Algorithm 1 is better than Algorithm 2 in terms of energy-harvesting. In fact, $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 1 is higher than $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 2 by the amount of above $30\sigma_0^2$ at each value of N; however, the values of $\mathcal{E}_{\text{total}}^{\text{avr}}$ in both algorithms are nearly the same at $N = 12$. For Algorithm 1, $\mathcal{E}_{\text{total}}^{\text{avr}}$ increases with $N \in \{5, 6, 7\}$ and decreases with $N \in \{8, \ldots, 12\}$. As for Algorithm 2, $\mathcal{E}_{\text{total}}^{\text{avr}}$ reaches a peak of $\mathcal{E}_{\text{total}}^{\text{avr}} = 384\sigma_0^2$ when $N = 9$.

In order to achieve the balance between $R_{\text{sec}}^{\text{avr}}$ and $\mathcal{E}_{\text{total}}^{\text{avr}}$, we observe Figs. 3–4 and suggest using either $N = 8$ for Algorithm 1 or $N = 9$ for Algorithm 2. Note that the system parameters used in these two figures are the same. Also in Figs. 3–4, the gap between the two algorithms tends to become closer when N increases. The curves are not increasing/decreasing monotonic, but they fluctuate with respect with N.

In Fig. 5, the relation between $R_{\text{sec}}^{\text{avr}}$ and K is shown. $R_{\text{sec}}^{\text{avr}}$ in Algorithm 1 reaches the highest peak at $K = 2$ and then steadily goes down; while $R_{\text{sec}}^{\text{avr}}$ in Algorithm 2 always decreases with all values of K. When compared with each other, the first proposed algorithm shows its superiority over the other at $K = \{1, \ldots, 4\}$, and both of algorithms reduce to zero at $K = \{7, 8\}$. The curves in Fig. 5 suggest choosing a small value of K to gain a satisfactory amount of the average secrecy rate.

In Fig. 6, the relation between $\mathcal{E}_{\text{total}}^{\text{avr}}$ and K is depicted. Once again, Algorithm 1 is superior to Algorithm 2 at all integer values of K, although the formulation of Algorithm 2 is inherently intended for maximizing the harvested energy. In reality, Algorithm 2 sometimes results in the instantaneously harvested energy better than Algorithm 1 at some realization of channels; however, on average, $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 2 is much lower than $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 1. Noticeably, even when we make use of the PS SWIPT scheme for all $N_{\text{B}}N$ informative samples by setting $K = N = 8$, the amount of harvested energy is not really among the highest ones, e.g. $\mathcal{E}_{\text{total}}^{\text{avr}}$ at $K = 8$ is worse than at $K = \{2, 3, 4\}$.

It can be seen from Figs. 5–6 that Algorithm 1 brings about much better system performance than Algorithm 2 in terms of both security and energy. Thus, we suggest using Algorithm 1 with the used parameters. Once Algorithm 1 has been used, the best value of K is $K = 2$ because this value

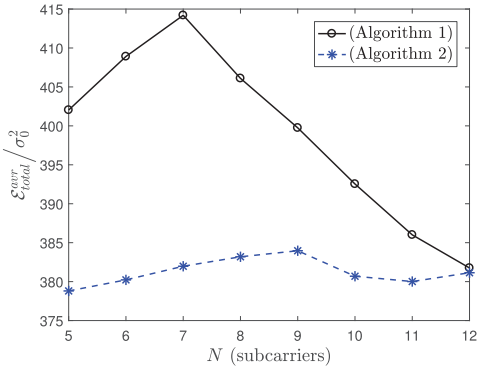

Fig. 4. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the number of subcarriers N. Other system parameters: $K = 2$ and $\{P_A, \sigma^2, \widetilde{\sigma}^2\} = \{30, 10, 10\}$ dBm.

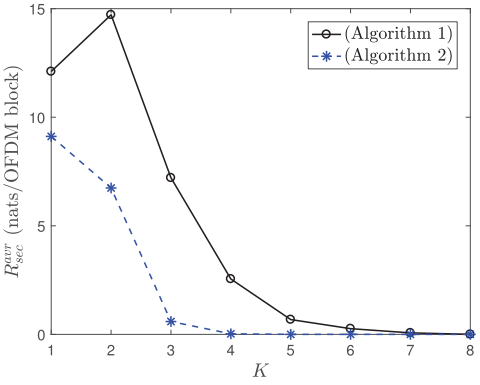

Fig. 5. The achievable secrecy rate R_{sec} as a function of the parameter K. Other system parameters: $N = 8$ and $\{P_A, \sigma^2, \widetilde{\sigma}^2\} = \{30, 10, 10\}$ dBm.

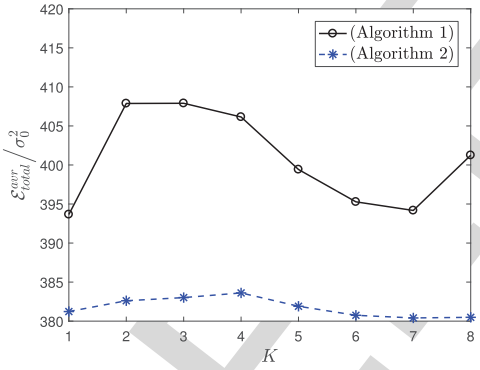

Fig. 6. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter K. Other system parameters: $N = 8$ and $\{P_A, \sigma^2, \widetilde{\sigma}^2\} = \{30, 10, 10\}$ dBm.

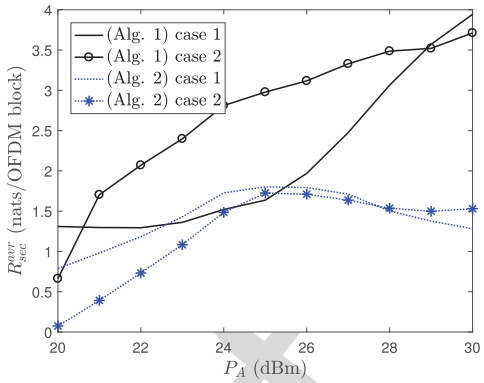

Fig. 7. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 3\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

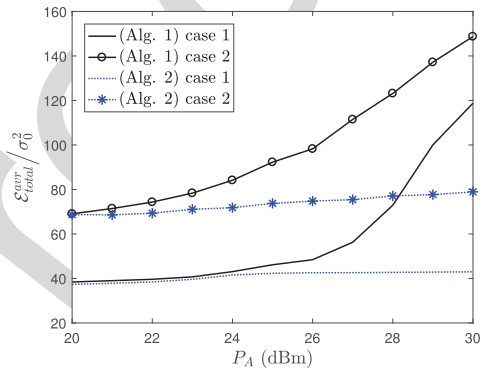

Fig. 8. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 3\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

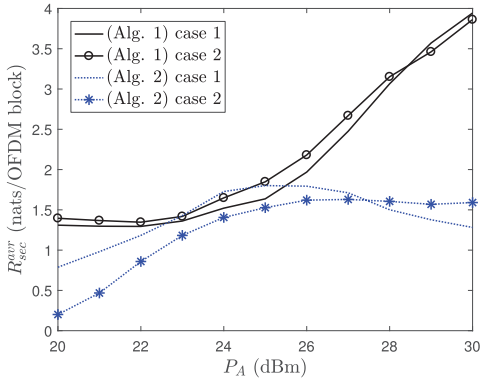

Fig. 9. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{2, 0\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

can lead to a good balance between highly achievable $R_{\text{sec}}^{\text{avr}}$ and $\mathcal{E}_{\text{total}}^{\text{avr}}$, i.e., $\left\{R_{\text{sec}}^{\text{avr}}, \frac{\mathcal{E}_{\text{total}}^{\text{avr}}}{\sigma_0^2}\right\} \approx \{14.7 \text{ nats/OFDM block}, 407.8\}$ at $K = 2$.

Fig. 7 shows that Algorithm 1 is superior to Algorithm 2 in terms of security in both considered sub-cases of. Regarding Algorithm 1, the changes in values are quite significant with $P_A \in (21, 28)$ dBm. Meanwhile, Algorithm 2 shows the slight difference between two sub-cases. When considering the first sub-case, one can see that the secure performance of Algorithm 1 is only slightly lower than Algorithm 2 at moderate $P_A \in (23, 25)$ dBm, but it is much higher than Algorithm 2 at high P_A. For the second sub-case, Algorithm 1 is almost better than Algorithm 2 at all values of P_A.

Fig. 8 shows that $\mathcal{E}_{\text{total}}^{\text{avr}}$ increases with P_A. Besides, the achieved values of $\mathcal{E}_{\text{total}}^{\text{avr}}$ in case 1 (with $\widetilde{\sigma}^2 = 0$ dBm) are lower than those in case 2 (with $\widetilde{\sigma}^2 = 3$ dBm). Interestingly, we can see that the larger $\widetilde{\sigma}^2$ (i.e., the more power we spend on generating the temporal AN $\widetilde{\mathbf{d}}$), the more energy Bob can

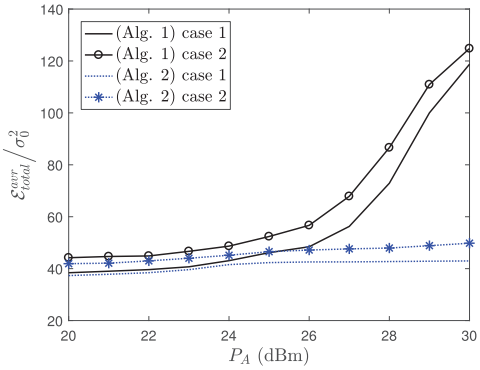

Fig. 10. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{2, 0\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

harvest. From Figs. 7–8, one can see that the difference in performance between Algorithm 1 and Algorithm 2 expands when P_A increases.

Both Fig. 9 and Fig. 10 confirm the superiority of Algorithm 1 over Algorithm 2 in terms of security and harvested energy, especially at high P_A. Moreover, Fig. 9 shows that the secure performance is not proportional to σ^2. This means that assigning more power to the frequency-domain AN may not help improve security level. While the energy efficiency seems to be proportional to the increase in σ^2 as shown in Fig. 10. When comparing Figs. 8 and 10, it is observed that in terms of energy, the power allocation for σ^2 (see Fig. 10) brings about worse performance than the power allocation for $\widetilde{\sigma}^2$ (see Fig. 8) does. This observation implies that instead of increasing σ^2 by the amount of 4 dBm, it is preferable to increase $\widetilde{\sigma}^2$ by the amount of 3 dBm.

VII. Conclusion

In this paper, we have analyzed a MIMO-OFDM SWIPT network and proposed two types of maximization problems to improve secrecy rate and harvested energy, respectively. Two path-following iterative algorithms of low computational complexity have been also provided to solve two different non-convex problems, whereby the sub-optimal solutions $(\rho^*, \mathbf{w}^*)$ have been given. The impact of other key parameters, related to the aspects of security and energy-harvesting, have been also evaluated through numerical results. Overall, we observed that the system performance is not proportional to N, K, σ^2 and $\widetilde{\sigma}^2$; thus the choice of these parameters will pose challenges to designers. In contrast, the system performance is enhanced with the increase in the power budget P_A. Moreover, it will be the responsibility of designers to choose the most suitable algorithm, because each algorithm results in a different performance. With the used parameters in this paper, we suggest using Algorithm 1 because it is superior to Algorithm 2 in resolving the trade-off problem between security and energy-harvesting. In the future, it is worth considering the impact of non-linear EH models on the secure performance of MIMO-OFDM SWIPT networks since such models reflect better the practical utility of EH circuits/receivers. Borrowing the idea of using machine learning and EH history to predict renewable energy generation trends [30], we can also consider making predictions about the amount of information leakage for future work.

Appendix

A. Locating an Initial Feasible Point for (41)

A feasible point for (41) must satisfy (41b) and (41c). Due to the non-convexity of (41b), we invoke once again the inner convex approximation by replacing $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ with $\mathcal{E}_{\text{lower}}^{(\vartheta+1)}(1/\rho_{\text{inv}}, \mathbf{w})$ at the $(\vartheta+1)$th iteration. In parallel, the accompanying constraint (55) (in which κ must be replaced with ϑ) are needed. In short, a feasible point for (41) can be found by solving the following inner convex approximation problem:

$$\begin{aligned} 2 \quad \underset{\rho_{\text{inv}}, \mathbf{W}}{\text{maximize}} \quad & 1 && \text{(62a)} \\ \text{subject to} \quad & \mathcal{E}_{\text{lower}}^{(\vartheta+1)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \mathcal{E}_0, && \text{(62b)} \\ & (9), (55), (57) && \text{(62c)} \end{aligned}$$

at the $(\vartheta+1)$th iteration. The above-proposed problem is to find an initial feasible point for Algorithm 1, but this problem itself requires an initial point to run. To find its own initial point, we simply find $(\rho_{\text{inv}}, \mathbf{w})$ satisfying (9), (55) and (57).

B. Locating an Initial Feasible Point for (42)

Similar to Appendix A, at the $(\vartheta+1)$th iteration, we need to solve the following inner convex approximation problem to find an initial feasible of (42):

$$\begin{aligned} 2 \quad \underset{\rho_{\text{inv}}, \mathbf{W}}{\text{maximize}} \quad & 1 && \text{(63a)} \\ \text{subject to} \quad & \Delta_{\text{lower}}^{(\vartheta+1)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \Delta_0, && \text{(63b)} \\ & (9), (57). && \text{(63c)} \end{aligned}$$

References

[1] T. M. Hoang, A. El Shafie, T. Q. Duong, H. D. Tuan, and A. Marshall, "Security in MIMO–OFDM SWIPT networks," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Bologna, Italy, Sep. 2018, pp. 1–6.

[2] K. Xiao, L. Gong, and M. Kadoch, "Opportunistic multicast NOMA with security concerns in a 5G massive MIMO System," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 91–95, Mar. 2018.

[3] R. Chaudhary, N. Kumar, and S. Zeadally, "Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 114–122, Nov. 2017.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[5] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State-of-the-art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[6] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," *IEEE Commun. Surveys Tutr.*, vol. 20, no. 1, pp. 264–302, 1st Quart., 2018.

[7] Q. Liu, K. S. Yildirim, P. Pawełczak, and M. Warnier, "Safe and secure wireless power transfer networks: Challenges and opportunities in RF-based systems," *IEEE Commun. Mag.*, vol. 54, no. 9, pp. 74–79, Sep. 2016.

[8] T. O. Olwal, K. Djouani, and A. M. Kurien, "A survey of resource management toward 5G radio access networks," *IEEE Commun. Surveys Tutr.*, vol. 18, no. 3, pp. 1656–1686, 3rd Quart., 2016.

[9] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 677–689, Feb. 2017.

[10] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secure and energy–efficient beamforming for simultaneous information and energy transfer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7523–7537, Nov. 2017.

[11] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "Joint beamforming and time switching design for secrecy rate maximization in wireless–powered FD relay systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 567–579, Jan. 2018.

[12] Z. Zhu, Z. Chu, N. Wang, S. Huang, Z. Wang, and I. Lee, "Beamforming and power splitting designs for an–aided secure multi–user MIMO SWIPT systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2861–2874, Dec. 2017.

[13] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2611–2626, Nov. 2017.

[14] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly Jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[15] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi–antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[16] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, Apr. 2016.

[17] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative Jamming for secure OFDM system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1331–1346, Feb. 2018.

[18] A. El Shafie, K. Tourki, and N. Al-Dhahir, "An artificial-noise-aided hybrid TS/PS scheme for OFDM–based SWIPT Systems," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 632–635, Mar. 2017.

[19] E. Boshkovska, D. W. K. Ng, N. Zlatanov, A. Koelpin, and R. Schober, "Robust resource allocation for MIMO wireless powered communication networks based on a non–linear EH model," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 1984–1999, May 2017.

[20] Y. Zeng, B. Clerckx, and R. Zhang, "Communications and signals design for wireless power transmission," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2264–2290, May 2017.

[21] P. N. Alevizos and A. Bletsas, "Sensitive and nonlinear far–field RF energy harvesting in wireless communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3670–3685, Jun. 2018.

[22] J. Gong and X. Chen, "Achievable rate region of non–orthogonal multiple access systems with wireless powered decoder," *IEEE J. Select. Areas Commun.*, vol. 35, no. 12, pp. 2846–2859, Dec. 2017.

[23] A. El Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3871–3886, May 2017.

[24] A. Van Zelst and T. Schenk, "Implementation of a MIMO OFDM–based wireless LAN system," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 483–494, Feb. 2004.

[25] Y. Yao and G. Giannakis, "Blind carrier frequency offset estimation in SISO, MIMO, and multiuser OFDM systems," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 173–183, Jan. 2005.

[26] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1691–1706, Jul. 2003.

[27] H. Bolcskei, D. Gesbert, and A. J. Paulraj, "On the capacity of OFDM-based spatial multiplexing systems," *IEEE Trans. Commun.*, vol. 50, no. 2, pp. 225–234, Feb. 2002.

[28] H. Tuy, *Convex Analysis and Global Optimization,*, 2nd ed. Springer, 2016.

[29] A. Nemirovski. (2004). *Interior Point Polynomial Time Methods in Convex Programming*. [Online]. Available: https://www2.isye.gatech.edu/~nemirovs/Lect_IPM.pdf

[30] M. Min, L. Xiao, Y. Chen, P. Cheng, D. Wu, and W. Zhuang, "Learning–based computation offloading for IoT devices with energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1930–1941, Feb. 2019.

AQ:6

Tiep M. Hoang received the B.Eng. degree in electronics and electrical engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2012, the M.Eng. degree in electronics and radio engineering from Kyung Hee University, South Korea, in 2014, and the Ph.D. degree from the Queen's University Belfast, U.K., in 2019. His current research interests include wireless security, massive multiple-input–multiple-output (MIMO), stochastic geometry, convex optimization, and the application of machine learning in wireless communications.

Ahmed El Shafie (Senior Member, IEEE) received the B.Sc. degree (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2009, the M.Sc. degree in communication and information technology from Nile University, Cairo, Egypt, in 2014, and the Ph.D. degree from The University of Texas at Dallas, Richardson, TX, USA, in 2018. Since 2018, he has been a Senior Systems Engineer with Qualcomm Technologies, San Diego, CA, USA. He was a recipient of the David Daniel Best Doctoral Thesis Award in 2018 and the Jonsson School Industrial Advisory Council Fellowship Award in 2017. He received IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer in 2015, 2016, and 2017, and the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer in 2016. He received the Qualcomm Star (Qualstar) Awards in February 2019, October 2019, and November 2019. He was nominated for the 2018 CGS/ProQuest Distinguished Dissertation Award. He currently serves as an Editor for IEEE COMMUNICATIONS LETTERS, IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY (IEEE OJ-COM), *Physical Communication*, and *Transactions on Emerging Technologies in Telecommunications*. He serves as a Guest Editor for IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

Daniel Benevides da Costa (Senior Member, IEEE) was born in Fortaleza, Brazil, in 1981. He received the B.Sc. degree in telecommunications from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil, in 2003, and the M.Sc. and Ph.D. degrees in electrical engineering (telecommunications) from the University of Campinas, Brazil, in 2006 and 2008, respectively. From 2008 to 2009, he was a Postdoctoral Research Fellow with INRS-EMT, University of Quebec, Montreal, QC, Canada. Since 2010, he has been with the Federal University of Ceará, where he is currently an Associate Professor. His Ph.D. thesis was awarded the Best Ph.D. Thesis in Electrical Engineering by the Brazilian Ministry of Education (CAPES) at the 2009 CAPES Thesis Contest. He was a recipient of four conference paper awards. He received the Exemplary Reviewer Certificate of IEEE WIRELESS COMMUNICATIONS LETTERS in 2013, the Exemplary Reviewer Certificate of IEEE COMMUNICATIONS LETTERS in 2016 and 2017, the Certificate of Appreciation of Top Associate Editor for outstanding contributions to IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2013, 2015, and 2016, the Exemplary Editor Award of IEEE COMMUNICATIONS LETTERS in 2016, and the Outstanding Editor Award of IEEE ACCESS in 2017. He is also the Vice-Chair of Americas of the IEEE Technical Committee of Cognitive Networks (TCCN), the Director of the TCCN Newsletter, and the Chair of the Special Interest Group on Energy-Harvesting Cognitive Radio Networks, IEEE TCCN. He is currently an Executive Editor of IEEE COMMUNICATIONS LETTERS and an Editor of IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE ACCESS, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, and *EURASIP Journal on Wireless Communications and Networking*. He has also served as an Associate Technical Editor for *IEEE Communications Magazine*. From 2012 to 2017 and from March 2019 to August 2019, he was an Editor of IEEE COMMUNICATIONS LETTERS. He also serves as an Area Editor of IEEE OPEN JOURNAL OF THE COMMUNICATION SOCIETY Area: Green, Cognitive, and Intelligent Communications and Networks and as a Guest Editor for several journal special issues. He has served on the organizing committee of several conferences. He is also the Latin American Chapters Coordinator of the IEEE Vehicular Technology Society. He acts as a Scientific Consultant of the National Council of Scientific and Technological Development (CNPq), Brazil, and he is a Productivity Research Fellow of CNPq. He is also a Distinguished Lecturer of the IEEE Vehicular Technology Society. He is a member of the IEEE Communications Society and the IEEE Vehicular Technology Society.

Trung Q. Duong (Senior Member, IEEE) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology (BTH), Sweden, in 2012.

He was a Lecturer (Assistant Professor) from 2013 to 2017 and a Reader (Associate Professor) from 2018 with Queen's University Belfast, U.K. He is currently with Queen's University Belfast. His current research interests include the Internet of Things (IoT), wireless communications, molecular communications, and signal processing. He has authored or coauthored 290 technical articles published in scientific journals (165 articles) and presented at international conferences (125 articles). He received the Best Paper Award at IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) in 2014, IEEE Global Communications Conference (GLOBECOM) in 2016, and IEEE Digital Signal Processing Conference (DSP) in 2017. He was a recipient of the prestigious Royal Academy of Engineering Research Fellowship (2016–2021) and the prestigious Newton Prize in 2017. He also serves as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, and *IET Communications*, and a Lead Senior Editor for IEEE COMMUNICATIONS LETTERS.

Hoang Duong Tuan received the Diploma (Hons.) and Ph.D. degrees in applied mathematics from Odessa State University, Ukraine, in 1987 and 1991, respectively. He spent nine academic years in Japan as an Assistant Professor at the Department of Electronic-Mechanical Engineering, Nagoya University, from 1994 to 1999, and then as an Associate Professor at the Department of Electrical and Computer Engineering, Toyota Technological Institute, Nagoya, from 1999 to 2003. He was a Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, from 2003 to 2011. He is currently a Professor with the School of Electrical and Data Engineering, University of Technology Sydney. He has been involved in research in the areas of optimization, control, signal processing, wireless communications, and biomedical engineering for more than 20 years.

Alan Marshall (Senior Member, IEEE) has spent over 24 years working in the telecommunications and defense industries. He is currently the Chair in communications networks with the University of Liverpool, where he is also the Director of the Advanced Networks Group and the Head of the department. He formed a successful spin-out company, Traffic Observation and Management Ltd. He has published over 200 scientific articles and holds a number of joint patents in the areas of communications and network security. His research interests include network architectures and protocols, mobile and wireless networks, network security, high-speed packet switching, QoS/QoE architectures, and multisensory communications, including haptics and olfaction. He is a fellow of the Institution of Engineering and Technology and a Senior Fellow of the Higher Education Academy. He is also a Section Editor of *The Computer Journal* of the British Computer Society and an Editorial Board Member of the *Journal of Networks*.

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

PLEASE NOTE: We cannot accept new source files as corrections for your article. If possible, please annotate the PDF proof we have sent you with your corrections and upload it via the Author Gateway. Alternatively, you may send us your corrections in list format. You may also upload revised graphics via the Author Gateway.

AQ:1 = Please confirm or add details for any funding or financial support for the research of this article.

AQ:2 = Please provide the department name for Queen's University Belfast where the authors Tiep M. Hoang and Trung Q. Duong are currently affiliated with.

AQ:3 = Please confirm the postal code for University of Technology Sydney.

AQ:4 = Please provide the department name for University of Liverpool where the author Alan Marshall is currently affiliated with.

AQ:5 = Note that if you require corrections/changes to tables or figures, you must supply the revised files, as these items are not edited for you.

AQ:6 = Please provide the publisher location for Ref. [28].

Security and Energy Harvesting for MIMO-OFDM Networks

Tiep M. Hoang, Ahmed El Shafie, *Senior Member, IEEE*, Daniel Benevides da Costa, *Senior Member, IEEE*, Trung Q. Duong, *Senior Member, IEEE*, Hoang Duong Tuan, and Alan Marshall, *Senior Member, IEEE*

***Abstract*— We consider a multiple-input multiple-output (MIMO) orthogonal frequency-division multiplexing (OFDM) network in which a source node, Alice, communicates with an energy-harvesting destination node, Bob, in the presence of a passive eavesdropper. To secure the wireless transmission, Alice generates a hybrid artificial noise (AN) in both frequency and time domains. Moreover, in order to collect more energy, Bob splits the received signal power of the cyclic prefix of each OFDM block. We then propose two non-convex optimization problems to balance both the need for security and the need for harvesting energy at Bob. While one considers maximizing the secrecy rate, the other approach aims at maximizing the harvested energy. Path-following algorithms of low computational complexity are developed and evaluated. Our numerical results show the gain of our proposed scheme and the effectiveness of our proposed algorithms.**

***Index Terms*— MIMO, OFDM, SWIPT, security, energy harvesting, hybrid artificial noise, path-following algorithms.**

I. Introduction

OVER the past decade, wireless security has been widely investigated since wireless networks are vulnerable to passive eavesdropping [2]–[5]. Harvesting energy in secure wireless networks has also drawn the research community's attention recently [6]–[8]. Obviously, considering wireless security and energy-harvesting is generally more challenging than considering each problem separately [7], [9], [10].

Many works have examined the impact of secrecy parameters on the harvested energy and clarified the role of energy-harvesting parameters on the physical-layer security performance. For example, [11] considered a relaying network and then designed beamforming vector and time-switching (TS) coefficient to maximize secrecy rate subject to energy-related constraints. Moreover, [12] focused on minimizing the transmit power subject to rate-related constraints and considered power-splitting (PS) protocol instead of TS protocol. Using the TS protocol for energy-harvesting and using game theory to cope with jamming attacks, the authors of [13] evaluated the secure performance of a wireless secret key generation system. The results in [14] indicated that the secure performance of a relaying network would be improved by using a TS-based relaying protocol (instead of merely processing information). Both the TS and PS protocols were discussed in [15] with the emphasis on protecting a relaying network. Furthermore, security and energy-harvesting for orthogonal frequency-division multiplexing (OFDM) systems were also simultaneously studied in previous works [16]–[18]. However, the proposed systems in [16] and [18] were single-input single-output (SISO) systems, while [17] had to invoke a jammer to cope with information leakage. Moreover, the methodologies used in these works might not be extended to more general cases such as multiple-input multiple-output (MIMO). Having said that, the idea of using OFDM to simultaneously improve security level and received energy in these works is worth our consideration. For instance, [18] took advantage of cyclic prefix, which is one of the most characteristics of the OFDM technique, to improve the energy harvested at the intended energy-harvesting user. Apart from the linear energy-harvesting (EH) model, several non-linear EH models are studied in [19]–[21]. In [19], the authors maximize the sum throughput and the minimum individual throughput based on the constraints of time and power allocation. From a hardware design perspective, the authors in [20] and [21] consider power conversion/transmission efficiency in connection with EH circuits. Especially, the EH model in [21] includes the sensitivity and saturation threshold of EH circuits. Such non-linear EH models are relatively practical, but applying them to secure wireless systems is really challenging. To simplify the

AQ:1 Manuscript received May 3, 2019; revised September 18, 2019 and November 11, 2019; accepted December 21, 2019. This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22. This article was presented in part at the IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Bologna, Italy, 2018. The associate editor coordinating the review of this article and approving it for publication was L. Xiao. *(Corresponding author: Trung Q. Duong.)*

AQ:2 Tiep M. Hoang and Trung Q. Duong are with Queen's University Belfast, Belfast BT7 1NN, U.K. (e-mail: mhoang02@qub.ac.uk; trung.q.duong@qub.ac.uk).

Ahmed El Shafie is with Qualcomm Inc., San Diego, CA 92121 USA (e-mail: ahmed.salahelshafie@gmail.com).

Daniel Benevides da Costa is with the Department of Computer Engineering, Federal University of Ceara (UFC), Sobral 62010-560, Brazil (e-mail: danielbcosta@ieee.org).

AQ:3 Hoang Duong Tuan is with the School of Electrical and Data Engineering, University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: tuan.hoang@uts.edu.au).

AQ:4 Alan Marshall is with the University of Liverpool, Liverpool L69 3GJ, U.K. (e-mail: alan.marshall@liverpool.ac.uk).

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

Digital Object Identifier 10.1109/TCOMM.2019.2962436

analysis, we choose to use a linear EH model as in most of the existing works. Hence, the topic of non-linear EH models is out of the scope of our paper.

Among the aforementioned works, our paper is closely related to [18]. In [18], the authors considered a SISO-OFDM simultaneous wireless information and power transfer (SWIPT) in the presence of a passive eavesdropper. As an extension of [18] to the MIMO case, this work considers a MIMO-OFDM SWPIT system. Noticeably, [18] suggests a non-convex problem for the trade-off between information security and energy-harvesting, but cannot solve it through any analytical methodology. In other words, the approach in [18] is unable to apply to similar works. In contrast, this paper provides a computational framework for resolving non-convex problems relating to the trade-off between security and energy-harvesting. Following that, we face the challenges in transforming non-convex problems into convex approximation ones[1]. More specifically, to address these non-convex optimization problems, we develop path-following iterative algorithms, which iteratively improve feasible points for the original non-convex problems. Thereby, we obtain at least a sub-optimal solution to each of the proposed problems. It should also be noted that this paper simultaneously discusses the frequency-domain artificial noise (freq. AN) design and the time-domain artificial noise (temporal AN) design. This type of hybrid AN was out of the scope of [11], [12], [14], [16]–[18], [22]. Although the hybrid AN design was proposed in [23], the topic of energy-harvesting was not considered. On the contrary, we take into account security and energy-harvesting, then resolving the trade-off problem between these two aspects. Our contributions can be summarized as follows:

- We propose a secure MIMO-OFDM SWIPT scheme in which the source node, Alice, employs a hybrid AN strategy to guarantee secure transmissions. In addition, a legitimate destination employs energy-harvesting circuitry to gather energy (see Fig. 1). We turn the process of removing the cyclic prefix into the process of harvesting energy, thereby improving the amount of achievable energy at the intended user.
- We consider two different optimization approaches. First, we maximize the secrecy rate of the system subject to the constraints of energy. Second, we maximize the harvested-energy rate at the legitimate energy-harvesting receiver subject to security constraints. As previously mentioned, we handle non-convex optimization problems by developing path-following algorithms to reach at least sub-optimal solutions.
- We quantitatively evaluate the system performance in terms of security and energy-harvesting, respectively. Through numerical results, the impact of system parameters is evaluated.

The remainder of this paper is organized as follows: Section II presents the system model and the specific setups at transceivers. Section III presents achievable secrecy rate and its lower bound. In Section IV, the total amount of harvested energy and its lower bound are derived. The two different maximization problems (i.e., maximizing the achievable secrecy rate and maximizing the harvested energy) are suggested in Section V. The numerical results and conclusions are provided in Sections VI and VII, respectively.

[1]As aforementioned, the SISO-OFDM in [18] does not provide any framework to transform non-convex problems into convex programming problems and thus, its approach fails to deal with the MIMO-OFDM case.

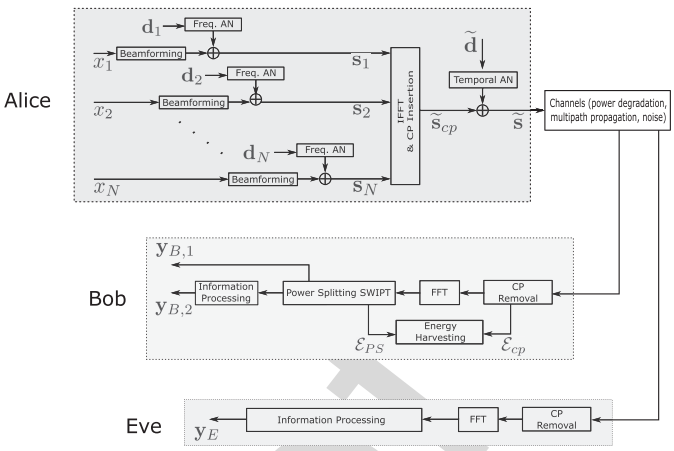

Fig. 1. System model.

Notation: $\mathbb{C}^{m\times n}$ denotes the set of all complex matrices of size m-by-n. $\Re\{\cdot\}$ and $\Im\{\cdot\}$ denote the real and imaginary parts of a complex number. $[\cdot]_{m,n}$ denotes the (m,n)th entry of a matrix. $(\cdot)^*$, $(\cdot)^\top$ and $(\cdot)^\dagger$ denote the conjugate, transpose and Hermitian operators, respectively. $\mathrm{trace}\{\cdot\}$ denotes the sum of the diagonal entries of a matrix. $(\mathbf{A})^\perp$ is an orthonormal basis for the null space of some matrix $\mathbf{A}$, i.e., $\mathbf{A}(\mathbf{A})^\perp = \mathbf{0}$. $\|.\|$ denotes the Euclidean norm of a vector. The expectation is denoted by $\mathbb{E}\{\cdot\}$. $\mathbf{z} \sim \mathcal{CN}_n(\mathbf{0}, \mathbf{\Sigma})$ denotes a complex Gaussian random vector $\mathbf{z} \in \mathbb{C}^{n\times 1}$ with mean $\mathbf{0}$ and covariance matrix $\mathbf{\Sigma} \in \mathbb{C}^{n\times n}$. Moreover, $z \sim \mathcal{CN}(0, \sigma^2)$ denotes a complex Gaussian random variable with zero-mean and covariance σ^2. $\mathrm{blkdiag}\{\cdot\}$ denotes a block diagonal matrix with its diagonal elements being matrices. The operator $\mathrm{resize}_{ij}\{\mathbf{a}\}$ resizes the vector $\mathbf{a} = [a_1, \ldots, a_i, \ldots, a_j, \ldots, a_M]$ to the vector $\mathbf{a}' = [a_i, \ldots, a_j]$.

II. System Model

In this section, we respectively present the system model and the specific setups at all nodes. The considered system consists of one source node (Alice), one energy-harvesting node (Bob), and one eavesdropper (Eve). Alice first converts the frequency-domain signals into the time-domain signals using an N-point *inverse fast Fourier transform* (IFFT), and then inserts a cyclic prefix (CP) of N_{cp} length into the beginning of each OFDM block. Let N_{A}, N_{B} and N_{E} be the number of antennas at Alice, Bob and Eve, respectively.

A. The Injection of Freq. AN and Temporal AN at Alice

Let $\mathbf{a}_n \in \mathbb{C}^{N_{\mathrm{A}}\times 1}$ and $\mathbf{B}_n$ be, respectively, the beamforming vector of subcarrier n and the frequency-domain AN precoding matrix of subcarrier n. The frequency-domain symbol vector, corresponding to the nth subcarrier, can be written as

$$\mathbf{s}_n = \mathbf{a}_n x_n + \mathbf{B}_n \mathbf{d}_n,$$

where $x_n \in \mathbb{C}$ is the frequency-domain symbol and $\mathbf{d}_n$ is the injected *freq.* AN vector. To maximize the interference at Eve, $\mathbf{d}_n$ is generated to be independent of $\mathbf{d}_m$ if $n \neq m$. Moreover, each entry in $\mathbf{d}_n$ is a complex Gaussian random variable with zero mean and covariance σ^2. The size of $\mathbf{B}_n$ and that of $\mathbf{d}_n$ will be determined later in Section II-D; however, the product $\mathbf{B}_n\mathbf{d}_n$ must be a vector, which lies in $\mathbb{C}^{N_{\mathrm{A}}\times 1}$.

As such, the frequency-domain symbol vector over all subcarriers can be written as

$$\mathbf{s} \triangleq \left[\mathbf{s}_1^\top, \mathbf{s}_2^\top, \ldots, \mathbf{s}_N^\top\right]^\top = \mathbf{X}\mathbf{a} + \mathbf{B}\mathbf{d} \tag{1}$$

where

$$\mathbf{X} = \mathrm{blkdiag}\left\{\mathbf{I}_{N_{\mathrm{A}}}x_1, \mathbf{I}_{N_{\mathrm{A}}}x_2, \ldots, \mathbf{I}_{N_{\mathrm{A}}}x_N\right\},$$
$$\mathbf{a} = \left[\mathbf{a}_1^\top, \mathbf{a}_2^\top, \ldots, \mathbf{a}_N^\top\right]^\top$$
$$\mathbf{B} = \mathrm{blkdiag}\left\{\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_N\right\}, \tag{2}$$
$$\mathbf{d} = \left[\mathbf{d}_1^\top, \mathbf{d}_2^\top, \ldots, \mathbf{d}_N^\top\right]^\top. \tag{3}$$

Remark 1: The covariance matrix of $\mathbf{s}$ *can be calculated as*:

$$\begin{aligned}\mathbb{E}\left\{\mathbf{s}\mathbf{s}^\dagger\right\} &= \mathbb{E}\left\{\mathbf{X}\mathbf{a}\mathbf{a}^\dagger\mathbf{X}^\dagger\right\} + \mathbb{E}\left\{\mathbf{B}\mathbf{d}\mathbf{d}^\dagger\mathbf{B}^\dagger\right\} \\ &= \sigma_0^2 \mathrm{blkdiag}\left\{\mathbf{W}_1, \mathbf{W}_2, \ldots, \mathbf{W}_N\right\} + \sigma^2\mathbf{B}\mathbf{B}^\dagger \end{aligned} \tag{4}$$

where $\mathbf{W}_n \triangleq \mathbf{w}_n\mathbf{w}_n^\dagger$, $\mathbf{w}_n \triangleq \sqrt{\frac{p_n}{\sigma_0^2}}\mathbf{a}_n$ *and* $p_n \triangleq \mathbb{E}\left\{|x_n|^2\right\}$. *Note that* σ_0^2 *is a constant, which is used to adjust the range of the ratio* (p_n/σ_0^2).

In order to convert the array $\{\mathbf{s}_n\}_{n=1,\ldots,N}$ into the time-domain signal, Alice uses the IFFT matrix $\mathbf{F}_{\mathrm{A}}^\dagger = \left(\mathbf{F}^\dagger \otimes \mathbf{I}_{N_{\mathrm{A}}}\right) \in \mathbb{C}^{N_{\mathrm{A}}N\times N_{\mathrm{A}}N}$ with $\mathbf{F} \in \mathbb{C}^{N\times N}$. Note that the (p,q)th element of $\mathbf{F} \in \mathbb{C}^{N\times N}$ takes the value of $[\mathbf{F}]_{p,q} = \sqrt{(1/N)}\exp\left(-j2\pi pq/N\right)$. After the conversion, Alice inserts a CP of N_{cp} samples into the beginning of that IFFT signal by using the following CP insertion matrix:

$$\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}} = \left[\left[\mathbf{0}_{N_{\mathrm{A}}N_{\mathrm{cp}}\times N_{\mathrm{A}}(N-N_{\mathrm{cp}})}, \mathbf{I}_{N_{\mathrm{A}}N_{\mathrm{cp}}}\right]^\top, \mathbf{I}_{N_{\mathrm{A}}N}\right]^\top.$$

As such, the transmitted signal in the time domain can be expressed as:

$$\widetilde{\mathbf{s}}^{\mathrm{cp}} = \mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{s}. \tag{5}$$

Let $\widetilde{\mathbf{d}}$ be the injected *temporal* AN vector, and let $\mathbf{Q}$ be the temporal AN precoding matrix. By adding $\widetilde{\mathbf{s}}^{\mathrm{cp}}$ and $\mathbf{Q}\widetilde{\mathbf{d}}$, we obtain the transmitted signal in the time domain, i.e.,

$$\widetilde{\mathbf{s}} = \widetilde{\mathbf{s}}^{\mathrm{cp}} + \mathbf{Q}\widetilde{\mathbf{d}} = \mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{s} + \mathbf{Q}\widetilde{\mathbf{d}}. \tag{6}$$

Note that the size of $\mathbf{Q}$ and the size of $\widetilde{\mathbf{d}}$ will be determined later in Section II-D. However, each entry of the vector $\widetilde{\mathbf{d}}$ will be assumed to obey $\mathcal{CN}\left(0, \widetilde{\sigma}^2\right)$.

Remark 2: The covariance matrix of the time-domain signal $\widetilde{\mathbf{s}}$ *can be calculated as*:

$$\begin{aligned}\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\} &= \mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\left(\sigma_0^2\mathbf{w}\mathbf{w}^\dagger + \sigma^2\mathbf{B}\mathbf{B}^\dagger\right)\mathbf{F}_A(\mathbf{T}_A^{cp})^\dagger + \widetilde{\sigma}^2\mathbf{Q}\mathbf{Q}^\dagger \\ &= \sigma_0^2\left[\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\mathbf{w}^\dagger\mathbf{F}_A(\mathbf{T}_A^{cp})^\dagger + \mathbf{\Lambda}\right] \end{aligned} \tag{7}$$

where

$$\mathbf{\Lambda} = \left(\sigma^2/\sigma_0^2\right)\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{B}\mathbf{B}^\dagger\mathbf{F}_A(\mathbf{T}_A^{cp})^\dagger + \left(\widetilde{\sigma}^2/\sigma_0^2\right)\mathbf{Q}\mathbf{Q}^\dagger$$

and

$$\mathbf{w} \triangleq \left[\mathbf{w}_1^\top, \ldots, \mathbf{w}_N^\top\right]^\top.$$

Then, the average power of the time-domain signal $\widetilde{\mathbf{s}}$ *is*

$$\begin{aligned}\mathbb{E}\left\{\|\widetilde{\mathbf{s}}\|^2\right\} &= \mathrm{trace}\left\{\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\}\right\} \\ &= \sigma_0^2\ \mathrm{trace}\left\{\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\mathbf{w}^\dagger\mathbf{F}_A\left(\mathbf{T}_A^{cp}\right)^\dagger + \mathbf{\Lambda}\right\} \\ &= \sigma_0^2\left[\left\|\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\right\|^2 + \mathrm{trace}\left\{\mathbf{\Lambda}\right\}\right]. \end{aligned} \tag{8}$$

Denote P_A *as the power budget of Alice. A power constraint is imposed on the signal* $\widetilde{\mathbf{s}}$ *as follows*:

$$\mathbb{E}\left\{\|\widetilde{\mathbf{s}}\|^2\right\} \leq P_A \Leftrightarrow \left\|\mathbf{T}_A^{cp}\mathbf{F}_A^\dagger\mathbf{w}\right\|^2 \leq \tfrac{P_A}{\sigma_0^2} - \mathrm{trace}\left\{\mathbf{\Lambda}\right\}. \tag{9}$$

B. Information Processing at Eve

Eve first removes the CP from her received time-domain OFDM signal by multiplying by the following CP removal matrix:

$$\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}} = \left[\mathbf{0}_{N_{\mathrm{E}}N\times N_{\mathrm{E}}N_{\mathrm{cp}}}, \mathbf{I}_{N_{\mathrm{E}}N}\right].$$

Then, a FFT algorithm is applied to convert the time-domain signals to the frequency-domain signals. This FFT algorithm is performed by multiplying the FFT matrix $\mathbf{F}_{\mathrm{E}} = (\mathbf{F} \otimes \mathbf{I}_{N_{\mathrm{E}}}) \in \mathbb{C}^{N_{\mathrm{E}}N\times N_{\mathrm{E}}N}$. As such, the frequency-domain received signal at Eve can be given by

$$\begin{aligned}\mathbf{y}_E &= \mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{EA}}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}} + \mathbf{F}_{\mathrm{E}}\widetilde{\mathbf{z}}_E \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{s} \\ &\quad + \sqrt{\beta_{\mathrm{EA}}}\mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \mathbf{F}_{\mathrm{E}}\widetilde{\mathbf{z}}_E \end{aligned} \tag{10}$$

where β_{EA} represents the impact of the large-scale fading, $\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}} \in \mathbb{C}^{N_{\mathrm{E}}(N+N_{\mathrm{cp}})\times N_{\mathrm{A}}(N+N_{\mathrm{cp}})}$ represents the small-scale fading, and $\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}$ represents the time-domain *channel impulse response* (CIR) matrix of the Eve-Alice link. Meanwhile, $\widetilde{\mathbf{z}}_E \in \mathbb{C}^{N_{\mathrm{E}}N\times 1}$ is the additive white Gaussian noise (AWGN) vector with each element distributed as $\mathcal{CN}\left(0, \sigma_0^2\right)$.

We assume that there are $L_{\mathrm{EA}} = L$ paths between Eve and Alice. Note that the multi-path delay spread is equal to $(L-1)$. In order to avoid inter-block interference at a legitimate user, it is required that the CP length is larger or equal to the multi-path delay spread, i.e., $N_{\mathrm{cp}} \geq L-1$. Also note that Alice is not aware of the Eve's presence; thus, the setting $N_{\mathrm{cp}} \geq L-1$ is not originally intended for Eve, but rather for Bob. In practice, N_{cp} is often assigned some fairly large number so that it will be able to cover most channels.

For the lth ($l \in \{0, 2, \ldots, L-1\}$) path between Eve and Alice, we denote $\mathbf{G}_{\mathrm{EA}_l} \in \mathbb{C}^{N_{\mathrm{E}}\times N_{\mathrm{A}}}$ be the time-domain fading channel matrix. According to [24], [25], $\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}$ is a block *circulant* matrix and takes the following form:

$$\begin{bmatrix} \mathbf{G}_{\mathrm{EA}_1} & \ldots & \mathcal{O}_{\mathrm{EA}} & \mathcal{O}_{\mathrm{EA}} & \ldots & \mathbf{G}_{\mathrm{EA}_2} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \mathbf{G}_{\mathrm{EA}_L} & \ldots & \mathbf{G}_{\mathrm{EA}_1} & \mathcal{O}_{\mathrm{EA}} & \ldots & \mathcal{O}_{\mathrm{EA}} \\ \mathcal{O}_{\mathrm{EA}} & \ldots & \mathbf{G}_{\mathrm{EA}_2} & \mathbf{G}_{\mathrm{EA}_1} & \ldots & \mathcal{O}_{\mathrm{EA}} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathcal{O}_{\mathrm{EA}} & \ldots & \mathcal{O}_{\mathrm{EA}} & \mathcal{O}_{\mathrm{EA}} & \ldots & \mathbf{G}_{\mathrm{EA}_1} \end{bmatrix}$$

where $\mathcal{O}_{\mathrm{EA}} \triangleq \mathbf{0}_{N_{\mathrm{E}}\times N_{\mathrm{A}}}$.

Defining $\mathbf{H}_{\mathrm{EA}} \triangleq \mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^{\dagger}$ and using the property of a circulant matrix,[2] we can express $\mathbf{H}_{\mathrm{EA}} \in \mathbb{C}^{N_{\mathrm{E}}N \times N_{\mathrm{A}}N}$ as a block-diagonal matrix, i.e.,

$$\mathbf{H}_{\mathrm{EA}} = \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{EA}_1}, \ldots, \mathbf{H}_{\mathrm{EA}_n}, \ldots, \mathbf{H}_{\mathrm{EA}_N}\right\} \quad (11)$$

where $\mathbf{H}_{\mathrm{EA}_n} = \sum_{l=1}^{L} \mathbf{G}_{\mathrm{EA}_l} e^{-j2\pi n(l-1)/N}$ represents the *frequency response* of the Eve-Alice link at the nth subcarrier. Finally, (10) is rewritten as:

$$\begin{aligned}\mathbf{y}_E &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\mathbf{s} + \mathbf{F}_{\mathrm{E}}\left[\sqrt{\beta_{\mathrm{EA}}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_E\right] \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\ \mathrm{diag}(\mathbf{a})\,[\,\underbrace{x_1, \ldots, x_1}_{N_{\mathrm{A}}\text{ elements}}, \ldots, \underbrace{x_N, \ldots, x_N}_{N_{\mathrm{A}}\text{ elements}}\,]^{\top} \\ &\quad + \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\mathbf{B}\mathbf{d} + \mathbf{F}_{\mathrm{E}}\left[\sqrt{\beta_{\mathrm{EA}}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_E\right].\end{aligned} \quad (12)$$

Let $\mathbf{y}_{\mathrm{E}_n}$ be the nth subcarrier received signal. The elements in $\mathbf{y}_{\mathrm{E}_n}$ are also the entries in $\mathbf{y}_E$, beginning at index $(n-1)N_{\mathrm{E}}+1$ and ending at index nN_{E}. We have

$$\begin{aligned}\mathbf{y}_{\mathrm{E}_n} &= \mathrm{resize}(n-1)N_{\mathrm{E}} + 1nN_{\mathrm{E}}\{\mathbf{y}_E\} \\ &= \underbrace{\left[\mathbf{0}_{N_{\mathrm{E}}\times(n-1)N_{\mathrm{E}}}\ \mathbf{I}_{N_{\mathrm{E}}}\ \mathbf{0}_{N_{\mathrm{E}}\times(N-n)N_{\mathrm{E}}}\right]}_{\triangleq \mathbf{C}_{\mathrm{E}_n}}\mathbf{y}_E \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{C}_{\mathrm{E}_n}\mathbf{H}_{\mathrm{EA}}\left(\mathbf{X}\mathbf{a} + \mathbf{B}\mathbf{d}\right) \\ &\quad + \mathbf{C}_{\mathrm{E}_n}\mathbf{F}_{\mathrm{E}}\left[\sqrt{\beta_{\mathrm{EA}}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_E\right] \\ &= \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}_n}\mathbf{a}_n x_n + \sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}_n}\mathbf{B}_n\mathbf{d}_n \\ &\quad + \sqrt{\beta_{\mathrm{EA}}}\mathbf{C}_{\mathrm{E}_n}\mathbf{F}_{\mathrm{E}}\mathbf{R}_{\mathrm{E}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{EA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \mathbf{C}_{\mathrm{E}_n}\mathbf{F}_{\mathrm{E}}\widetilde{\mathbf{z}}_E\end{aligned} \quad (13)$$

where the last equality is obtained by using block matrix multiplication to shorten the first term $\mathbf{C}_{\mathrm{E}_n}\mathbf{H}_{\mathrm{EA}}\mathbf{X}\mathbf{a}$ and the second term $\mathbf{C}_{\mathrm{E}_n}\mathbf{H}_{\mathrm{EA}}\mathbf{B}\mathbf{d}$.

C. Information Processing and Energy Harvesting at Bob

Similar to the previous sub-section, the channel between Alice and Bob is a MIMO frequency selective fading channel with L_{BA} paths. For simplicity, we also assume $L_{\mathrm{BA}} = L$. For the lth path between Bob and Alice, $\mathbf{G}_{\mathrm{BA}_l} \in \mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{A}}}$ is the time-domain fading channel matrix.

The employment of OFDM at Alice leads to the fact that each MIMO-OFDM transmission block can be viewed as N parallel frequency-domain MIMO channels. If Bob does not adopt any energy-harvesting scheme, the received frequency-domain signal at Bob (say $\mathbf{y}_{B,\varnothing}$) would be formulated exactly the same way we attained (10)–(12), i.e.,

$$\begin{aligned}\mathbf{y}_{B,\varnothing} &= \mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^{\dagger}\mathbf{s} \\ &\quad + \mathbf{F}_{\mathrm{B}}\left[\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},\varnothing}\right] \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\mathbf{s} + \mathbf{F}_{\mathrm{B}}\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},\varnothing}\right]\end{aligned} \quad (14)$$

where β_{BA} represents the impact of the large-scale fading, $\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}} \in \mathbb{C}^{N_{\mathrm{B}}(N+N_{\mathrm{cp}})\times N_{\mathrm{A}}(N+N_{\mathrm{cp}})}$ represents the small-scale fading, and $\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}$ represents the time-domain CIR matrix of the Bob-Alice link. In (14), $\widetilde{\mathbf{z}}_{\mathrm{B},\varnothing} \in \mathbb{C}^{N_{\mathrm{B}}N\times 1}$ is the AWGN vector with each element distributed as $\mathcal{CN}\left(0, \sigma_0^2\right)$, the CP removal matrix at Bob is $\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}} = \left[\mathbf{0}_{N_{\mathrm{B}}N\times N_{\mathrm{B}}N_{\mathrm{cp}}}, \mathbf{I}_{N_{\mathrm{B}}N}\right]$, and $\mathbf{H}_{\mathrm{BA}}$ is defined as

$$\begin{aligned}\mathbf{H}_{\mathrm{BA}} &\triangleq \mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^{\dagger} \\ &= \mathrm{blkdiag}\Big\{\mathbf{H}_{\mathrm{BA}_1}, \ldots, \mathbf{H}_{\mathrm{BA}_n}, \ldots, \mathbf{H}_{\mathrm{BA}_N}\Big\}\end{aligned} \quad (15)$$

with $\mathbf{H}_{\mathrm{BA}_n} = \sum_{l=1}^{L}\mathbf{G}_{\mathrm{BA}_l}e^{-j2\pi n(l-1)/N}$.

Bob is assumed to adopt the PS SWIPT scheme, the received signal $\mathbf{y}_{\mathrm{B}}$ will be derived in a slightly different way. Obviously, we have $\mathbf{y}_{\mathrm{B}} \neq \mathbf{y}_{B,\varnothing}$. A detailed description of information processing and energy-harvesting at Bob will be presented below.[3]

- The time duration of an OFDM block is divided into three smaller portions: the first portion is from 0 to $\tau^{\mathrm{cp}} = N_{\mathrm{cp}}\tau_s$, the second portion is from τ^{cp} to $\tau^{\mathrm{cp}} + K\tau_s$ (with $K \in \{1, \ldots, N\}$), and the remaining part is from $\tau^{\mathrm{cp}} + K\tau_s$ to the end of the OFDM block duration (i.e., $N\tau_s$). Herein, τ_s represents the sampling time (the sampling rate is thus equal to $1/\tau_s$).
- The first portion is to remove the CP from the received time-domain OFDM signal at Bob. In other words, the first $N_{\mathrm{B}}N_{\mathrm{cp}}$ elements of the vector $\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}}$ are not be treated as information elements and will not go through any information processing. Instead, these elements are employed for the purpose of harvesting energy. Thus, the energy harvested by Bob can be calculated as follows:

$$\mathcal{E}_{\mathrm{cp}} = \eta\tau^{\mathrm{cp}}\,\mathbb{E}\left\{\left\|\mathrm{resize}1N_{\mathrm{B}}N_{\mathrm{cp}}\left\{\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}}\right\}\right\|^2\right\} \quad (16)$$

  where $\eta \in [0,1]$ is the energy conversion efficiency of the energy-harvester circuit, and $\mathbf{C}^{\mathrm{cp}} \triangleq \left[\mathbf{I}_{N_{\mathrm{B}}N_{\mathrm{cp}}}\ \mathbf{0}_{N_{\mathrm{B}}N_{\mathrm{cp}}\times N_{\mathrm{B}}N}\right]$
- During the second portion, Bob uses the PS SWIPT scheme to decode information and harvest energy simultaneously. More specifically, the obtained signal is divided into two streams based on a PS coefficient $\rho \in (0,1]$. For information processing, the received power of one stream will be multiplied by the coefficient ρ. Given that the multiplication of the received power by ρ is equivalent to the multiplication of noise by $1/\rho$, we can express the received signal in the frequency domain (after the FFT operation) as follows:

$$\begin{aligned}&\mathbf{y}_{\mathrm{B},1} \\ &= \mathrm{resize}1N_{\mathrm{B}}K\left\{\mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}} + \frac{1}{\sqrt{\rho}}\mathbf{F}_{\mathrm{B}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\right\} \\ &= \mathbf{C}_1\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{F}_{\mathrm{B}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}} + \frac{1}{\sqrt{\rho}}\mathbf{F}_{\mathrm{B}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\right] \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{C}_1\mathbf{H}_{\mathrm{BA}}\mathbf{s} \\ &\quad + \mathbf{C}_1\mathbf{F}_{\mathrm{B}}\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \frac{1}{\sqrt{\rho}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\right]\end{aligned} \quad (17)$$

[2] If a square matrix $\mathbf{C}$ is circulant, then it can be diagonalized by the FFT matrix $\mathbf{F}$ and the IFFT matrix $\mathbf{F}^{\dagger}$, i.e., $\mathbf{F}\mathbf{C}\mathbf{F}^{\dagger}$ is a diagonal matrix [25].

[3] In [18], only SISO channels and temporal AN were discussed. In contrast, our work extends SISO channels to MIMO channels and yet, the injection of additional frequency-domain AN is also taken into account.

where $\mathbf{C}_1 \triangleq \left[\mathbf{I}_{N_\mathrm{B}K} \;\; \mathbf{0}_{N_\mathrm{B}K\times N_\mathrm{B}(N-K)}\right]$ and $\widetilde{\mathbf{z}}_{\mathrm{B},1} \in \mathbb{C}^{N_\mathrm{B}N\times 1}$ is the AWGN vector with each element distributed as $\mathcal{CN}\left(0,\sigma_0^2\right)$. In parallel, for energy-harvesting, the remaining stream will be transformed into energy. The harvested energy during this portion is given by

$$\mathcal{E}_{\mathrm{PS}} = \eta\left(K\tau_s\right)\left(1-\rho\right) \times \mathbb{E}\left\{\left\|\mathrm{resize}1N_\mathrm{B}K\left\{\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}}\right\}\right\|^2\right\}. \tag{18}$$

Different from $\mathbf{y}_{\mathrm{B},1}$ in (17), the term $\mathrm{resize}1N_\mathrm{B}K\left\{\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\widetilde{\mathbf{s}}\right\}$ in (18) is the signal which does not go through information processing (thus, there is no noise term) as well as FFT operation.

- During the third/last portion, Bob processes the signal in the same way as Eve does. Given that there are $N_\mathrm{B}(N-K)$ samples left for this portion, the received signal from time $\tau_s + K\tau_s$ to time $N\tau_s$ can be written as:

$$\begin{aligned}\mathbf{y}_{\mathrm{B},2} &= \mathrm{resize}N_\mathrm{B}(K+1)N_\mathrm{B}N\Bigg\{\sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\mathbf{s} \\ &\quad + \mathbf{F}_\mathrm{B}\left(\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},2}\right)\Bigg\} \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{C}_2\mathbf{H}_{\mathrm{BA}}\mathbf{s} \\ &\quad + \mathbf{C}_2\mathbf{F}_\mathrm{B}\left[\sqrt{\beta_{\mathrm{BA}}}\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \widetilde{\mathbf{z}}_{\mathrm{B},2}\right]\end{aligned} \tag{19}$$

where $\mathbf{C}_2 \triangleq \left[\mathbf{0}_{N_\mathrm{B}(N-K)\times N_\mathrm{B}K} \;\; \mathbf{I}_{N_\mathrm{B}(N-K)}\right]$ and $\widetilde{\mathbf{z}}_{\mathrm{B},2} \in \mathbb{C}^{N_\mathrm{B}N\times 1}$ is the AWGN vector with each element distributed as $\mathcal{CN}\left(0,\sigma_0^2\right)$.

In short, the received signal $\mathbf{y}_\mathrm{B} = \left[\mathbf{y}_{\mathrm{B},1}^\top, \mathbf{y}_{\mathrm{B},2}^\top\right]^\top$ at Bob can be given by

$$\begin{aligned}\mathbf{y}_\mathrm{B} &= \begin{bmatrix}\mathbf{C}_1\\ \mathbf{C}_2\end{bmatrix}\sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\left(\mathbf{X}\mathbf{a}+\mathbf{B}\mathbf{d}\right) \\ &\quad + \begin{bmatrix}\mathbf{C}_1\\ \mathbf{C}_2\end{bmatrix}\mathbf{F}_\mathrm{B}\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\left(\sqrt{\beta_{\mathrm{BA}}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)\mathbf{Q}\widetilde{\mathbf{d}} \\ &\quad + \begin{bmatrix}\mathbf{C}_1\mathbf{F}_\mathrm{B} & \mathbf{0}_{N_\mathrm{B}K\times N_\mathrm{B}N}\\ \mathbf{0}_{N_\mathrm{B}(N-K)\times N_\mathrm{B}N} & \mathbf{C}_2\mathbf{F}_\mathrm{B}\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{\rho}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\\ \widetilde{\mathbf{z}}_{\mathrm{B},2}\end{bmatrix} \\ &\overset{(a)}{=} \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\left(\mathbf{X}\mathbf{a}+\mathbf{B}\mathbf{d}\right) \\ &\quad + \sqrt{\beta_{\mathrm{BA}}}\mathbf{F}_\mathrm{B}\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q}\widetilde{\mathbf{d}} + \mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B}\end{aligned} \tag{20}$$

where (a) is obtained by defining

$$\mathbf{C}_{\mathrm{BA}} \triangleq \begin{bmatrix}\mathbf{C}_1\mathbf{F}_\mathrm{B} & \mathbf{0}_{N_\mathrm{B}K\times N_\mathrm{B}N}\\ \mathbf{0}_{N_\mathrm{B}(N-K)\times N_\mathrm{B}N} & \mathbf{C}_2\mathbf{F}_\mathrm{B}\end{bmatrix},$$

$$\widetilde{\mathbf{z}}_\mathrm{B} \triangleq \begin{bmatrix}\frac{1}{\sqrt{\rho}}\widetilde{\mathbf{z}}_{\mathrm{B},1}\\ \widetilde{\mathbf{z}}_{\mathrm{B},2}\end{bmatrix} \sim \mathcal{CN}_{2\;N_\mathrm{B}N}\left(\mathbf{0},\mathbf{J}\right)$$

$$\text{with } \mathbf{J} = \begin{bmatrix}(1/\rho)\sigma_0^2\mathbf{I}_{N_\mathrm{B}N} & \mathbf{0}_{N_\mathrm{B}N}\\ \mathbf{0}_{N_\mathrm{B}N} & \sigma_0^2\mathbf{I}_{N_\mathrm{B}N}\end{bmatrix},$$

and using the fact that $\begin{bmatrix}\mathbf{C}_1\\ \mathbf{C}_2\end{bmatrix} \equiv \mathbf{I}_{N_\mathrm{B}N}$. The covariance matrix of $\mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B}$ can be calculated as follows:

$$\begin{aligned}\mathbf{C}_{\mathrm{BA}}\mathbf{J}\mathbf{C}_{\mathrm{BA}}^\dagger &= \begin{bmatrix}(1/\rho)\sigma_0^2\mathbf{C}_1\mathbf{F}_\mathrm{B}\mathbf{F}_\mathrm{B}^\dagger\mathbf{C}_1^\dagger & \mathbf{0}\\ \mathbf{0} & \sigma_0^2\mathbf{C}_2\mathbf{F}_\mathrm{B}\mathbf{F}_\mathrm{B}^\dagger\mathbf{C}_2^\dagger\end{bmatrix} \\ &= \begin{bmatrix}(1/\rho)\sigma_0^2\mathbf{I}_{N_\mathrm{B}K} & \mathbf{0}\\ \mathbf{0} & \sigma_0^2\mathbf{I}_{N_\mathrm{B}(N-K)}\end{bmatrix}\end{aligned} \tag{21}$$

where the last equality follows that $\mathbf{F}_\mathrm{B}\mathbf{F}_\mathrm{B}^\dagger = \mathbf{I}_{N_\mathrm{B}N}$, $\mathbf{C}_1\mathbf{C}_1^\dagger = \mathbf{I}_{N_\mathrm{B}K}$ and $\mathbf{C}_2\mathbf{C}_2^\dagger = \mathbf{I}_{N_\mathrm{B}(N-K)}$.

Let $\mathbf{y}_{\mathrm{B}_n}$ be the nth subcarrier received signal. We have

$$\begin{aligned}\mathbf{y}_{\mathrm{B}_n} &= \mathrm{resize}(n-1)N_\mathrm{B} + 1nN_\mathrm{B}\left\{\mathbf{y}_\mathrm{B}\right\} \\ &= \underbrace{\left[\mathbf{0}_{N_\mathrm{B}\times(n-1)N_\mathrm{B}} \;\; \mathbf{I}_{N_\mathrm{B}} \;\; \mathbf{0}_{N_\mathrm{B}\times(N-n)N_\mathrm{B}}\right]}_{\triangleq\mathbf{C}_{\mathrm{B}_n}}\mathbf{y}_\mathrm{B} \\ &= \mathbf{C}_{\mathrm{B}_n}\mathbf{y}_\mathrm{B}.\end{aligned} \tag{22}$$

D. AN Design at Alice to Cancel Interference at Bob

As seen in (20), the presence of AN terms $\mathbf{d}$ and $\widetilde{\mathbf{d}}$ causes interference at Bob. To cancel the interference, Alice can design $\mathbf{B}$ and $\mathbf{Q}$ subject to

$$\begin{cases}\mathbf{H}_{\mathrm{BA}}\mathbf{B} &= \mathbf{0}\\ \mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\mathbf{Q} &= \mathbf{0}.\end{cases} \tag{23}$$

Using (2) and (15), we can find out the solution $\mathbf{B}$ to the equation $\mathbf{H}_{\mathrm{BA}}\mathbf{B} = \mathbf{0}$ as follows:

$$\begin{aligned}\mathbf{H}_{\mathrm{BA}}\mathbf{B} = \mathbf{0} &\Leftrightarrow \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{BA}_1}\mathbf{B}_1,\ldots,\mathbf{H}_{\mathrm{BA}_N}\mathbf{B}_N\right\} = \mathbf{0} \\ &\Leftrightarrow \mathbf{B}_n = \mathbf{H}_{\mathrm{BA}_n}^\perp,\ \forall n\in\{1,\ldots,N\}.\end{aligned} \tag{24}$$

Now it is obvious that $\mathbf{B} = \mathrm{blkdiag}\left\{\mathbf{B}_1,\ldots,\mathbf{B}_N\right\} = \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{BA}_1}^\perp,\ldots,\mathbf{H}_{\mathrm{BA}_N}^\perp\right\}$ is a matrix with $N_\mathrm{A}N$ rows and $(N_\mathrm{A}-N_\mathrm{B})N$ columns due to $\mathbf{B}_n \in \mathbb{C}^{N_\mathrm{A}\times(N_\mathrm{A}-N_\mathrm{B})}$. The existence of $\mathbf{B}$, in general, depends on the existence of all elements $\{\mathbf{B}_n\}_{n=1}^N$. Each $\mathbf{B}_n$ exists if and only if its second dimension is positive, i.e.,

$$N_\mathrm{A} - N_\mathrm{B} > 0 \Leftrightarrow N_\mathrm{B} < N_\mathrm{A}. \tag{25}$$

Likewise, we deduce $\mathbf{Q} \in \mathbb{C}^{N_\mathrm{A}(N+N_{\mathrm{cp}})\times(N_\mathrm{A}(N+N_{\mathrm{cp}})-r)}$ with $r = \mathrm{rank}\left(\mathbf{R}_\mathrm{B}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right) = \min\{N_\mathrm{B}N, N_\mathrm{A}(N+N_{\mathrm{cp}})\}$. For the existence of $\mathbf{Q}$, it is required to have the condition $N_\mathrm{A}(N+N_{\mathrm{cp}})-r>0$, which leads to

$$r = N_\mathrm{B}N \Leftrightarrow N_\mathrm{B}N < N_\mathrm{A}(N+N_{\mathrm{cp}}). \tag{26}$$

Note that once (25) has been satisfied, (26) will be satisfied as well. Thus, the case of $N_\mathrm{A} > N_\mathrm{B}$ is taken into account in this paper. Then, we will be able to design $\mathbf{B}_n \in \mathbb{C}^{N_\mathrm{A}\times(N_\mathrm{A}-N_\mathrm{B})}$, $\mathbf{d}_n \in \mathbb{C}^{(N_\mathrm{A}-N_\mathrm{B})\times 1}$, $\mathbf{Q} \in \mathbb{C}^{N_\mathrm{A}(N+N_{\mathrm{cp}})\times(N_\mathrm{A}(N+N_{\mathrm{cp}})-N_\mathrm{B}N)}$ and $\widetilde{\mathbf{d}} \in \mathbb{C}^{(N_\mathrm{A}(N+N_{\mathrm{cp}})-N_\mathrm{B}N)\times 1}$.

Substituting (23) into (20) and (22), we can rewrite

$$\begin{aligned}\mathbf{y}_\mathrm{B} &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\mathbf{X}\mathbf{a} + \mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B} \\ &= \sqrt{\beta_{\mathrm{BA}}}\mathbf{H}_{\mathrm{BA}}\;\mathrm{diag}\left(\mathbf{a}\right)\big[\underbrace{x_1,\ldots,x_1}_{N_\mathrm{A}\text{ elements}},\ldots,\underbrace{x_N,\ldots,x_N}_{N_\mathrm{A}\text{ elements}}\big]^\top \\ &\quad + \mathbf{C}_{\mathrm{BA}}\widetilde{\mathbf{z}}_\mathrm{B}\end{aligned} \tag{27}$$

TABLE I
A TABLE OF FREQUENTLY-USED SYMBOLS

Parameters	Physical Meanings
$\mathbf{G}_{\mathrm{BA}_{l_\mathrm{B}}} \in \mathbb{C}^{N_\mathrm{B}\times N_\mathrm{A}}$	The *time-domain* fading channel matrix corresponding to the l_Bth path between Bob and Alice, for given $l_\mathrm{B} \in \{1,\ldots,L_\mathrm{BA}\}$.
$\mathbf{G}_{\mathrm{EA}_{l_\mathrm{E}}} \in \mathbb{C}^{N_\mathrm{E}\times N_\mathrm{A}}$	The *time-domain* fading channel matrix corresponding to the lth path between Eve and Alice, for given $l_\mathrm{E} \in \{1,\ldots,L_\mathrm{EA}\}$.
$\mathbf{H}_{\mathrm{BA}_n} = \sum_{l=0}^{L_\mathrm{BA}} \mathbf{G}_{\mathrm{BA}_l} e^{-j2\pi\frac{nl}{N}}$	The *frequency response* of the Bob-Alice link at the nth subcarrier, for given $n \in \{1,\ldots,N\}$.
$\mathbf{H}_{\mathrm{EA}_n} = \sum_{l=0}^{L_\mathrm{EA}} \mathbf{G}_{\mathrm{EA}_l} e^{-j2\pi\frac{nl}{N}}$	The *frequency response* of the Eve-Alice link at the nth subcarrier, for given $n \in \{1,\ldots,N\}$.
N_cp	The CP length. To prevent Bob from being affected by inter-block interference, it is required to have $N_\mathrm{cp} \geq L_\mathrm{BA}-1$.
$\mathbf{T}_\mathrm{A}^\mathrm{cp}$	The CP insertion matrix at Alice.
$\mathbf{R}_\mathrm{B}^\mathrm{cp}$ and $\mathbf{R}_\mathrm{E}^\mathrm{cp}$	The CP removal matrices at Bob and at Eve, respectively.
$\mathbf{F}_\mathrm{A}^\dagger = \left(\mathbf{F}^\dagger \otimes \mathbf{I}_{N_\mathrm{A}}\right)$	The N-point IFFT matrix at Alice.
$\mathbf{F}_\mathrm{B} = \left(\mathbf{F} \otimes \mathbf{I}_{N_\mathrm{B}}\right)$	The N-point FFT matrix at Bob.
$\mathbf{F}_\mathrm{E} = \left(\mathbf{F} \otimes \mathbf{I}_{N_\mathrm{E}}\right)$	The N-point FFT matrix at Eve.
$\mathbf{a}_n \in \mathbb{C}^{N_\mathrm{A}\times 1}$	The beamforming vector corresponding to subcarrier n.
$\mathbf{B}_n = \mathbf{H}_{\mathrm{BA}_n}^\perp$	The frequency-domain AN precoding matrix corresponding to subcarrier n.
$\mathbf{d}_n \in \mathbb{C}^{(N_\mathrm{A}-N_\mathrm{B})\times 1}$	The injected frequency-domain AN vector corresponding to subcarrier n. Each entry obeys $\mathcal{CN}\left(0,\sigma^2\right)$.
$\mathbf{Q} = \left(\mathbf{R}_\mathrm{B}^\mathrm{cp}\widetilde{\mathbf{H}}_\mathrm{BA}^\mathrm{cp}\right)^\perp$	The temporal AN precoding matrix.
$\widetilde{\mathbf{d}} \in \mathbb{C}^{(N_\mathrm{A}(N+N_\mathrm{cp})-N_\mathrm{B}N)\times 1}$	The temporal AN vector. Each entry obeys $\mathcal{CN}\left(0,\widetilde{\sigma}^2\right)$.

and

$$\begin{aligned}\mathbf{y}_{\mathrm{B}_n} &= \sqrt{\beta_\mathrm{BA}}\mathbf{C}_{\mathrm{B}_n}\mathbf{H}_\mathrm{BA}\mathbf{X}\mathbf{a} + \mathbf{C}_{\mathrm{B}_n}\mathbf{C}_\mathrm{BA}\widetilde{\mathbf{z}}_\mathrm{B}\\ &\overset{(a)}{=} \sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\mathbf{a}_n x_n + \mathbf{C}_{\mathrm{B}_n}\mathbf{C}_\mathrm{BA}\widetilde{\mathbf{z}}_\mathrm{B} \qquad (28)\end{aligned}$$

where (a) is obtained by using block matrix multiplication to calculate the product $\mathbf{C}_{\mathrm{B}_n}\mathbf{H}_\mathrm{BA}\mathbf{X}\mathbf{a}$. The covariance matrix of $\mathbf{C}_{\mathrm{B}_n}\mathbf{C}_\mathrm{BA}\widetilde{\mathbf{z}}_\mathrm{B}$ can be calculated as:

$$\begin{aligned}&\mathbf{C}_{\mathrm{B}_n}\left(\mathbf{C}_\mathrm{BA}\mathbf{J}\mathbf{C}_\mathrm{BA}^\dagger\right)\mathbf{C}_{\mathrm{B}_n}^\dagger = (1/\varrho_n)\sigma_0^2\mathbf{I}_{N_\mathrm{B}}\\ &\text{where } \varrho_n = \begin{cases}\rho & \text{if } 1\leq n\leq K\\ 1 & \text{if } K+1\leq n\leq N\end{cases}. \qquad (29)\end{aligned}$$

For readability, we present a table of symbols, Table I, at the top of the next page.

III. ACHIEVABLE SECRECY RATE

In this section, we formulate the achievable secrecy rate, which is the lower-bound of the capacity difference between the Bob-Alice link and the Eve-Alice link.

A. Mutual Information Between Bob and Alice

Let $\mathcal{I}_{\mathrm{BA}_n}\left(\mathbf{y}_{\mathrm{B}_n};x_n\right)$ (or simply $\mathcal{I}_{\mathrm{BA}_n}$) be the mutual information of the nth MIMO-OFDM subcarrier between Bob and Alice. From (28), $\mathcal{I}_{\mathrm{BA}_n}\left(\mathbf{y}_{\mathrm{B}_n};x_n\right)$ (in nats/OFDM block) can be expressed as [26]:

$$\begin{aligned}&\mathcal{I}_{\mathrm{BA}_n}\left(\mathbf{y}_{\mathrm{B}_n};x_n\right) \equiv \mathcal{I}_{\mathrm{BA}_n}\\ &= \ln\det\Bigg(\mathbf{I}_{N_\mathrm{B}} + \left(\sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\right)\mathbf{a}_n\,\mathbb{E}\left\{|x_n|^2\right\}\mathbf{a}_n^\dagger\\ &\quad\times\left(\sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\right)^\dagger\left(\frac{\sigma_0^2}{\varrho_n}\mathbf{I}_{N_\mathrm{B}}\right)^{-1}\Bigg)\\ &= \ln\left(1+\frac{\left\|\sqrt{\beta_\mathrm{BA}}\mathbf{H}_{\mathrm{BA}_n}\mathbf{w}_n\right\|^2}{(1/\varrho_n)}\right) \qquad (30)\end{aligned}$$

where $\mathbf{w}_n \triangleq \sqrt{\frac{\mathbb{E}\{|x_n|^2\}}{\sigma_0^2}}\,\mathbf{a}_n = \sqrt{\frac{p_n}{\sigma_0^2}}\,\mathbf{a}_n$.

Let $\mathcal{I}_\mathrm{BA}\left(\mathbf{y}_\mathrm{B};\{x_n\}_{n=1,\ldots,N}\right)$ (or simply $\mathcal{I}_\mathrm{BA}$) be the total mutual information of the MIMO-OFDM subcarriers between Bob and Alice. From (27), we have [27]

$$\begin{aligned}\mathcal{I}_\mathrm{BA} &= \ln\det\Big(\mathbf{I}_{N_\mathrm{B}N} + \sqrt{\beta_\mathrm{BA}}\mathbf{H}_\mathrm{BA}\,\mathrm{diag}\left(\mathbf{a}\right)\\ &\quad\times\mathrm{diag}\big(\underbrace{p_1,\ldots,p_1}_{N_\mathrm{A}\text{ elements}},\ldots,\underbrace{p_N,\ldots,p_N}_{N_\mathrm{A}\text{ elements}}\big)\\ &\quad\times\left(\sqrt{\beta_\mathrm{BA}}\mathbf{H}_\mathrm{BA}\,\mathrm{diag}\left(\mathbf{a}\right)\right)^\dagger\left(\mathbf{C}_\mathrm{BA}\mathbf{J}\mathbf{C}_\mathrm{BA}^\dagger\right)^{-1}\Big)\\ &\overset{(a)}{=} \ln\det\Big(\mathbf{I}_{N_\mathrm{B}N} + \mathrm{blkdiag}\Big(\varrho_1\beta_\mathrm{BA}\mathbf{H}_{\mathrm{BA}_1}\mathbf{W}_1{\mathbf{H}_{\mathrm{BA}_1}}^\dagger,\\ &\quad\ldots,\ \varrho_N\beta_\mathrm{BA}\mathbf{H}_{\mathrm{BA}_N}\mathbf{W}_N{\mathbf{H}_{\mathrm{BA}_N}}^\dagger\Big)\Big)\\ &= \sum_{n=1}^{N}\mathcal{I}_{\mathrm{BA}_n} \qquad (31)\end{aligned}$$

where (a) is obtained by using (21) and the substitutions of $\mathbf{H}_\mathrm{BA} = \mathrm{blkdiag}\left\{\mathbf{H}_{\mathrm{BA}_1},\ldots,\mathbf{H}_{\mathrm{BA}_N}\right\}$ and $\mathbf{W}_n = (p_n/\sigma_0^2)\mathbf{a}_n\mathbf{a}_n^\dagger$.

B. Mutual Information Between Eve and Alice

From (13), the mutual information (in nats/OFDM block) of the nth MIMO-OFDM subcarrier between Eve and Alice can be expressed as follows:

$$\begin{aligned}&\mathcal{I}_{\mathrm{EA}_n}\left(\mathbf{y}_{\mathrm{E}_n};x_n\right) = \mathcal{I}_{\mathrm{EA}_n}\\ &= \ln\det\Big(\mathbf{I}_{N_\mathrm{E}} + \left(\sqrt{\beta_\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_n}\right)\mathbf{a}_n\,\mathbb{E}\left\{|x_n|^2\right\}\mathbf{a}_n^\dagger\\ &\quad\times\left(\sqrt{\beta_\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_n}\right)^\dagger\left(\sigma_0^2\Xi_n\right)^{-1}\Big)\\ &= \ln\Big(1+\beta_\mathrm{EA}\mathbf{w}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}^\dagger\,\Xi_n^{-1}\mathbf{H}_{\mathrm{EA}_n}\mathbf{w}_n\Big) \qquad (32)\end{aligned}$$

where

$$\begin{aligned}\Xi_n &\triangleq (\sigma^2/\sigma_0^2)\beta_\mathrm{EA}\mathbf{H}_{\mathrm{EA}_n}\mathbf{B}_n\mathbf{B}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}^\dagger\\ &\quad+\mathbf{C}_{\mathrm{E}_n}\left[(\widetilde{\sigma}^2/\sigma_0^2)\beta_\mathrm{EA}\mathbf{E}\mathbf{E}^\dagger+\mathbf{I}_{N_\mathrm{E}N}\right]\mathbf{C}_{\mathrm{E}_n}^\dagger,\\ \mathbf{E} &\triangleq \mathbf{F}_\mathrm{E}\mathbf{R}_\mathrm{E}^\mathrm{cp}\widetilde{\mathbf{H}}_\mathrm{EA}^\mathrm{cp}\mathbf{Q}.\end{aligned}$$

Note that Ξ_n is a positive definite matrix we can make singular value decomposition $\Xi_n = \mathbf{V}_n\mathbf{D}_n\mathbf{V}_n^\dagger$ with a nonegative diagonal matrix $\mathbf{D}_n$ and unitary matrix $\mathbf{V}_n$. Then

$$\Xi_n^{-1} = \mathbf{V}_n\mathbf{D}_n^{-1/2}\left(\mathbf{V}_n\mathbf{D}_n^{-1/2}\right)^\dagger$$

and $\mathcal{I}_{\mathrm{EA}_n}$ in (32) is expressed as

$$\begin{aligned}\mathcal{I}_{\mathrm{EA}_n} &= \ln\Big(1+\beta_{\mathrm{EA}}\mathbf{w}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}^\dagger\mathbf{V}_n\mathbf{D}_n^{-1/2}\\ &\quad\times\left(\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}\mathbf{w}_n\right)\Big)\\ &= \ln\left(1+\left\|\sqrt{\beta_{\mathrm{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\mathrm{EA}_n}\mathbf{w}_n\right\|^2\right). \quad (33)\end{aligned}$$

Meanwhile, the total mutual information $\mathcal{I}_{\mathrm{EA}}$ (in nats/OFDM block) of all MIMO-OFDM subcarriers between Eve and Alice can be deduced from (12) as follows:

$$\begin{aligned}\mathcal{I}_{\mathrm{EA}} &= \ln\det\Big(\mathbf{I}_{N_{\mathrm{E}}N}+\sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\ \mathrm{diag}(\mathbf{a})\\ &\quad\times\mathrm{diag}\big(\underbrace{p_1,\ldots,p_1}_{N_{\mathrm{A}}\text{ elements}},\ldots,\underbrace{p_N,\ldots,p_N}_{N_{\mathrm{A}}\text{ elements}}\big)\\ &\quad\times\left(\sqrt{\beta_{\mathrm{EA}}}\mathbf{H}_{\mathrm{EA}}\ \mathrm{diag}(\mathbf{a})\right)^\dagger\left(\sigma_0^2\Xi\right)^{-1}\Big)\\ &\overset{(a)}{=}\ln\det\Big(\mathbf{I}_{N_{\mathrm{E}}N}+\mathrm{blkdiag}\Big\{\beta_{\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_1}\mathbf{W}_1\mathbf{H}_{\mathrm{EA}_1}^\dagger\Xi_1^{-1},\\ &\quad\ldots,\beta_{\mathrm{EA}}\mathbf{H}_{\mathrm{EA}_N}\mathbf{W}_N\mathbf{H}_{\mathrm{EA}_N}^\dagger\Xi_N^{-1}\Big\}\Big)\\ &=\sum_{n=1}^{N}\mathcal{I}_{\mathrm{EA}_n} \quad (34)\end{aligned}$$

where

$$\begin{aligned}\Xi &= \frac{\sigma^2}{\sigma_0^2}\beta_{\mathrm{EA}}\mathbf{H}_{\mathrm{EA}}\mathbf{B}\mathbf{B}^\dagger\mathbf{H}_{\mathrm{EA}}^\dagger+\frac{\widetilde{\sigma}^2}{\sigma_0^2}\beta_{\mathrm{EA}}\mathbf{E}\mathbf{E}^\dagger+\mathbf{I}_{N_{\mathrm{E}}N}\\ &= (\sigma^2/\sigma_0^2)\beta_{\mathrm{EA}}\mathrm{blkdiag}\Big\{\mathbf{H}_{\mathrm{EA}_1}\mathbf{B}_1\mathbf{B}_1^\dagger\mathbf{H}_{\mathrm{EA}_1}^\dagger,\\ &\quad\ldots,\mathbf{H}_{\mathrm{EA}_N}\mathbf{B}_N\mathbf{B}_N^\dagger\mathbf{H}_{\mathrm{EA}_N}^\dagger\Big\}\\ &\quad+(\widetilde{\sigma}^2/\sigma_0^2)\beta_{\mathrm{EA}}\mathbf{E}\mathbf{E}^\dagger+\mathbf{I}_{N_{\mathrm{E}}N}\\ &= \mathrm{blkdiag}\left\{\Xi_1,\ldots,\Xi_N\right\}.\end{aligned}$$

The equality (a) is obtained by using the fact that $\Xi^{-1}=\mathrm{blkdiag}\left\{\Xi_1^{-1},\ldots,\Xi_N^{-1}\right\}$.

IV. Harvested Energy

In this section, we present the total energy that Bob harvests during the first and second portions.

Firstly, the harvested energy during the first portion can be calculated from (16) as follows:

$$\begin{aligned}\mathcal{E}_{\mathrm{cp}} &= \eta\tau^{\mathrm{cp}}\beta_{\mathrm{BA}}\ \mathrm{trace}\left\{\mathbf{C}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\,\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\}\left(\mathbf{C}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)^\dagger\right\}\\ &= \eta\tau^{\mathrm{cp}}\sigma_0^2\Big[\left\|\sqrt{\beta_{\mathrm{BA}}}\boldsymbol{\Upsilon}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{w}\right\|^2\\ &\quad+\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{cp}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{cp}}\right)^\dagger\right\}\Big] \quad (35)\end{aligned}$$

where $\boldsymbol{\Upsilon}^{\mathrm{cp}}=\mathbf{C}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}$. Secondly, from (18) we can also calculate the harvested energy during the second portion as follows:

$$\begin{aligned}\mathcal{E}_{\mathrm{PS}} &= \eta(K\tau_s)(1-\rho)\beta_{\mathrm{BA}}\mathbb{E}\left\{\left\|\mathrm{resize}1N_{\mathrm{B}}K\left\{\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\widetilde{\mathbf{s}}\right\}\right\|^2\right\}\\ &= \eta K\tau_s(1-\rho)\beta_{\mathrm{BA}}\\ &\quad\times\mathrm{trace}\left\{\mathbf{C}_1\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\,\mathbb{E}\left\{\widetilde{\mathbf{s}}\widetilde{\mathbf{s}}^\dagger\right\}\left(\mathbf{C}_1\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}\right)^\dagger\right\}\\ &= \eta\left(K\tau_s\right)\left(1-\rho\right)\\ &\quad\times\sigma_0^2\Big[\left\|\sqrt{\beta_{\mathrm{BA}}}\boldsymbol{\Upsilon}^{\mathrm{PS}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger\mathbf{w}\right\|^2\\ &\quad+\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{PS}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{PS}}\right)^\dagger\right\}\Big] \quad (36)\end{aligned}$$

where $\boldsymbol{\Upsilon}^{\mathrm{PS}}=\mathbf{C}_1\mathbf{R}_{\mathrm{B}}^{\mathrm{cp}}\widetilde{\mathbf{H}}_{\mathrm{BA}}^{\mathrm{cp}}$. Then, the total harvested energy can be given by

$$\begin{aligned}\mathcal{E}_{\mathrm{total}}\left(\rho,\mathbf{w}\right) &= \mathcal{E}_{\mathrm{cp}}+\mathcal{E}_{\mathrm{PS}}\\ &= \sigma_0^2\Big[-\rho\mathcal{E}_1+\mathcal{E}_2+\left\|\sqrt{\beta_{\mathrm{BA}}}\Gamma_1\mathbf{w}\right\|^2\\ &\quad+(1-\rho)\left\|\sqrt{\beta_{\mathrm{BA}}}\Gamma_2\mathbf{w}\right\|^2\Big]\\ &= \sigma_0^2\Big[-\rho\mathcal{E}_1+\mathcal{E}_2+\left\|\sqrt{\beta_{\mathrm{BA}}}\mathbf{M}\mathbf{w}\right\|^2\\ &\quad-\rho\left\|\sqrt{\beta_{\mathrm{BA}}}\Gamma_2\mathbf{w}\right\|^2\Big] \quad (37)\end{aligned}$$

where

$$2\mathcal{E}_1 = \eta K\tau_s\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{PS}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{PS}}\right)^\dagger\right\}, \quad (38a)$$

$$\mathcal{E}_2 = \mathcal{E}_1+\eta\tau^{\mathrm{cp}}\mathrm{trace}\left\{\boldsymbol{\Upsilon}^{\mathrm{cp}}\left(\beta_{\mathrm{BA}}\boldsymbol{\Lambda}\right)\left(\boldsymbol{\Upsilon}^{\mathrm{cp}}\right)^\dagger\right\}, \quad (38b)$$

$$\Gamma_1 = \sqrt{\eta\tau^{\mathrm{cp}}}\ \boldsymbol{\Upsilon}^{\mathrm{cp}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger, \quad (38c)$$

$$\Gamma_2 = \sqrt{\eta K\tau_s}\ \boldsymbol{\Upsilon}^{\mathrm{PS}}\mathbf{T}_{\mathrm{A}}^{\mathrm{cp}}\mathbf{F}_{\mathrm{A}}^\dagger, \quad (38d)$$

$$\mathbf{M}=\mathbf{M}^\dagger=\left(\Gamma_1^\dagger\Gamma_1+\Gamma_2^\dagger\Gamma_2\right)^{1/2}. \quad (38e)$$

V. Trade-off Problem Formulation

This section tackles the trade-off problems between the secure performance and the total harvested energy. Such trade-off problems will be presented in terms of optimization problems. For the purpose of comparing the performance of the system, we propose the following two maximization problems:

- Maximizing the difference

$$\Delta\left(\rho,\mathbf{w}\right)=\mathcal{I}_{\mathrm{BA}}-\mathcal{I}_{\mathrm{EA}}=\textstyle\sum_{n=1}^{N}\mathcal{I}_{\mathrm{BA}_n}-\sum_{n=1}^{N}\mathcal{I}_{\mathrm{EA}_n} \quad (39)$$

subject to $\mathcal{E}_{\mathrm{total}}$-based and power-based constraints. Herein, it must be noted that the achievable secrecy rate R_{sec} will be calculated as

$$R_{\mathrm{sec}}=\max\{0,\Delta\left(\rho,\mathbf{w}\right)\}. \quad (40)$$

Due to this relation, we only need to focus on $\Delta\left(\rho,\mathbf{w}\right)$ rather than R_{sec}. In short, our first problem is to

$$\begin{aligned}\underset{\rho,\mathbf{w}}{\text{maximize}}\quad & \Delta\left(\rho,\mathbf{w}\right) && (41a)\\ \text{subject to}\quad & \mathcal{E}_{\mathrm{total}}\left(\rho,\mathbf{w}\right)\geq\mathcal{E}_0, && (41b)\\ & \text{and (9).} && (41c)\end{aligned}$$

- Maximizing the total harvested energy $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ subject to Δ-based and power-based constraints. In particular, our second problem is to

$$\begin{aligned} 2 \quad \underset{\rho, \mathbf{w}}{\text{maximize}} \quad & \mathcal{E}_{\text{total}}(\rho, \mathbf{w}) && \text{(42a)} \\ \text{subject to} \quad & \Delta(\rho, \mathbf{w}) \geq \Delta_0, && \text{(42b)} \\ & \text{and (9).} && \text{(42c)} \end{aligned}$$

Note that $\mathcal{E}_0$ in (41b) and Δ_0 in (42b) are the desired energy and the desired secrecy rate, respectively. These two quantities reflect the quality-of-service of our secure scheme, and their values are pre-determined.

A. Inner Convex Approximations for Non-Convex Problems

The optimization problems (41) and (42) are non-convex because both the objective function $\Delta(\rho, \mathbf{w})$ in (39) and the objective function $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ in (37) are not concave, while both constraint (41b) and constraint (42b) are not convex. To address (41) and (42) we will employ inner convex approximation at each iteration. Let $(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)})$ be a feasible point for (41) or (42), which is found at the $(\kappa-1)$th iteration. At the κth iteration, we will

- Approximate $\Delta(\rho, \mathbf{w})$ in (39) by a lower bounding concave function $\Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w})$, which matches with $\Delta(\rho, \mathbf{w})$ at $\left(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}\right)$, i.e.

$$\Delta(\rho, \mathbf{w}) \geq \Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \quad \forall\ (\rho, \mathbf{w}) \tag{43}$$

and

$$\Delta(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}) = \Delta_{\text{lower}}^{(\kappa)}(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}). \tag{44}$$

- Approximate $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ in (37) by a lower bounding concave function $\mathcal{E}_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w})$, which matches with $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ at $\left(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}\right)$, i.e.

$$\mathcal{E}_{\text{total}}(\rho, \mathbf{w}) \geq \mathcal{E}_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \quad \forall\ (\rho, \mathbf{w}), \tag{45}$$

and

$$\mathcal{E}_{\text{total}}(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}) = \mathcal{E}_{\text{lower}}^{(\kappa)}(\rho^{(\kappa)}, \mathbf{w}^{(\kappa)}). \tag{46}$$

- Innerly approximate the nonconvex constraints (41b) and (42b) by the convex constraint

$$\mathcal{E}_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \geq \mathcal{E}_0, \tag{47}$$

and

$$\Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) \geq \Delta_0, \tag{48}$$

respectively. Indeed, it follows from (43) and (45) that any feasible point for the convex constraint (47) ((48), resp.) is also feasible for the nonconvex constraint (41b) ((42b), resp.).

Proposition 1: Let $x \in \mathbb{C}$, $\bar{x} \in \mathbb{C}$, $y > 0$ and $\bar{y} > 0$. The inequality

$$\begin{aligned} \ln\left(1 + \frac{|x|^2}{y}\right) \geq \ln\left(1 + \frac{|\bar{x}|^2}{\bar{y}}\right) - \frac{|\bar{x}|^2}{\bar{y}} \\ + 2\frac{\Re\{\bar{x}^* x\}}{\bar{y}} - \frac{|\bar{x}|^2}{\bar{y}\left(\bar{y} + |\bar{x}|^2\right)}\left(y + |x|^2\right) \end{aligned} \tag{49}$$

holds true [9]. The RHS of (49) *is a concave function [28].*

Proposition 2: For $x > 0$ and $\bar{x} > 0$, the inequality

$$\ln(1 + x) \leq \ln(1 + \bar{x}) - \frac{\bar{x}}{1 + \bar{x}} + \frac{x}{1 + \bar{x}} \tag{50}$$

always holds true. The RHS of (50) *is a convex function of x.* Note that (50) holds true because its RHS is the first-order Taylor approximation of its left hand side (LHS), which is a concave function [28].

1) Obtaining $\Delta_{lower}^{(\kappa)}(\rho, \mathbf{w})$: Applying Proposition 1 to $\mathcal{I}_{\text{BA}_n}$ in (30) yields

$$\begin{aligned} \mathcal{I}_{\text{BA}_n} \geq \ln & \left(1 + \frac{\left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2}{1\Big/\varrho_n^{(\kappa)}}\right) \\ & - \frac{\left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2}{1\Big/\varrho_n^{(\kappa)}} \\ & - \frac{\left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2 \left(\frac{1}{\varrho_n} + \left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n\right\|^2\right)}{1\Big/\varrho_n^{(\kappa)}\left(1\Big/\varrho_n^{(\kappa)} + \left\|\sqrt{\beta_{\text{BA}}}\mathbf{H}_{\text{BA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2\right)} \\ \triangleq\ & f^{(\kappa)}(\mathbf{w}_n, \varrho_n) \\ =\ & \begin{cases} f^{(\kappa)}(\mathbf{w}_n, \rho) & \text{if } 1 \leq n \leq K \\ f^{(\kappa)}(\mathbf{w}_n, 1) & \text{if } K+1 \leq n \leq N \end{cases} \end{aligned} \tag{51}$$

At the same time, applying Proposition 2 yields

$$\begin{aligned} \mathcal{I}_{\text{EA}_n} \leq & \ln\left(1 + \left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2\right) \\ & - \frac{\left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2}{1 + \left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2} \\ & + \frac{\left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n\right\|^2}{1 + \left\|\sqrt{\beta_{\text{EA}}}\mathbf{D}_n^{-1/2}\mathbf{V}_n^\dagger\mathbf{H}_{\text{EA}_n}\mathbf{w}_n^{(\kappa)}\right\|^2} \\ \triangleq\ & g^{(\kappa+1)}(\mathbf{w}_n). \end{aligned} \tag{52}$$

Using (39), (51) and (52), the concave function

$$\begin{aligned} \Delta_{\text{lower}}^{(\kappa)}(\rho, \mathbf{w}) = & \sum_{n=1}^{K} f^{(\kappa)}(\mathbf{w}_n, \rho) + \sum_{n=K+1}^{N} f^{(\kappa)}(\mathbf{w}_n, 1) \\ & - \sum_{n=1}^{N} g^{(\kappa)}(\mathbf{w}_n) \end{aligned} \tag{53}$$

satisfies (43) and (44) and thus is qualified as a lower bounding approximation of $\Delta_{\text{lower}}(\rho, \mathbf{w})$.

2) Obtaining $\mathcal{E}_{lower}^{(\kappa)}(\rho, \mathbf{w})$: Let $\mathbf{M} = [\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_{N_{\text{A}}N}]$ with $\mathbf{m}_i$ being the ith column of $\mathbf{M}$. One can derive the following inequality:

$$\begin{aligned} \|\mathbf{M}\mathbf{w}\|^2 = \|\mathbf{M}^\dagger\mathbf{w}\|^2 &= \sum_{i=1}^{N_{\text{A}}N} \left|\mathbf{m}_i^\dagger\mathbf{w}\right|^2 \\ &\geq 2\sum_{i=1}^{N_{\text{A}}N} \Re\left\{(\mathbf{m}_i^\dagger\mathbf{w}^{(\kappa)})^*(\mathbf{m}_i^\dagger\mathbf{w})\right\} - \left\|\mathbf{M}^\dagger\mathbf{w}^{(\kappa)}\right\|^2 \\ &\triangleq (1/\beta_{\text{BA}})\,\eth^{(\kappa+1)}(\mathbf{w}) \end{aligned} \tag{54}$$

over the trust region

$$2\Re\left\{(\mathbf{m}_i^\dagger \mathbf{w}^{(\kappa)})^*(\mathbf{m}_i^\dagger \mathbf{w})\right\} - |\mathbf{m}_i^\dagger \mathbf{w}^{(\kappa)}|^2 > 0, i = 1, \ldots, N_{\mathrm{A}}N. \tag{55}$$

Substituting (54) into (37), we can obtain

$$\begin{aligned}
&\mathcal{E}_{\text{total}}(\rho, \mathbf{w}) \\
&\geq \sigma_0^2 \left[-\rho\mathcal{E}_1 + \mathcal{E}_2 + \eth^{(\kappa+1)}(\mathbf{w}) - \rho \left\| \sqrt{\beta_{\text{BA}}}\Gamma_2 \mathbf{w} \right\|^2 \right] \\
&= \sigma_0^2 \left[\mathcal{E}_2 + \eth^{(\kappa+1)}(\mathbf{w}) - \left\| \begin{bmatrix} \sqrt{\mathcal{E}_1} \\ \sqrt{\beta_{\text{BA}}}\,\Gamma_2 \mathbf{w} \end{bmatrix} \right\|^2 \Big/ \rho_{\text{inv}} \right] \\
&\triangleq \mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w})
\end{aligned} \tag{56}$$

where

$$\rho_{\text{inv}} \triangleq \frac{1}{\rho} \geq 1, \tag{57}$$

verifying (45) and (46), making $\mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w})$ qualified as a lower bounding approximation of $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$.

3) Algorithms and Convergence: At the κ-th the iteration we solve the following convex optimization problems to generate the next feasible point $\left(\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}\right)$ for (41) and (42), respectively:

$$\begin{aligned}
2 \quad \underset{\rho_{\text{inv}}, \mathbf{w}}{\text{maximize}} \quad & \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w}) && \text{(58a)} \\
\text{subject to} \quad & \mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \mathcal{E}_0, && \text{(58b)} \\
& (9), (55), (57) && \text{(58c)}
\end{aligned}$$

and

$$\begin{aligned}
2\text{maximize} \quad \underset{\rho_{\text{inv}}, \mathbf{w}}{} \quad & \mathcal{E}_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}, \mathbf{w}) && \text{(59a)} \\
\text{subject to} \quad & \Delta_{\text{lower}}^{(\kappa+1)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \Delta_0, && \text{(59b)} \\
& (9), (55), (57). && \text{(59c)}
\end{aligned}$$

Note that the convex constraints (58b) and (59b) correspond to the convex constraints (47) and (48), respectively. Furthermore, we have

$$\Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}) > \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)}) \tag{60}$$

where $(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)})$ is the optimal solution of (58) and $(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)})$ is a feasible point for (58), which together with (43) and (44) yield

$$\begin{aligned}
\Delta_{\text{lower}}(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}) &\geq \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}) \\
&> \Delta_{\text{lower}}^{(\kappa)}(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)}),
\end{aligned} \tag{61}$$

i.e. $(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)})$ is a better feasible point than $(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)})$ for (41). Therefore, Algorithm 1, which generates the sequence $\{(1/\rho_{\text{inv}}^{(\kappa)}, \mathbf{w}^{(\kappa)})\}$, at least converges to a locally optimal solution of (41) [9, Proposition 2]).

Analogously, Algorithm 2 at least converges to a locally optimal solution of (42). Once initialized from an initial feasible point, both algorithms converge after a few iterations for a given error tolerance.

Convergence: The problem (58) includes two variables ρ and $\mathbf{w}$. Given that $\mathbf{w}$ is a vector of $N_{\mathrm{A}}N$ complex elements, the total number of scalar variables is equal to $2\ N_{\mathrm{A}}N + 1$. Herein, the real part and the imaginary part of each complex element in $\mathbf{w}$ are considered as independent variables. The number of quadratic constraints is equal to $\epsilon_1 = 2$. Thus, the per-iteration computational complexity of Algorithm 1 is $\mathcal{O}\left((2\ N_{\mathrm{A}}N + 1)^2\epsilon_1^{2.5} + \epsilon_1^{3.5}\right)$ [29, Ch. 10]. Likewise, Algorithm 2 is also invoked to resolve (59). With $2N_{\mathrm{A}}N+1$ distinct variables and $\epsilon_2 = 2$ quadratic constraints, the per-iteration cost is $\mathcal{O}\left((2\ N_{\mathrm{A}}N + 1)^2\epsilon_2^{2.5} + \epsilon_2^{3.5}\right)$.

Algorithm 1 Path-Following Algorithm for (41)

1: **Initialization**: Set $\kappa = 0$ with an initial feasible point $\left\{\rho_{\text{inv}}^{(0)}, \mathbf{w}^{(0)}\right\}$ for (41) (see Appendix A).
2: **repeat**
3: At the $(\kappa+1)$th iteration, solve the inner convex approximation problem (58) to obtain the optimal values $\rho_{\text{inv}}^{(\kappa+1)}$ and $\mathbf{w}^{(\kappa+1)}$ of variables ρ_{inv} and $\mathbf{w}$, respectively.
4: Reset $\kappa := \kappa + 1$.
5: **until** $\left|\Delta_{\text{lower}}^{(\kappa+1)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa+1)}}, \mathbf{w}^{(\kappa+1)}\right) - \Delta_{\text{lower}}^{(\kappa)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa)}}, \mathbf{w}^{(\kappa)}\right)\right|$ converges.
6: **return** $(\rho^*, \mathbf{w}^*) = \left(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}\right)$ as the desired feasible point for (41).

Algorithm 2 Path-Following Algorithm for (42)

1: **Initialization**: Set $\kappa = 0$ with an initial feasible point $\left\{\rho_{\text{inv}}^{(0)\text{th}}, \mathbf{w}^{(0)\text{th}}\right\}$ for (42) (see Appendix B).
2: **repeat**
3: At the $(\kappa+1)$th iteration, solve the inner convex approximation problem (59) to obtain the optimal values $\rho_{\text{inv}}^{(\kappa+1)}$ and $\mathbf{w}^{(\kappa+1)}$ of variables ρ_{inv} and $\mathbf{w}$, respectively.
4: Reset $\kappa := \kappa + 1$.
5: **until** $\left|\mathcal{E}_{\text{lower}}^{(\kappa+1)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa+1)}}, \mathbf{w}^{(\kappa+1)}\right) - \mathcal{E}_{\text{lower}}^{(\kappa)}\left(\frac{1}{\rho_{\text{inv}}^{(\kappa)}}, \mathbf{w}^{(\kappa)}\right)\right|$ converges.
6: **return** $(\rho^*, \mathbf{w}^*) = \left(1/\rho_{\text{inv}}^{(\kappa+1)}, \mathbf{w}^{(\kappa+1)}\right)$ as the desired feasible point for (42).

VI. Numerical Results

In this section, we provide numerical results to evaluate the performance of proposed maximization problems. More particularly, we draw the *average* curves of the achievable secrecy rate $R_{\text{sec}}(\rho, \mathbf{w}) = \max\{0, \Delta(\rho, \mathbf{w})\}$ and the total harvested energy $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ over numerous realizations of $\beta_{\text{BA}}, \beta_{\text{EA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N$ and $\{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N$.

While the realization of $\left\{\beta_{\text{BA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N\right\}$ implies the *instantaneous* observation of the channel between Alice and Bob, the realization of $\left\{\beta_{\text{EA}}, \{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N\right\}$ corresponds to *instantaneous* observation of the Alice-Eve channel at the time of measurement. Note that Algorithm 1 and Algorithm 2 are conducted in the case that $\beta_{\text{BA}}, \beta_{\text{EA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N$ and $\{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N$ are given. Let $\{\rho^\star, \mathbf{w}^\star\}$ be one of the feasible solutions after running Algorithm 1 (or Algorithm 2). Then, our goals are to evaluate

$$\begin{aligned}
R_{\text{sec}}^{\text{avr}} &= \mathbb{E}_{\{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N, \{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N}\left\{R_{\text{sec}}(\rho^*, \mathbf{w}^*)\right\}, \\
\mathcal{E}_{\text{total}}^{\text{avr}} &= \mathbb{E}_{\{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N, \{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N}\left\{\mathcal{E}_{\text{total}}(\rho^*, \mathbf{w}^*)\right\}.
\end{aligned}$$

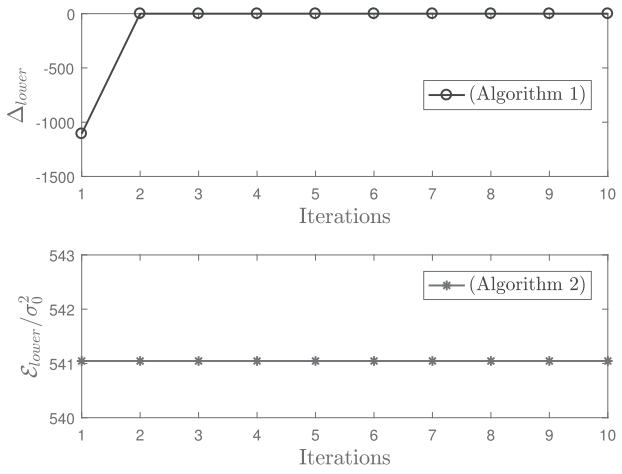

Fig. 2. The convergence rate of the proposed algorithms. Other parameters: $N = 10$, $K = 2$, and $\{P_A, \sigma^2, \bar{\sigma}^2\} = \{30, 10, 10\}$ dBm.

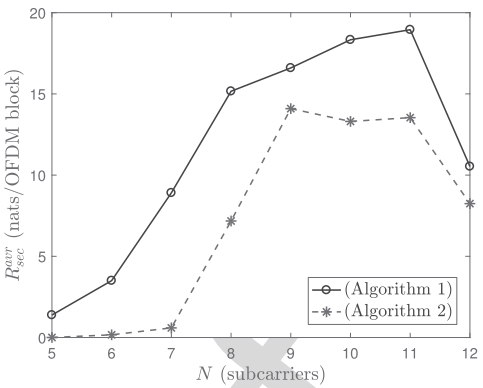

Fig. 3. The achievable secrecy rate R_{sec} as a function of the number of subcarriers N. Other system parameters: $K = 2$ and $\{P_A, \sigma^2, \bar{\sigma}^2\} = \{30, 10, 10\}$ dBm.

In short, the use of Algorithm 1 (or Algorithm 2, respectively) to solve (58) (or (59), respectively) yields a certain point $\{\rho^\star, \mathbf{w}^\star\}$. Then, the substitution $\rho = \rho^\star, \mathbf{w} = \mathbf{w}^\star$ into the expressions of R_{sec} and $\mathcal{E}$ will yield the instantaneous values at the time of measurement. Generating sufficiently large number of realizations of $\beta_{\text{BA}}, \beta_{\text{EA}}, \{\mathbf{G}_{\text{BA}_l}\}_{l=1}^N$ and $\{\mathbf{G}_{\text{EA}_l}\}_{l=1}^N$, we can calculate the average values for the secrecy rate and harvested energy.

In simulation, the time-domain fading channel matrices $\mathbf{G}_{\text{BA}_l}$ and $\mathbf{G}_{\text{EA}_l}$ can be assumed to be symmetric complex Gaussian random variables. More particularly, we assume $\mathbf{G}_{\text{BA}_l} \sim \mathcal{CN}(0,1)$ and $\mathbf{G}_{\text{EA}_l} \sim \mathcal{CN}(0,1)$ for $\forall l \in \{1, \ldots, L\}$. The values of β_{BA} and β_{EA} rely on the rule of power degradation and the shadowing fading effect. For instance, if the distance between two transceivers is below 50 meters, the path loss can be around -90 dB. That may lead to $\beta_{\text{BA}} = 10^{(-90+\mathcal{S}_{\text{BA}})/10}$, and $\beta_{\text{EA}} = 10^{(-90+\mathcal{S}_{\text{EA}})/10}$ where $\mathcal{S}_{\text{BA}}$ and $\mathcal{S}_{\text{EA}}$ represent the shadowing. For simplicity, let us set $\mathcal{S}_{\text{BA}} = \mathcal{S}_{\text{EA}} = 10$. Other simulation parameters are as follows: $N_{\text{cp}} = 3$, $N_{\text{A}} = 6$, $N_{\text{B}} = 3$, $N_{\text{E}} = 4$, $L = 3$, $\sigma_0^2 = -80$ dBm, $\tau_s = 0.1$ s, $\eta = 80\%$, $\Delta_0 = 0$, and $\mathcal{E}_0 = 20\ \sigma_0^2$.

Fig. 2 illustrates the convergence rate for each of the proposed algorithms. It is not surprising that Algorithm 1 and Algorithm 2 converge within only 2 iterations because of the fact that (58) and (59) contain only quadratic and linear constraints.

Fig. 3 shows the relation between $R_{\text{sec}}^{\text{avr}}$ and N. The largest value of $R_{\text{sec}}^{\text{avr}}$ is obtained at $N = 11$ in the case of Algorithm 1. Meanwhile, $R_{\text{sec}}^{\text{avr}}$ takes the largest value at $N = 9$ subcarriers in the case of Algorithm 2. The curve of Algorithm 1 shows an uptrend with $N \in \{5, \ldots, 11\}$ but start a strong downtrend at $N = 12$. While the curve of Algorithm 2 is in an uptrend with $N \in \{5, \ldots, 9\}$, then slightly reducing at $N = 10$, increasing at $N = 11$ before reducing again at $N = 12$. Lastly, on average, Algorithm 1 provides higher secrecy rate than Algorithm 2.

In Fig. 4, the relation between $\mathcal{E}_{\text{total}}^{\text{avr}}$ and N is illustrated. We can see that Algorithm 1 is better than Algorithm 2 in terms of energy-harvesting. In fact, $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 1 is higher than $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 2 by the amount of above $30\sigma_0^2$ at each value of N; however, the values of $\mathcal{E}_{\text{total}}^{\text{avr}}$ in both algorithms are nearly the same at $N = 12$. For Algorithm 1, $\mathcal{E}_{\text{total}}^{\text{avr}}$ increases with $N \in \{5, 6, 7\}$ and decreases with $N \in \{8, \ldots, 12\}$. As for Algorithm 2, $\mathcal{E}_{\text{total}}^{\text{avr}}$ reaches a peak of $\mathcal{E}_{\text{total}}^{\text{avr}} = 384\sigma_0^2$ when $N = 9$.

In order to achieve the balance between $R_{\text{sec}}^{\text{avr}}$ and $\mathcal{E}_{\text{total}}^{\text{avr}}$, we observe Figs. 3–4 and suggest using either $N = 8$ for Algorithm 1 or $N = 9$ for Algorithm 2. Note that the system parameters used in these two figures are the same. Also in Figs. 3–4, the gap between the two algorithms tends to become closer when N increases. The curves are not increasing/decreasing monotonic, but they fluctuate with respect with N.

In Fig. 5, the relation between $R_{\text{sec}}^{\text{avr}}$ and K is shown. $R_{\text{sec}}^{\text{avr}}$ in Algorithm 1 reaches the highest peak at $K = 2$ and then steadily goes down; while $R_{\text{sec}}^{\text{avr}}$ in Algorithm 2 always decreases with all values of K. When compared with each other, the first proposed algorithm shows its superiority over the other at $K = \{1, \ldots, 4\}$, and both of algorithms reduce to zero at $K = \{7, 8\}$. The curves in Fig. 5 suggest choosing a small value of K to gain a satisfactory amount of the average secrecy rate.

In Fig. 6, the relation between $\mathcal{E}_{\text{total}}^{\text{avr}}$ and K is depicted. Once again, Algorithm 1 is superior to Algorithm 2 at all integer values of K, although the formulation of Algorithm 2 is inherently intended for maximizing the harvested energy. In reality, Algorithm 2 sometimes results in the instantaneously harvested energy better than Algorithm 1 at some realization of channels; however, on average, $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 2 is much lower than $\mathcal{E}_{\text{total}}^{\text{avr}}$ in Algorithm 1. Noticeably, even when we make use of the PS SWIPT scheme for all $N_{\text{B}}N$ informative samples by setting $K = N = 8$, the amount of harvested energy is not really among the highest ones, e.g. $\mathcal{E}_{\text{total}}^{\text{avr}}$ at $K = 8$ is worse than at $K = \{2, 3, 4\}$.

It can be seen from Figs. 5–6 that Algorithm 1 brings about much better system performance than Algorithm 2 in terms of both security and energy. Thus, we suggest using Algorithm 1 with the used parameters. Once Algorithm 1 has been used, the best value of K is $K = 2$ because this value

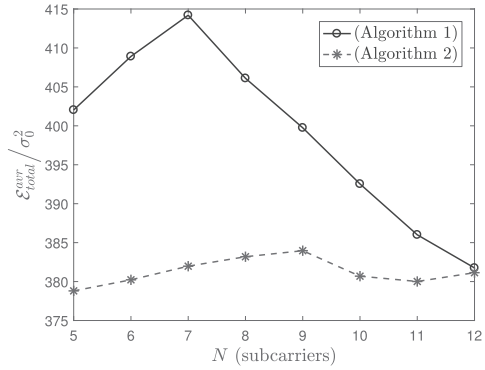

Fig. 4. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the number of subcarriers N. Other system parameters: $K = 2$ and $\{P_A, \sigma^2, \widetilde{\sigma}^2\} = \{30, 10, 10\}$ dBm.

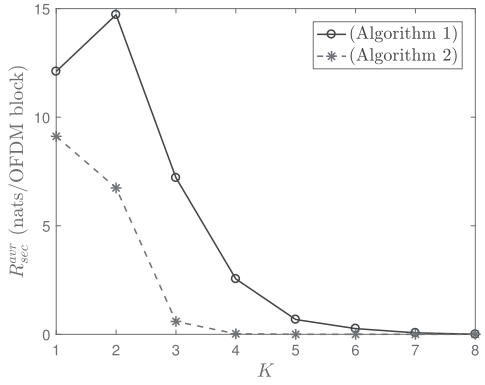

Fig. 5. The achievable secrecy rate R_{sec} as a function of the parameter K. Other system parameters: $N = 8$ and $\{P_A, \sigma^2, \widetilde{\sigma}^2\} = \{30, 10, 10\}$ dBm.

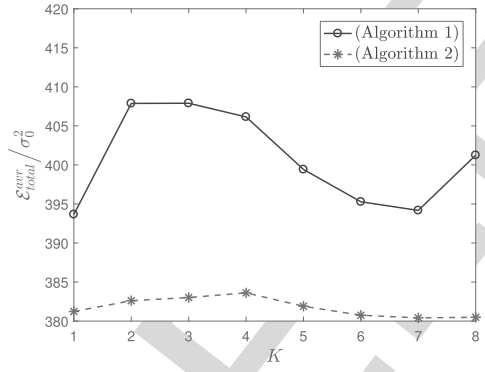

Fig. 6. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter K. Other system parameters: $N = 8$ and $\{P_A, \sigma^2, \widetilde{\sigma}^2\} = \{30, 10, 10\}$ dBm.

can lead to a good balance between highly achievable $R_{\text{sec}}^{\text{avr}}$ and $\mathcal{E}_{\text{total}}^{\text{avr}}$, i.e., $\left\{R_{\text{sec}}^{\text{avr}}, \frac{\mathcal{E}_{\text{total}}^{\text{avr}}}{\sigma_0^2}\right\} \approx \{14.7 \text{ nats/OFDM block}, 407.8\}$ at $K = 2$.

Fig. 7 shows that Algorithm 1 is superior to Algorithm 2 in terms of security in both considered sub-cases of. Regarding Algorithm 1, the changes in values are quite significant with $P_A \in (21, 28)$ dBm. Meanwhile, Algorithm 2 shows the slight difference between two sub-cases. When considering the first sub-case, one can see that the secure performance of Algorithm 1 is only slightly lower than Algorithm 2 at moderate $P_A \in (23, 25)$ dBm, but it is much higher than Algorithm 2 at high P_A. For the second sub-case, Algorithm 1 is almost better than Algorithm 2 at all values of P_A.

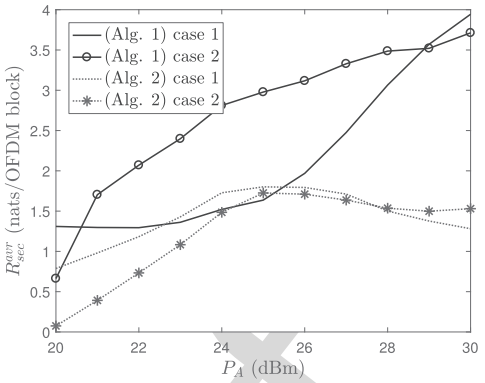

Fig. 7. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 3\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

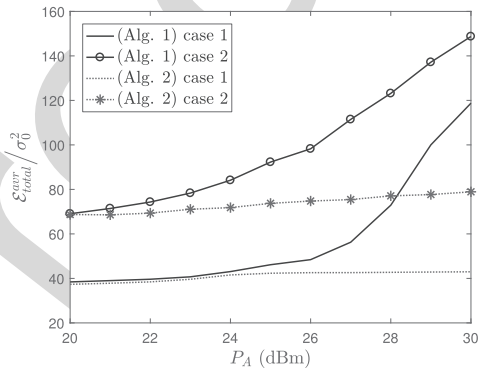

Fig. 8. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 3\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

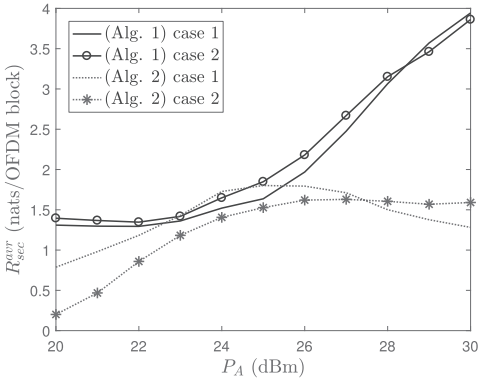

Fig. 9. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{2, 0\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

Fig. 8 shows that $\mathcal{E}_{\text{total}}^{\text{avr}}$ increases with P_A. Besides, the achieved values of $\mathcal{E}_{\text{total}}^{\text{avr}}$ in case 1 (with $\widetilde{\sigma}^2 = 0$ dBm) are lower than those in case 2 (with $\widetilde{\sigma}^2 = 3$ dBm). Interestingly, we can see that the larger $\widetilde{\sigma}^2$ (i.e., the more power we spend on generating the temporal AN $\widetilde{\mathbf{d}}$), the more energy Bob can

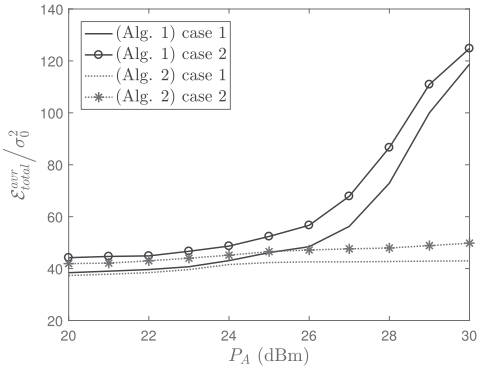

Fig. 10. The ratio of total harvested energy $\mathcal{E}_{\text{total}}^{\text{avr}}$ to σ_0^2 as a function of the parameter P_A. Two sub-cases are considered. In the first sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{-2, 0\}$ dBm. The second sub-case, we set $\{\sigma^2, \widetilde{\sigma}^2\} = \{2, 0\}$ dBm. Other system parameters: $N = 7$ and $K = 3$.

harvest. From Figs. 7–8, one can see that the difference in performance between Algorithm 1 and Algorithm 2 expands when P_A increases.

Both Fig. 9 and Fig. 10 confirm the superiority of Algorithm 1 over Algorithm 2 in terms of security and harvested energy, especially at high P_A. Moreover, Fig. 9 shows that the secure performance is not proportional to σ^2. This means that assigning more power to the frequency-domain AN may not help improve security level. While the energy efficiency seems to be proportional to the increase in σ^2 as shown in Fig. 10. When comparing Figs. 8 and 10, it is observed that in terms of energy, the power allocation for σ^2 (see Fig. 10) brings about worse performance than the power allocation for $\widetilde{\sigma}^2$ (see Fig. 8) does. This observation implies that instead of increasing σ^2 by the amount of 4 dBm, it is preferable to increase $\widetilde{\sigma}^2$ by the amount of 3 dBm.

VII. Conclusion

In this paper, we have analyzed a MIMO-OFDM SWIPT network and proposed two types of maximization problems to improve secrecy rate and harvested energy, respectively. Two path-following iterative algorithms of low computational complexity have been also provided to solve two different non-convex problems, whereby the sub-optimal solutions $(\rho^*, \mathbf{w}^*)$ have been given. The impact of other key parameters, related to the aspects of security and energy-harvesting, have been also evaluated through numerical results. Overall, we observed that the system performance is not proportional to N, K, σ^2 and $\widetilde{\sigma}^2$; thus the choice of these parameters will pose challenges to designers. In contrast, the system performance is enhanced with the increase in the power budget P_A. Moreover, it will be the responsibility of designers to choose the most suitable algorithm, because each algorithm results in a different performance. With the used parameters in this paper, we suggest using Algorithm 1 because it is superior to Algorithm 2 in resolving the trade-off problem between security and energy-harvesting. In the future, it is worth considering the impact of non-linear EH models on the secure performance of MIMO-OFDM SWIPT networks since such models reflect better the practical utility of EH circuits/receivers. Borrowing the idea of using machine learning and EH history to predict renewable energy generation trends [30], we can also consider making predictions about the amount of information leakage for future work.

Appendix

A. Locating an Initial Feasible Point for (41)

A feasible point for (41) must satisfy (41b) and (41c). Due to the non-convexity of (41b), we invoke once again the inner convex approximation by replacing $\mathcal{E}_{\text{total}}(\rho, \mathbf{w})$ with $\mathcal{E}_{\text{lower}}^{(\vartheta+1)}(1/\rho_{\text{inv}}, \mathbf{w})$ at the $(\vartheta+1)$th iteration. In parallel, the accompanying constraint (55) (in which κ must be replaced with ϑ) are needed. In short, a feasible point for (41) can be found by solving the following inner convex approximation problem:

$$\begin{aligned} 2 \quad \underset{\rho_{\text{inv}}, \mathbf{W}}{\text{maximize}} \quad & 1 && \text{(62a)} \\ \text{subject to} \quad & \mathcal{E}_{\text{lower}}^{(\vartheta+1)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \mathcal{E}_0, && \text{(62b)} \\ & (9), (55), (57) && \text{(62c)} \end{aligned}$$

at the $(\vartheta+1)$th iteration. The above-proposed problem is to find an initial feasible point for Algorithm 1, but this problem itself requires an initial point to run. To find its own initial point, we simply find $(\rho_{\text{inv}}, \mathbf{w})$ satisfying (9), (55) and (57).

B. Locating an Initial Feasible Point for (42)

Similar to Appendix A, at the $(\vartheta+1)$th iteration, we need to solve the following inner convex approximation problem to find an initial feasible of (42):

$$\begin{aligned} 2 \quad \underset{\rho_{\text{inv}}, \mathbf{W}}{\text{maximize}} \quad & 1 && \text{(63a)} \\ \text{subject to} \quad & \Delta_{\text{lower}}^{(\vartheta+1)}(1/\rho_{\text{inv}}, \mathbf{w}) \geq \Delta_0, && \text{(63b)} \\ & (9), (57). && \text{(63c)} \end{aligned}$$

References

[1] T. M. Hoang, A. El Shafie, T. Q. Duong, H. D. Tuan, and A. Marshall, "Security in MIMO–OFDM SWIPT networks," in *Proc. IEEE 29th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Bologna, Italy, Sep. 2018, pp. 1–6.

[2] K. Xiao, L. Gong, and M. Kadoch, "Opportunistic multicast NOMA with security concerns in a 5G massive MIMO System," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 91–95, Mar. 2018.

[3] R. Chaudhary, N. Kumar, and S. Zeadally, "Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 114–122, Nov. 2017.

[4] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[5] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State-of-the-art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015.

[6] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," *IEEE Commun. Surveys Tutr.*, vol. 20, no. 1, pp. 264–302, 1st Quart., 2018.

[7] Q. Liu, K. S. Yildirim, P. Pawełczak, and M. Warnier, "Safe and secure wireless power transfer networks: Challenges and opportunities in RF-based systems," *IEEE Commun. Mag.*, vol. 54, no. 9, pp. 74–79, Sep. 2016.

[8] T. O. Olwal, K. Djouani, and A. M. Kurien, "A survey of resource management toward 5G radio access networks," *IEEE Commun. Surveys Tutr.*, vol. 18, no. 3, pp. 1656–1686, 3rd Quart., 2016.

[9] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 677–689, Feb. 2017.

[10] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secure and energy–efficient beamforming for simultaneous information and energy transfer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 11, pp. 7523–7537, Nov. 2017.

[11] J. Qiao, H. Zhang, X. Zhou, and D. Yuan, "Joint beamforming and time switching design for secrecy rate maximization in wireless–powered FD relay systems," *IEEE Trans. Veh. Technol.*, vol. 67, no. 1, pp. 567–579, Jan. 2018.

[12] Z. Zhu, Z. Chu, N. Wang, S. Huang, Z. Wang, and I. Lee, "Beamforming and power splitting designs for an–aided secure multi–user MIMO SWIPT systems," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 12, pp. 2861–2874, Dec. 2017.

[13] E. V. Belmega and A. Chorti, "Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 11, pp. 2611–2626, Nov. 2017.

[14] T. M. Hoang, T. Q. Duong, N.-S. Vo, and C. Kundu, "Physical layer security in cooperative energy harvesting networks with a friendly Jammer," *IEEE Wireless Commun. Lett.*, vol. 6, no. 2, pp. 174–177, Apr. 2017.

[15] A. Salem, K. A. Hamdi, and K. M. Rabie, "Physical layer security with RF energy harvesting in AF multi–antenna relaying networks," *IEEE Trans. Commun.*, vol. 64, no. 7, pp. 3025–3038, Jul. 2016.

[16] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, Apr. 2016.

[17] G. Zhang, J. Xu, Q. Wu, M. Cui, X. Li, and F. Lin, "Wireless powered cooperative Jamming for secure OFDM system," *IEEE Trans. Veh. Technol.*, vol. 67, no. 2, pp. 1331–1346, Feb. 2018.

[18] A. El Shafie, K. Tourki, and N. Al-Dhahir, "An artificial-noise-aided hybrid TS/PS scheme for OFDM–based SWIPT Systems," *IEEE Commun. Lett.*, vol. 21, no. 3, pp. 632–635, Mar. 2017.

[19] E. Boshkovska, D. W. K. Ng, N. Zlatanov, A. Koelpin, and R. Schober, "Robust resource allocation for MIMO wireless powered communication networks based on a non–linear EH model," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 1984–1999, May 2017.

[20] Y. Zeng, B. Clerckx, and R. Zhang, "Communications and signals design for wireless power transmission," *IEEE Trans. Commun.*, vol. 65, no. 5, pp. 2264–2290, May 2017.

[21] P. N. Alevizos and A. Bletsas, "Sensitive and nonlinear far–field RF energy harvesting in wireless communications," *IEEE Trans. Wireless Commun.*, vol. 17, no. 6, pp. 3670–3685, Jun. 2018.

[22] J. Gong and X. Chen, "Achievable rate region of non–orthogonal multiple access systems with wireless powered decoder," *IEEE J. Select. Areas Commun.*, vol. 35, no. 12, pp. 2846–2859, Dec. 2017.

[23] A. El Shafie, Z. Ding, and N. Al-Dhahir, "Hybrid spatio-temporal artificial noise design for secure MIMOME-OFDM systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3871–3886, May 2017.

[24] A. Van Zelst and T. Schenk, "Implementation of a MIMO OFDM–based wireless LAN system," *IEEE Trans. Signal Process.*, vol. 52, no. 2, pp. 483–494, Feb. 2004.

[25] Y. Yao and G. Giannakis, "Blind carrier frequency offset estimation in SISO, MIMO, and multiuser OFDM systems," *IEEE Trans. Commun.*, vol. 53, no. 1, pp. 173–183, Jan. 2005.

[26] G. Caire and S. Shamai, "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1691–1706, Jul. 2003.

[27] H. Bolcskei, D. Gesbert, and A. J. Paulraj, "On the capacity of OFDM-based spatial multiplexing systems," *IEEE Trans. Commun.*, vol. 50, no. 2, pp. 225–234, Feb. 2002.

[28] H. Tuy, *Convex Analysis and Global Optimization,*, 2nd ed. Springer, 2016.

[29] A. Nemirovski. (2004). *Interior Point Polynomial Time Methods in Convex Programming*. [Online]. Available: https://www2.isye.gatech.edu/~nemirovs/Lect_IPM.pdf

[30] M. Min, L. Xiao, Y. Chen, P. Cheng, D. Wu, and W. Zhuang, "Learning–based computation offloading for IoT devices with energy harvesting," *IEEE Trans. Veh. Technol.*, vol. 68, no. 2, pp. 1930–1941, Feb. 2019.

AQ:6

Tiep M. Hoang received the B.Eng. degree in electronics and electrical engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2012, the M.Eng. degree in electronics and radio engineering from Kyung Hee University, South Korea, in 2014, and the Ph.D. degree from the Queen's University Belfast, U.K., in 2019. His current research interests include wireless security, massive multiple-input–multiple-output (MIMO), stochastic geometry, convex optimization, and the application of machine learning in wireless communications.

Ahmed El Shafie (Senior Member, IEEE) received the B.Sc. degree (Hons.) in electrical engineering from Alexandria University, Alexandria, Egypt, in 2009, the M.Sc. degree in communication and information technology from Nile University, Cairo, Egypt, in 2014, and the Ph.D. degree from The University of Texas at Dallas, Richardson, TX, USA, in 2018. Since 2018, he has been a Senior Systems Engineer with Qualcomm Technologies, San Diego, CA, USA. He was a recipient of the David Daniel Best Doctoral Thesis Award in 2018 and the Jonsson School Industrial Advisory Council Fellowship Award in 2017. He received IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer in 2015, 2016, and 2017, and the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer in 2016. He received the Qualcomm Star (Qualstar) Awards in February 2019, October 2019, and November 2019. He was nominated for the 2018 CGS/ProQuest Distinguished Dissertation Award. He currently serves as an Editor for IEEE COMMUNICATIONS LETTERS, IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY (IEEE OJ-COM), *Physical Communication*, and *Transactions on Emerging Technologies in Telecommunications*. He serves as a Guest Editor for IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

Daniel Benevides da Costa (Senior Member, IEEE) was born in Fortaleza, Brazil, in 1981. He received the B.Sc. degree in telecommunications from the Military Institute of Engineering (IME), Rio de Janeiro, Brazil, in 2003, and the M.Sc. and Ph.D. degrees in electrical engineering (telecommunications) from the University of Campinas, Brazil, in 2006 and 2008, respectively. From 2008 to 2009, he was a Postdoctoral Research Fellow with INRS-EMT, University of Quebec, Montreal, QC, Canada. Since 2010, he has been with the Federal University of Ceará, where he is currently an Associate Professor. His Ph.D. thesis was awarded the Best Ph.D. Thesis in Electrical Engineering by the Brazilian Ministry of Education (CAPES) at the 2009 CAPES Thesis Contest. He was a recipient of four conference paper awards. He received the Exemplary Reviewer Certificate of IEEE WIRELESS COMMUNICATIONS LETTERS in 2013, the Exemplary Reviewer Certificate of IEEE COMMUNICATIONS LETTERS in 2016 and 2017, the Certificate of Appreciation of Top Associate Editor for outstanding contributions to IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY in 2013, 2015, and 2016, the Exemplary Editor Award of IEEE COMMUNICATIONS LETTERS in 2016, and the Outstanding Editor Award of IEEE ACCESS in 2017. He is also the Vice-Chair of Americas of the IEEE Technical Committee of Cognitive Networks (TCCN), the Director of the TCCN Newsletter, and the Chair of the Special Interest Group on Energy-Harvesting Cognitive Radio Networks, IEEE TCCN. He is currently an Executive Editor of IEEE COMMUNICATIONS LETTERS and an Editor of IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE ACCESS, IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, and *EURASIP Journal on Wireless Communications and Networking*. He has also served as an Associate Technical Editor for *IEEE Communications Magazine*. From 2012 to 2017 and from March 2019 to August 2019, he was an Editor of IEEE COMMUNICATIONS LETTERS. He also serves as an Area Editor of IEEE OPEN JOURNAL OF THE COMMUNICATION SOCIETY Area: Green, Cognitive, and Intelligent Communications and Networks and as a Guest Editor for several journal special issues. He has served on the organizing committee of several conferences. He is also the Latin American Chapters Coordinator of the IEEE Vehicular Technology Society. He acts as a Scientific Consultant of the National Council of Scientific and Technological Development (CNPq), Brazil, and he is a Productivity Research Fellow of CNPq. He is also a Distinguished Lecturer of the IEEE Vehicular Technology Society. He is a member of the IEEE Communications Society and the IEEE Vehicular Technology Society.

Trung Q. Duong (Senior Member, IEEE) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology (BTH), Sweden, in 2012.

He was a Lecturer (Assistant Professor) from 2013 to 2017 and a Reader (Associate Professor) from 2018 with Queen's University Belfast, U.K. He is currently with Queen's University Belfast. His current research interests include the Internet of Things (IoT), wireless communications, molecular communications, and signal processing. He has authored or coauthored 290 technical articles published in scientific journals (165 articles) and presented at international conferences (125 articles). He received the Best Paper Award at IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) in 2014, IEEE Global Communications Conference (GLOBECOM) in 2016, and IEEE Digital Signal Processing Conference (DSP) in 2017. He was a recipient of the prestigious Royal Academy of Engineering Research Fellowship (2016–2021) and the prestigious Newton Prize in 2017. He also serves as an Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, and *IET Communications*, and a Lead Senior Editor for IEEE COMMUNICATIONS LETTERS.

Hoang Duong Tuan received the Diploma (Hons.) and Ph.D. degrees in applied mathematics from Odessa State University, Ukraine, in 1987 and 1991, respectively. He spent nine academic years in Japan as an Assistant Professor at the Department of Electronic-Mechanical Engineering, Nagoya University, from 1994 to 1999, and then as an Associate Professor at the Department of Electrical and Computer Engineering, Toyota Technological Institute, Nagoya, from 1999 to 2003. He was a Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, from 2003 to 2011. He is currently a Professor with the School of Electrical and Data Engineering, University of Technology Sydney. He has been involved in research in the areas of optimization, control, signal processing, wireless communications, and biomedical engineering for more than 20 years.

Alan Marshall (Senior Member, IEEE) has spent over 24 years working in the telecommunications and defense industries. He is currently the Chair in communications networks with the University of Liverpool, where he is also the Director of the Advanced Networks Group and the Head of the department. He formed a successful spin-out company, Traffic Observation and Management Ltd. He has published over 200 scientific articles and holds a number of joint patents in the areas of communications and network security. His research interests include network architectures and protocols, mobile and wireless networks, network security, high-speed packet switching, QoS/QoE architectures, and multisensory communications, including haptics and olfaction. He is a fellow of the Institution of Engineering and Technology and a Senior Fellow of the Higher Education Academy. He is also a Section Editor of *The Computer Journal* of the British Computer Society and an Editorial Board Member of the *Journal of Networks*.