IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 1, 2021, accepted January 4, 2022, date of publication February 7, 2022, date of current version February 16, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3149169

Secure Full-Duplex Wireless Power Transfer Systems With Energy-Information Correlation

SANTIAGO FERNÁNDEZ[1], F. JAVIER LÓPEZ-MARTÍNEZ[2], (Senior Member, IEEE), FERNANDO H. GREGORIO[1], AND JUAN E. COUSSEAU[1], (Senior Member, IEEE)

[1]Departamento de Ingeniería Eléctrica y de Computadoras, UNS-CONICET, Instituto de Investigaciones en Ingeniería Eléctrica "Alfredo Desages" (IIIE), Universidad Nacional del Sur, Bahía Blanca 8000, Argentina

[2]Communications and Signal Processing Laboratory, ETSI Telecomunicación, CEI Andalucía TECH, Instituto Universitario de Investigación en Telecomunicación (TELMA), Universidad de Málaga, 29010 Málaga, Spain

Corresponding author: Santiago Fernández (sfernandez@iiie-conicet.gob.ar)

This work was supported in part by the Spanish Ministry of Science and the European Fund for Regional Development FEDER through grant TEC2017-87913-R (CERSEI), in part by Consejería de Innovación de la Junta de Andalucía through grant P18-RT-3175 (TETRA5G), in part by Universidad de Málaga, in part by the Agencia Nacional de Promoción Científica y Tecnológica (PICT-FONCYT 2016-0051), in part by the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), and in part by the Universidad Nacional del Sur (PGI 24K081).

ABSTRACT We investigate the secrecy performance and energy-efficiency trade-offs associated to the secure communication between a full-duplex (FD) power beacon (PB) and an energy harvesting (EH) device, in the presence of an eavesdropper. Specifically, we analyze the feasibility of a jamming strategy implemented at the FD-PB under several practical constraints, such as imperfect self-interference (SI) cancellation, EH non-linearity, channel aging and energy-information correlation. The design of the optimal time-splitting factor for the simultaneous wireless information and power transfer (SWIPT) strategy, the adequacy of different beamforming strategies for proper system operation, and the impact of channel correlation between the energy and information transmission phases in SWIPT are thoroughly discussed. Results indicate that under practical constraints such as EH non-linearity and imperfect SI cancellation, the transmit powers at the FD-PB for the generation of energy and jamming signals are the key parameters to be optimized from both points of view: secrecy and energy efficiency. We also verify the positive impact of correlation between the energy and information links in wireless power transfer systems, from a physical layer security perspective.

INDEX TERMS Secrecy capacity, secrecy energy efficiency, wireless power transmission, friendly jamming, full-duplex.

I. INTRODUCTION

A. RELATED WORK

Future wireless communication systems consider that millions of low complexity devices, such as internet of things (IoT) nodes, are able to communicate in an efficient way with a targeted quality of service using a low-power energy supply. Day by day, the number of devices connected to wireless networks increases considerably, and this number is expected to grow even more due to the continuous deployment of fifth generation evolution (5G+) technologies and IoT [1].

Considering this increasing number of devices, the implementation of efficient techniques to power them becomes necessary. These techniques need not only provide energy for operation, but also avoid replacing batteries in hard-to-reach devices. This includes hazardous or toxic environments, or even inaccessible places, e.g., sensors embedded in building structures or inside human bodies [2]. Above all, it becomes mandatory to reduce the pollution that the batteries of these devices cause on the planet Earth. In this line, radio frequency (RF) energy harvesting (EH) technology, which allows devices to harvest the energy required for their operation, rises as a promising alternative. One of the EH techniques that seems well-suited to feed all devices in a certain area is wireless power transmission (WPT), which employs dedicated power beacons (PBs) to

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed F. Zobaa.

wirelessly provide energy to the network agents. Moreover, the use of RF signals enables simultaneous energy and information transmission in a cost-effective way under the *simultaneous wireless information and power transfer* (SWIPT) paradigm, which at the same time energizes a great number of low complexity nodes and allows them to transmit/receive information.

As an additional requisite in the road to sixth generation (6G) technologies, the provision of security is a major concern in the context of future wireless networks [3], and those operating under the EH paradigm are no exception [4]. However, the inherent broadcast nature of wireless communications makes them vulnerable to many physical-layer threats such as eavesdropping (interception, traffic analysis), contaminating (pilot contamination, feedback contamination), spoofing (identity spoofing, sybil attacks) or jamming (pilot jamming, proactive jamming, reactive jamming) [5]. In order to design a robust system that meets the desirable security requirements, high-level encryption techniques have been conventionally used to protect the information against these threats [6].

However, the implementation of such algorithms, which consist in the distribution and management of cryptographic keys, requires a large complexity. In the context of ultra-high speed and ultra-low latency communications supported for the future wireless IoT networks, requisites are highly challenging and can not be afforded in the IoT context where low-cost/complexity nodes, with tight energy and resources constraints, are the main components [7].

Unlike traditional methods for security provision in upper layers, physical layer security (PLS) exploits the randomness of the wireless channel to transmit secure information in the presence of malicious eavesdroppers [8], [9], regardless of computational power of this latter. In this context, PLS has attracted considerable research attentions as an alternative technique based on information-theoretic to improve security in IoT communications [5].

In order for PLS to succeed, the transmission of secure information cannot exceed a maximum rate called secrecy capacity. That is possible under two (somehow mild) conditions: (*i*) the use of additional redundancy through a wiretap code and (*ii*) that the legitimate receiver has some sort of advantage over the illegitimate one, typically in terms of signal-to-noise ratio (SNR). Under these premises, several techniques can be used to increase the secrecy rates by improving/degrading the SNRs at the legitimate/illegitimate receivers [10]. One popular option is the injection of artificial noise (AN) by the transmitter [11] in the direction of the eavesdropper, while the legitimate user signal remains unaffected. In the context of WPT-based EH communications, the PB can act as an energy transmitter *and* as a friendly jammer that injects AN [12] simultaneously, by means of operating in a full-duplex fashion.

In the last years, the investigation on PLS techniques for WPT-enabled systems has drawn a considerable attention because of their undeniable practical interest associated to the IoT use case deployment [5], [13]. From a technical viewpoint, there are three main sets of challenges associated to the deployment of WPT-based solution for secure communications in EH-systems:

1) On the one hand, there is *a vast number of ingredients* that can be combined into designing a feasible solution. Techniques such as beamforming, full-duplex (FD) operation, EH capabilities, jamming and SWIPT are known to provide advantages for PLS, although their applicability in this specific context is usually tied to the second challenge addressed below.
2) Practical aspects and limitations associated to these systems and techniques will limit their performance. Specifically, the lack of channel state information (CSI) impacts the ability of transmitters to beamforming the signal in the desired direction – either the legitimate EH device for energy transmission, or the illegitimate receiver for jamming operation. Similarly, the use of FD techniques that enable the jamming operation at the PB also cause non-negligible self-interference that needs to be mitigated [14]. The non-linearity (NL) of EH devices is also known to have an impact [15] on the choice of the optimal duration of the information and energy transfer phases in SWIPT. Very recently, the correlation between the energy and information links in WPT has been shown to also have an impact on the achievable rate [16] and PLS performances [17].
3) Last, but not least, the different constraints that can be used for system design often require trade-offs that are virtually impossible to meet at the same time. For the specific case of PLS, the system can be designed either to maximize the rate of secure information [18] or to minimize the unitary cost of energy required to transmit at a certain secure rate [19]. In this context, performance metrics such as the achievable secrecy rate and the secrecy energy efficiency may be used.

One illustrative example of the previous considerations is the use of AN techniques for PLS in FD-enabled systems: ideally, the use of jamming techniques to enhance PLS security may always seem beneficial. However, a practical FD system implemented at the PB (playing the roles of friendly jammer and information receiver simultaneously) is unable to perfectly remove self-interference. Hence, there is a trade-off between the amount of energy that can be used for jamming, and the residual self-interference that remains at the legitimate receiver [14]. Similarly, incorporating energy efficiency requisites into the system operation may imply different system design decisions [19] compared to neglecting such energy constraints. With all these aspects in mind, we aim to answer the following questions: *(i) How to design a WPT-based system with security and energy efficiency practical constraints?*, and *(ii) how do the practical constraints associated with that system affect the inherent design trade-offs that allow secure and efficient operation?*

We formulate a realistic scenario on which a multiantenna PB transmits energy to a legitimate non-linear EH-device to

enable its operation, with the ultimate goal that the EH-device reports some information back to the PB in the presence of an external eavesdropper [20]. The PB operates in FD mode, so that it is able to receive the information transmitted by the EH-device while generating a jamming signal to degrade the signal received by the eavesdropper. Because of imperfect CSI and FD cancellation, the generation of the jamming signal also affects its ability to receive the legitimate information [14], [21]. Because of the inherent low-variability of fading in this context, the energy and information links between the PB and the EH-device exhibit a non-negligible correlation and have line-of-sight nature. We provide important insights on the effect and interplay of all the parameters involved for a proper system design, when either secrecy rate or secrecy energy efficiency (SEE) maximization are considered. As the preliminary results in [17] state, the correlation between energy and information links increases the average signal to noise ratio, and this correlation turns out being beneficial from a PLS perspective, thus reflecting in a significant improvement on the metrics under consideration.

B. CONTRIBUTIONS AND ORGANIZATION

To the best of our knowledge, secrecy capacity and secrecy energy efficiency evaluation, considering correlation between energy and information channels and a PB with full-duplex capacity have not been evaluated. To fill this gap, in this work we make specific contributions that can be summarized as follows:

- A full-duplex friendly-jamming scheme is implemented at the PB to optimize the system secure performance, extending the schemes in [14] to the specific WPT-based scenario under consideration. Beamforming schemes with full, partial and no explicit use of the eavesdropper's CSI are evaluated, and we verified that having full CSI knowledge for the eavesdropper's link (PB-RX) does not provide a major benefit, compared to the case of no-CSI. The crucial role of the residual self-interference is analyzed and the required self-interference remotion capabilities for a given jamming transmit power are also discussed.
- The benefits of the use of a PB with full-duplex capabilities and its performance compared with a PB operating in half-duplex fashion is studied. The recommended regions for FD and HD operation are determined under practical constraints.
- We highlight the balance and interplay between energy efficiency and secrecy capacity. Practical recommendations are established in order to reach a secure system with a high energy efficiency.
- We discuss in depth the role of correlation between the energy and information links, and aspect that has been largely overlooked in the literature. We highlight its beneficial role for physical layer security, confirming that they have an important impact in practical scenarios.
- We exemplify how the very-high complexity optimization techniques required to solve the problem can be circumvented in the proposed scenario. Specifically, we show how the design can be relaxed by first choosing the time-splitting ratio for SWIPT operation (θ), and then designing the rest of parameters (information/jamming transmit power), for a given choice of beamforming vector.

The remainder of the paper is organized as follows: the system model under consideration is described in Section II. The problem formulation associated to system design is presented in Section III. The beamforming vector design options for energy transmission and friendly jamming are analyzed in Section IV. Then, the power allocation problem at the PB and the time-splitting factor for SWIPT operation are discussed in Section V. Finally, the main conclusions and design recommendations are summarized in Section VI.

II. SYSTEM MODEL

The system under consideration consists of three nodes (see Figure 1): a dedicated PB, an energy-harvesting (constrained) (EH) source and a non-legitimate user (RX) that plays the role of eavesdropper. The system operation is described as follows: The multiantenna PB is equipped with N_{T} transmit and N_{R} receive antennas. Because the system agents are low-complexity nodes, we consider for simplicity but without loss of generality that EH and RX are single antenna devices. The scenario with an arbitrary number of antennas at the eavesdropper is addressed in [22]. However, to avoid the blur of the effects of full-duplex operation and the other system parameters under evaluation, a single antenna scenario is studied. The distances between the system agents are denoted as d_{PE} (between PB and EH), d_{PR} (between PB and RX) and d_{ER} (between EH and RX), respectively.

We consider a frame-based protocol to implement the SWIPT system, where the whole transmission process is divided into L frames as illustrated in Figure 2. Considering a transmission block length of T seconds, each block is divided into two phases using a time switching protocol: the period θT employed for energy transfer, and the remaining period, $(1-\theta)T$, is dedicated to information transmission, where θ is the time switching ratio ($0 < \theta < 1$).

Each transmission block of length T(s) is divided in two phases that can be can be summarized as follows:

- Phase 1: a portion θT seconds is employed to transfer energy. The PB acts as a power source and transfers energy to the EH device.
- Phase 2: the remaining portion, $(1-\theta)T$, is employed for information transmission. The EH device, which now plays the role of Alice (the legitimate transmitter) employs the harvested energy to report information back to the PB, that acts as Bob (the legitimate receiver).

We consider that the PB has FD capabilities; hence, during Phase 2 it is able to generate a jamming signal towards the eavesdropper (Eve) RX. This jamming signal degrades the illegitimate receiver operation, but also the signal received

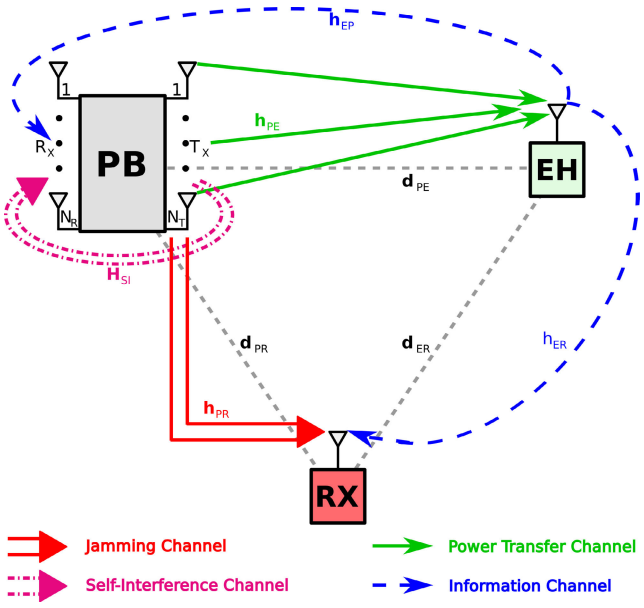

FIGURE 1. System model considering the power beacon (PB), the energy harvesting node (EH) and the eavesdropper (RX).

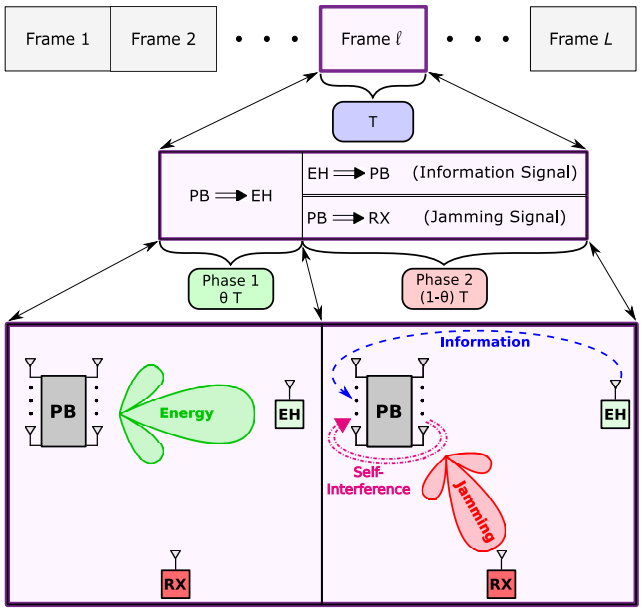

FIGURE 2. Time switching protocol and energy and jamming beamformings.

by the PB (i.e., Bob) because of imperfect self-interference cancellation. Thanks to the N_{T} transmission antennas, the PB is able to use beamforming in order to improve the energy transfer to the EH node, as well as to generate a jamming signal towards the RX node. The design of each beamforming vector depends on the operation phase.

A. CHANNEL MODEL

Consistent with the scenario under consideration, we assume that the channel fading coefficients for each of the links in Fig. 1, i.e., $\mathbf{h}_{\mathrm{PE}} \in \mathbb{C}^{N_T \times 1}$, $\mathbf{h}_{\mathrm{PR}} \in \mathbb{C}^{N_T \times 1}$, and h_{ER} are those of a quasi-static block-fading setting with frequency non-selective parameters, and their coherence time, T_{c}, is longer than the frame duration T. Because of the relatively short range of operation of WPT-systems, we assume a line-of-sight (LOS) condition for the fading links between the PB and the EH device. Without loss of generality, the links involving the eavesdropper, i.e. PB-RX and EH-RX, are assumed to have non-LOS condition.

Since the PB acts in full-duplex mode, reciprocity between $\mathbf{h}_{\mathrm{PE}}$ (i.e., the forward energy link) and $\mathbf{h}_{\mathrm{EP}}$ (i.e., the backward legitimate information link) channels is assumed. Hence, the PB can estimate the channel vector $\mathbf{h}_{\mathrm{EP}}$ using a pilot signal previously sent by the EH, and then uses this estimation along L frames (i.e., during the channel coherence time).

In order to properly capture the essence of the channel model under consideration, a correlated block fading model is used. In this situation, the energy and legitimate information channels at the initial frame can be expressed as:

$$\mathbf{h}_{\mathrm{PE}}(1) = \sqrt{\frac{K}{1+K}}\mathbf{1}_{\mathrm{N}_T} + \sqrt{\frac{1}{1+K}}\mathbf{z}_1^E \tag{1}$$

$$\begin{aligned}\mathbf{h}_{\mathrm{EP}}(1) &= \left[\sqrt{\frac{K}{1+K}}\mathbf{1}_{\mathrm{N}_T} \right. \\ &\quad \left. + \sqrt{\frac{1}{1+K}}\left(\rho\mathbf{z}_1^E + \sqrt{1-\rho^2}\mathbf{z}_1^I\right)\right] \\ &= \sqrt{\frac{K}{1+K}}\mathbf{1}_{\mathrm{N}_T} + \sqrt{\frac{1}{1+K}}\mathbf{h}_{new}^I(1)\end{aligned} \tag{2}$$

where the Rician K factor is defined as the ratio of the NLOS/LOS powers for the energy/information links, $\mathbf{1}_{\mathrm{N}_T} \in \mathbb{R}^{N_T \times 1}$ is an all-one column vector of dimension N_T, $\mathbf{z}_1^E \in \mathbb{C}^{N_T \times 1}$ and $\mathbf{z}_1^I \in \mathbb{C}^{N_T \times 1}$ are auxiliary vectors with complex normal random variable i.i.d. entries, where the superscript E is associated with the energy transmission vector and the superscript I is associated with the information transmission vector, and to the other hand, the subscript 1 is associated with the first frame. ρ denotes the correlation coefficient for each of the complex normal random variables that varies from 0 (uncorrelated) to 1 (fully-correlated) and is defined as $\rho = \mathrm{cov}(\mathbf{h}_{\mathrm{PE}}(\ell), \mathbf{h}_{\mathrm{EP}}(\ell))/\sqrt{\mathrm{var}(\mathbf{h}_{\mathrm{PE}}(\ell))\mathrm{var}(\mathbf{h}_{\mathrm{EP}}(\ell))}$. It becomes clear that the term $\left(\rho\mathbf{z}_1^E + \sqrt{1-\rho^2}\mathbf{z}_2^I\right)$ in (2) is replaced for $\mathbf{h}_{new}^I(1)$ in order to simplify the notation.

The temporal evolution of the channels along $l-th$ frame is described by:

$$\begin{aligned}\mathbf{h}_{\mathrm{PE}}(\ell) &= \left[\sqrt{\tfrac{K}{1+K}}\mathbf{1}_{\mathrm{N}_T} \right. \\ &\quad \left. + \sqrt{\tfrac{1}{1+K}}\left(\rho\,\mathbf{h}_{new}^I(\ell-1) + \sqrt{1-\rho^2}\mathbf{z}_\ell^E\right)\right] \\ &= \sqrt{\tfrac{K}{1+K}}\mathbf{1}_{\mathrm{N}_T} + \sqrt{\tfrac{1}{1+K}}\mathbf{h}_{new}^E(\ell)\end{aligned} \tag{3}$$

$$\mathbf{h}_{\mathrm{EP}}(\ell) = \left[\sqrt{\tfrac{K}{1+K}}\mathbf{1}_{\mathrm{N}_T}\right.$$

$$+\sqrt{\tfrac{1}{1+K}}\left(\rho\,\mathbf{h}^{E}_{new}(\ell)+\sqrt{1-\rho^2}\mathbf{z}^{I}_{\ell}\right)\Big] = \sqrt{\tfrac{K}{1+K}}\mathbf{1}_{\mathrm{N}_T}+\sqrt{\tfrac{1}{1+K}}\mathbf{h}^{I}_{new}(\ell) \quad (4)$$

where $\mathbf{z}^{I}_{\ell} \in \mathbb{C}^{N_T\times 1}$ and $\mathbf{z}^{E}_{\ell} \in \mathbb{C}^{N_T\times 1}$ are again auxiliary vectors with i.i.d. complex normal entries, and noting that the subscript ℓ is associated with the $\ell-th$ frame. It becomes clear that the term $\left(\rho\,\mathbf{h}^{I}_{new}(\ell-1)+\sqrt{1-\rho^2}\mathbf{z}^{E}_{\ell}\right)$ in (3) is replaced for $\mathbf{h}^{E}_{new}(\ell)$ and the term $\left(\rho\,\mathbf{h}^{E}_{new}(\ell)+\sqrt{1-\rho^2}\mathbf{z}^{I}_{\ell}\right)$ in (4) is replaced for $\mathbf{h}^{I}_{new}(\ell)$ both in order to simplify the notation. It is worth to note that the aging of the channel estimation is modeled through the correlation coefficient ρ.

The temporal interdependence captured by the correlated block-fading model will model two effects: (*i*) the correlation between the energy and information links, and (*ii*) the effect of channel aging on the energy beamforming transmission by the PB.[1] In the following, we describe the signal model for each of the SWIPT phases.

In our setup, RX and EH are considered quasi-stationary. The scenario of nodes including mobility is not considered in our analysis. In this case, the user's mobility will affect the channel coherence time and the number of frames will be reduced. In an scenario with high mobility, the correlation between energy and information channels will be close to zero. Scenarios considering random mobile users in IoT were addressed in [25], [26]. However, power transmission is not included in [25], while PLS is not addressed in [26].

B. SIGNAL MODEL FOR THE ENERGY TRANSFER PHASE

The signal received at the EH can be expressed as

$$y_{\mathrm{EH}}(\ell) = \sqrt{P_1 L_{\mathrm{PE}}}x_E(\ell)\mathbf{h}^{T}_{\mathrm{PE}}(\ell)\mathbf{w}_T + n_{\mathrm{EH}}(\ell) \quad (5)$$

where P_1 is the transmitted power by the PB at the phase 1, $\mathbf{w}_T$ is the transmission beamforming vector, L_{PE} includes the path loss between the PB and the EH, x_E is the energy signal and n_{EH} is the noise at the EH. The $N_T \times 1$ channel between PB-EH at frame ℓ (time-index) is denoted as $\mathbf{h}_{\mathrm{PE}}(\ell) = [h^{1}_{\mathrm{PE}}(\ell), h^{2}_{\mathrm{PE}}(\ell), \cdots, h^{N_T}_{\mathrm{PE}}(\ell)]$ and $()^T$ denotes the transpose operator.

During the energy transfer phase, the energy beamformer employs a maximum-ratio transmission (MRT) precoding in order to maximize the energy transmitted to the EH.

Considering that the portion of the period of length θT is employed for wireless power transfer, the total harvested energy in this period is

$$E_i(\ell) = P_1 L_{\mathrm{PE}}\left|\mathbf{h}^{T}_{\mathrm{PE}}(\ell)\mathbf{w}_T\right|^2\theta T$$

and, assuming that all the harvested energy is used during the information transmission phase, $(1-\theta)T$, the available power at the input of the EH is given by

$$P_i(\ell) = \frac{E_i(\ell)}{(1-\theta)T} = P_1 L_{\mathrm{PE}}\left|\mathbf{h}^{T}_{\mathrm{PE}}(\ell)\mathbf{w}_T\right|^2\left(\frac{\theta}{1-\theta}\right) = P_1 L_{\mathrm{PE}}\left|\mathbf{h}^{T}_{\mathrm{PE}}(\ell)\frac{\mathbf{h}_{\mathrm{PE}}(1)^*}{\|\,\mathbf{h}_{\mathrm{PE}}(1)\,\|}\right|^2\left(\frac{\theta}{1-\theta}\right) \quad (6)$$

where $()^*$ denotes the conjugate operator. It is worth to mention that the transmit beamforming vector $\mathbf{w}_T$ is calculated from the estimation of $\mathbf{h}_{\mathrm{PE}}$ in the first frame. Hence, it remains constant along an entire subframe, while $\mathbf{h}_{\mathrm{PE}}$ varies according to the correlated block-fading model previously described. Hence, the mismatched beamforming vector will cause a degradation in the available energy at EH. The harvested power is given by

$$P_{\mathrm{EH}}(\ell) = g(P_i(\ell)) \quad (7)$$

where $g(\cdot)$ represents the transfer function of the EH, which in general has a non-linear behavior. The nonlinear characteristic of the EH can be modeled by a sigmoid function as [15], [27]

$$g(P_i) = \frac{\frac{P_s}{1+\exp(-a(P_i-b))} - P_s\Omega}{1-\Omega} \quad (8)$$

where $\Omega = 1/(1+\exp(ab))$, a defines the abruptness of the sensitivity transition, b is the EH sensitivity, and P_s is the maximum amount of harvested power when the EH circuit is saturated. This NL model is useful to obtain a good representation of a realistic EH transfer function, than an ideal linear model $P_{\mathrm{EH}}(\ell) = \eta P_i(\ell)$ (where η is fixed) conventionally used in the literature.

C. SIGNAL MODEL FOR THE INFORMATION TRANSFER PHASE

In this second phase, the EH uses the harvested power to transmit information to the PB. The received signal at the PB is weighted by the $N_R \times 1$ receiver beamforming vector $\mathbf{w}_R$. At the same time, the PB acts as a friendly jammer and generates a jamming signal towards the eavesdropper RX. Because of imperfect self-interference cancellation, part of this jamming signal is leaked into the received signal. After down-conversion, the sampled baseband signal at the PB is given by

$$y_{\mathrm{PB}}(\ell) = \Big[\mathbf{w}^{H}_{R}\left(\sqrt{P_{\mathrm{EH}}(\ell)L_{\mathrm{EP}}}\mathbf{h}_{\mathrm{EP}}(\ell)x(\ell) + \sqrt{P_2\beta_{\mathrm{SI}}}\mathbf{H}_{\mathrm{SI}}\mathbf{w}_J z(\ell) + n_{\mathrm{PB}}(\ell)\right)\Big] = \Big[\sqrt{P_{\mathrm{EH}}(\ell)L_{\mathrm{EP}}}\mathbf{w}^{H}_{R}\mathbf{h}_{\mathrm{EP}}(\ell)x(\ell) + \sqrt{P_2\beta_{\mathrm{SI}}}\mathbf{w}^{H}_{R}\mathbf{H}_{\mathrm{SI}}\mathbf{w}_J z(\ell) + \mathbf{w}^{H}_{R}n_{\mathrm{PB}}(\ell)\Big] \quad (9)$$

[1] Equations (1), (2), (3) and (4) use the conventional model for channel aging, on which the zero-mean Gaussian part evolves as a Gaussian process according to a correlation coefficient, which weighs the static and dynamic parts of the channel [23]. Note that additional variations in the LOS part can also be incorporated as in [24]. Due to the inherent low mobility of the scenario under consideration, we assume that channel variation is likely to be associated to mobility of scatterers that generate the diffuse component of channel fading, whereas the phase of the line-of-sight component can be regarded as static for the duration of a frame.

where P_2 is the transmitted power by the PB at the information phase when the PB acts as friendly jammer, $x(\ell)$ is the sampled information signal transmitted from the EH, and n_{PB} is the baseband AWGN. Besides, $\mathbf{H}_{\text{SI}}$ is the $N_R \times N_T$ self-interference channel matrix and β_{SI} denotes the isolation between transmitter and receiver antennas of the PB (that includes, for example, the attenuation due to physical antenna separation, antenna polarization, and also the implementation of a RF canceller), L_{EP} is the path loss between the EH and the PB and the $N_R \times 1$ small-scale fading channel between EH-PB at frame ℓ is defined as $\mathbf{h}_{\text{EP}}(\ell) = [h^1_{\text{EP}}(\ell), h^2_{\text{EP}}(\ell), \cdots, h^{N_R}_{\text{EP}}(\ell)]$. Finally, z is the jamming signal with unitary power, and the $N_T \times 1$ vector $\mathbf{w}_J$ is the transmission beamforming vector of the PB acting as a friendly jammer.

On the other hand, the signal that reaches the eavesdropper (RX) is expressed by

$$y_{\text{RX}}(\ell) = \Big[\sqrt{P_{\text{EH}}(\ell)L_{\text{ER}}}h_{\text{ER}}(\ell)x(\ell) + \sqrt{P_2 L_{\text{PR}}}\mathbf{h}^T_{\text{PR}}(\ell)\mathbf{w}_J z(\ell) + n_{\text{RX}}(\ell)\Big] \tag{10}$$

where again $\mathbf{w}_J$ is the beamforming vector used by the PB to generate the jamming signal towards RX, L_{ER} is the path loss between the EH and RX, h_{ER} is the channel between the EH and RX. n_{RX} is the AWGN noise at RX, L_{PR} is the path loss that affects the jamming signal, $\mathbf{h}_{\text{PR}}$ is the $[N_T \times 1]$ small-scale fading channel between the PB and RX defined as $\mathbf{h}_{\text{PR}}(\ell) = [h^1_{\text{PR}}(\ell), h^2_{\text{PR}}(\ell), \cdots, h^{N_T}_{\text{PR}}(\ell)]$ and z is the jamming signal with unitary power.

Then, the instantaneous end-to-end signal-to-interference-plus-noise ratio (SINR) at the legitimate user (Bob) can be evaluated as

$$\gamma_B(\ell) = \frac{P_{\text{EH}}(\ell)L_{\text{EP}}|\mathbf{w}_R^H\,\mathbf{h}_{\text{EP}}(\ell)|^2}{P_2\beta_{\text{SI}}|\mathbf{w}_R^H\,\mathbf{H}_{\text{SI}}\mathbf{w}_J|^2 + N_0} = \frac{g\left(\frac{P_1 L_{\text{PE}}\theta}{1-\theta}\left|\mathbf{h}^T_{\text{PE}}(\ell)\frac{\mathbf{h}_{\text{PE}}(1)^*}{\|\mathbf{h}_{\text{PE}}(1)\|}\right|^2\right)L_{\text{EP}}|\mathbf{w}_R^H\mathbf{h}_{\text{EP}}(\ell)|^2}{P_2\beta_{\text{SI}}|\mathbf{w}_R^H\mathbf{H}_{\text{SI}}\mathbf{w}_J|^2 + N_0} \tag{11}$$

and the average SINR is given by $\overline{\gamma}_B = \mathbb{E}[\gamma_B(\ell)]$, where $\mathbb{E}[\cdot]$ denotes expectation.

Likewise, the instantaneous SINR at the eavesdropper RX (Eve) can be expressed as

$$\gamma_E(\ell) = \frac{P_{\text{EH}}(\ell)\,L_{\text{ER}}\,|h_{\text{ER}}(\ell)|^2}{P_2\,L_{\text{PR}}\,|\mathbf{h}^T_{\text{PR}}(\ell)\,\mathbf{w}_J|^2 + N_0} = \frac{g\left(\frac{P_1 L_{\text{PE}}\theta}{1-\theta}\left|\mathbf{h}^T_{\text{PE}}(\ell)\frac{\mathbf{h}_{\text{PE}}(1)^*}{\|\mathbf{h}_{\text{PE}}(1)\|}\right|^2\right)L_{\text{ER}}|h_{\text{ER}}(\ell)|^2}{P_2 L_{\text{PR}}|\mathbf{h}^T_{\text{PR}}(\ell)\mathbf{w}_J|^2 + N_0} \tag{12}$$

and the average SINR is given by $\overline{\gamma}_E = \mathbb{E}[\gamma_E(\ell)]$.

D. SECURE PERFORMANCE METRICS

With the previous definitions, we can define the instantaneous achievable secrecy rate[2] C_s as

$$C_s(\ell) = (1-\theta)\begin{cases}\big[\log_2(1+\gamma_B(\ell)) & \\ -\log_2(1+\gamma_E(\ell))\big] & \text{if}\gamma_B(\ell) > \gamma_E(\ell)\\ 0 & \text{if}\gamma_B(\ell) \le \gamma_E(\ell)\end{cases} \tag{13}$$

where γ_B and γ_E denote the SINR at the legitimate user and at the eavesdropper, respectively, as defined in (11) and (12).

The previous definition does not contemplate energy efficiency aspects of secure communications. In the set-up under consideration, when non-linear harvesters are considered, the converter reaches the saturation and its conversion efficiency is drastically reduced. Moreover, considering that our system requires an initial channel estimation, the energy and time dedicated to transmit pilot symbols needs to be taken into account to calculate the energy and spectral efficiency [28], together with the quality of the channel estimates. With these considerations, we employ the *secrecy energy efficiency* (SEE) [29] as the key metric to measure the security of the system and the energy required to reach this value. The power consumed at the PB can be written as

$$P_{C_{\text{PB}}} = \eta_{pa}(P_1\theta + P_2(1-\theta)) + P_{S_P} \tag{14}$$

where η_{pa} is the PB power amplifier (PA) efficiency, P_1 and P_2 are the transmitted power by PB at phases 1 (energy) and 2 (jamming) respectively. P_{S_P} is the static power consumed by the transmitter and receiver blocks, that includes the power required by the signal processing and analog blocks to operate, and also the power required to implement the self-interference removal when operating in FD mode.

The instantaneous SEE of the secure communication link is defined as the ratio between the system's achievable secrecy rate, and the total power consumed [29]–[31]

$$\text{SEE} = \frac{C_s}{P_{C_{\text{PB}}}} \tag{15}$$

where C_s is the secrecy capacity as defined in (13) and $P_{C_{\text{PB}}}$ is the power consumption of the link defined in (14).

III. SYSTEM DESIGN

A. PROBLEM FORMULATION FOR C_s AND SEE MAXIMIZATION

In the proposed scenario, our goal is to design the system parameters with the ultimate target of maximizing a given performance metric. The parameters to be designed are the following:

- Jamming Vector $\mathbf{w}_j$; the choice of the energy beamforming vector at the PB $\mathbf{w}_T$ and the receive beamforming operation at the information receiver $\mathbf{w}_R$ are designed according to MRT and MRC criteria, respectively,

[2]Throughout the rest of the paper, for the sake of readability and with a slight abuse of notation, we will refer to this achievable secrecy rate as secrecy capacity.

in order to maximize the energy transfer and the receive signal power at each phase.
- Time switching ratio θ: the period dedicated for energy/information transmission will depend on the harvester transfer function.
- PB transmitted power: the transmit power for the energy transmission and jamming phases, P_1 and P_2, respectively needs to be optimized. P_1 will depend on the energy harvester transfer function (linearity, saturation point), and P_2 will present a dependence with the residual self-interference.

Depending on whether our goal is to maximize the secrecy capacity or the SEE, the optimization problem is defined accordingly.

- **S1: Secrecy Capacity Maximization**. The secrecy capacity maximization problem is defined as:

$$(S1): \max_{P_1,P_2,\theta,\mathbf{w}_j} C_s \quad \text{s.t. } P_1 \leq P_{max}, \; P_2 \leq P_{max}, \; 0 < \theta < 1, \; ||\mathbf{w}_j|| = 1, \tag{16}$$

where C_s can be obtained from Eq. (13), P_1 and P_2 are the transmitted power by PB at phases 1 (energy) and 2 (jamming) respectively.
- **J1: Secrecy Energy Efficiency Maximization**. Similar to S1, the secrecy energy efficiency maximization problem is formulated as:

$$(J1): \max_{P_1,P_2,\theta,\mathbf{w}_j} SEE \quad \text{s.t. } P_1 \leq P_{max}, \; P_2 \leq P_{max}, \; 0 < \theta < 1, \; ||\mathbf{w}_j|| = 1, \tag{17}$$

where the SEE can be obtained from Eq. (15).

Depending on the CSI availability at the PB, the previous optimization goals may not be attainable. For instance, the maximization of the instantaneous C_s or SEE is only possible when perfect CSI of the RX is available at the PB. In such case, the beamforming vector $\mathbf{w}_j$ can be optimized using this CSI. In the absence of RX's CSI, the instantaneous capacity of the eavesdropper's link may not be used for beamforming design. In this situation, the power allocation problem, i.e., P_1, P_2 and θ is solved with the goal of maximizing the average secrecy capacity or SEE.

We choose the Genetic Algorithm (GA) due to its ability to solve problems of highly nonlinear objective functions that have several local extreme values.

Even in the absence of self-interference, the solution of the optimization problems previously defined is rather hard because of the non-convexity of the secrecy metrics [29]. The joint design of time split ratio and transmit beamforming vector is addressed in [32]. However, only half-duplex operation was considered. For this reason, we propose to solve an iterative approach to choose the system parameters $\mathbf{w}_j$, P_1, P_2 and θ. First, we will study the impact of different beamforming strategies on the achievable performance. Then, the design of the rest of parameters is carried out: as we will later see, the choice of the time-splitting ratio parameter is not critical within a range of values of θ. Hence, the transmit powers (P_1, P_2) for the energy transmission and jamming phases can be designed for a fixed θ with little impact. The optimal values of P_1 and P_2 for a given full-duplex cancellation performance, and the comparison between full-duplex and half-duplex operation are then discussed. The optimal solution in this scenario requires an optimization technique of high complexity. We note that analytical results are only available for the simplified scenario presented in [17] where the impact of correlation between the energy and information links in wireless power transfer systems was addressed, from a physical layer security perspective. Specifically, a single-antenna half-duplex scenario with linear energy-harvester was assumed, and the optimization of θ was not considered.

IV. BEAMFORMING VECTOR DESIGN: ENERGY TRANSMISSION AND FRIENDLY JAMMER

In this section, we address the design of the beamforming vectors at the PB. As previously described, the PB operates as energy transmitter and friendly jammer during phase 1 and phase 2, respectively. During phase 1, the beamforming vector is designed to maximize the received energy at the EH. For this reason, and assuming that the $N_T \times 1$ channel $\mathbf{h}_{\text{PE}}(\ell) = [h^1_{\text{PE}}(\ell), h^2_{\text{PE}}(\ell), \cdots, h^{N_T}_{\text{PE}}(\ell)]$ between PB-EH is known at the PB, the energy beamformer employs a MRT precoding scheme maximizing the power transmitted to the EH. The transmission vector $\mathbf{w}_T$ is a $N_T \times 1$ vector that verifies $||\mathbf{w}_T|| = 1$ such that $\mathbf{w}_T = \mathbf{h}_{\text{PE}}(1)^*/ \parallel \mathbf{h}_{\text{PE}}(1) \parallel$. Note that this transmission beamforming vector is calculated from the estimation of $\mathbf{h}_{\text{PE}}$ at the first frame. Therefore, it will be affected by channel aging along the duration of a frame.

During the second phase, in order to maximize the power of the information signal received at the PB from the EH device, the former employs a maximum ratio combining (MRC) scheme to generate a receive vector $\mathbf{w}_R$. Assuming that the $N_R \times 1$ channel $\mathbf{h}_{\text{EP}}(\ell) = [h^1_{\text{EP}}(\ell), h^2_{\text{EP}}(\ell), \cdots, h^{N_R}_{\text{EP}}(\ell)]$ between EH-PB is known at the PB, $\mathbf{w}_R = \mathbf{h}_{\text{EP}}(\ell)/\|\mathbf{h}_{\text{EP}}(\ell)\|$ is the $N_R \times 1$ receive vector that verifies $||\mathbf{w}_R|| = 1$. In this phase, the PB operates in FD mode and acts as friendly jammer. Hence, this motivates a beamforming design that contemplates the trade-off between the minimization of the self-interference and the maximization of the transmitted jamming signal to the eavesdropper (RX). The PB transmit the jamming signal with the ultimate goal of degrading the received signal at the eavesdropper. However, due to its full-duplex operation, the residual self-interference signal also increases the receiver noise floor and affects the legitimate user's signal to noise ratio level.

To minimize the SI, there are several alternatives that can be used in this context [33], [34]. Considering that

the PB is equipped with $N_T > 1$ transmit antennas, and the receiver beamforming vector $\mathbf{w}_R$ is calculated using MRC, the self-interference effect can be cancelled out by projecting the transmit jamming signal to the null space of the received signal at the PB input. Thus, the optimal transmit beamforming vector $\mathbf{w}_j$ that minimizes the transmitted signal to its own RX antennas, and maximizes the jamming signal to the eavesdropper is obtained by solving the following problem

$$\max_{\|\mathbf{w}_j\|=1} |\hat{\mathbf{h}}_{\mathrm{PR}}^{T}(1)\mathbf{w}_j|^2 \quad \text{s.t. } \mathbf{h}_{\mathrm{EP}}^{H}(1)\mathbf{H}_{\mathrm{SI}}\mathbf{w}_j = 0. \tag{18}$$

where $\hat{\mathbf{h}}_{\mathrm{PR}}(\ell) = [\hat{h}_{\mathrm{PR}}^{1}(\ell), \hat{h}_{\mathrm{PR}}^{2}(\ell), \cdots, \hat{h}_{\mathrm{PR}}^{N_T}(\ell)]$ is the $[N_T \times 1]$ channel estimate of the link PB-RX.

The optimal transmit beamforming vector $\mathbf{w}_j$ can be obtained by following the approach proposed in [35]. The solution is given by

$$\mathbf{w}_j = \frac{A\,\hat{\mathbf{h}}_{\mathrm{PR}}^{*}(1)}{\|A\,\hat{\mathbf{h}}_{\mathrm{PR}}^{*}(1)\|} \tag{19}$$

where

$$A = \mathbf{I}_{N_T} - \left(\mathbf{H}_{\mathrm{SI}}^{H}\mathbf{h}_{\mathrm{EP}}(1)\mathbf{h}_{\mathrm{EP}}^{H}(1)\mathbf{H}_{\mathrm{SI}}\right) / \left(\|\mathbf{h}_{\mathrm{EP}}^{H}(1)\mathbf{H}_{\mathrm{SI}}\|^2\right).$$

It is worth to mention that the null-projection design reserves one antenna element for spatial cancellation, so that the system diversity gain is reduced to $\min(N_R, N_T - 1)$. Such reduction needs to be quantified in terms of the additional energy required to reach an identical performance when a conventional MIMO PB with (N_R, N_T) antennas are dedicated to signal reception/transmission.

We assume that an estimate of $\mathbf{H}_{\mathrm{SI}}$ and $\mathbf{h}_{\mathrm{EP}}$ is available at the PB. This allows us to project the TX signal to a null space of the RX signal and minimize the self-interference.

Considering a realistic scenario, a noisy self-interference channel estimate is available. It can be modeled as

$$\hat{\mathbf{H}}_{\mathrm{SI}} = \mathbf{H}_{\mathrm{SI}} + \epsilon_{\mathrm{SI}} \tag{20}$$

where $\hat{\mathbf{H}}_{\mathrm{SI}}$ represents the estimate of the true channel, and ϵ_{SI} is a random estimation error.

Next, we consider different scenarios according to the level of available CSI of $\mathbf{h}_{\mathrm{PR}}$ at the PB.

A. FULL CSI

With perfect CSI of $\mathbf{h}_{\mathrm{PR}}$, we are able to maximize the interference at the eavesdropper. In this case, $\hat{\mathbf{h}}_{\mathrm{PR}} = \mathbf{h}_{\mathrm{PR}}$ is replaced in Eqs (18) and (19). In this situation, the transmitter beamformer is capable to generate a direct beam into the eavesdropper's direction reducing its effective signal to noise ratio.

B. NO-CSI: COMPLEMENTARY BEAMFORMING

Assuming that $\mathbf{h}_{\mathrm{PE}}$ is known at the PB, but the CSI of the eavesdropper channel $\mathbf{h}_{\mathrm{PR}}$ is not available, then the transmit beamforming vector can be calculated to minimize the energy radiation to the EH. This can be done using the complementary beamforming (CB) technique [36]. In our case, the interference over the EH may not be an issue because in phase 2 it operates as a transmitter. However, PB energy reduction can be obtained by avoiding the radiation to the EH region. This can also be useful to avoid the potential saturation of the EH transmitter because of imperfect isolation. With this strategy, the $\mathbf{h}_{\mathrm{PR}}$ is generated from the singular value decomposition (SVD) of the matrix $\Pi_{\mathbf{h}_{PE}}$ defined in [37] as

$$\Pi_{\mathbf{h}_{\mathrm{PE}}} = \mathbf{U}_{\mathrm{PE}}\Delta_{PE}\mathbf{V}_{\mathrm{PE}}^{*} \tag{21}$$

where $\Pi_{\mathbf{h}_{\mathrm{PE}}} = \mathbf{I}_{N_T} - \mathbf{h}_{\mathrm{PE}}^{*}(1)\left[\mathbf{h}_{\mathrm{PE}}^{H}(1)\mathbf{h}_{\mathrm{PE}}^{*}(1)\right]^{-1}\mathbf{h}_{\mathrm{PE}}^{H}(1)$. The set of the column space of $\Pi_{\mathbf{h}_{\mathrm{PE}}}$ is composed by the $N_T - 1$ left singular vectors $\mathbf{u}_i$ associated with $N_T - 1$ non-zero singular values. Thus, $\mathbf{u}_i$ can be expressed as the linear combination of the column vectors of $\Pi_{\mathbf{h}_{PE}}$, and, as a consequence, $\mathbf{h}_{\mathrm{PE}}^{H}\mathbf{u}_i = 0$. Hence, the vector $\mathbf{h}_{\mathrm{PR}}$ can be arbitrarily selected from $N_T - 1$ left singular vectors $\mathbf{u}_i$, and then used in Eqs (18) and (19).

TABLE 1. Set of general simulation parameters.

Parameter	Value	Reference
d_{PE}	5 m	PB-EH distance
d_{ER}	10 m	EH-RX distance
d_{PR}	10 m	PB-RX distance
N_T / N_R	8 / 8	transmit / receive antennas of the PB
β	20 dB	PB antenna isolation
ϵ_{SI}	-40 dB	self-interference channel estimation error
$P_{\mathrm{s_p}}$	10 dBm	static power consumed at the PB
η_{pa}	0.7	PA efficiency
f	915 MHz	operating frequency
γ	3	path loss exponent

C. NO-CSI: RANDOM BEAMFORMING

A random beamforming (RB) vector is a simple alternative that can be employed when CSI is not available at the PB. In this case, the vector is obtained from a random realization of the channel vector, i.e. $\hat{\mathbf{h}}_{\mathrm{PR}}$ is $N_T \times 1$ random vector that verifies $|\hat{\mathbf{h}}_{\mathrm{PR}}|^2 = 1$.

D. EFFECT OF BEAMFORMING DESIGN: NUMERICAL RESULTS

We now evaluate the performance of the beamforming strategies previously introduced. In all instances, the average secrecy capacity ($\overline{C_s}$) and average secrecy energy efficiency ($\overline{\mathrm{SEE}}$) metrics are evaluated by averaging over all L frames on which transmission is organized and over J channel realizations. A value of $L = 10$ frames is assumed, with $J = 10^4$ Monte Carlo runs per frame.

Considering two sets of values for ρ, i.e., $\rho = 0.1$ and $\rho = 0.99$, as well as NLOS/LOS scenarios with $K = 0$ and $K = 4$, respectively, and taken the time-splitting factor $\theta = 1/3$. Simulation parameters are summarized in Table 1, where ϵ_{SI} models the imperfect FD cancellation in (20). We consider a realistic scenario with values around $30 - 40$ dB of channel

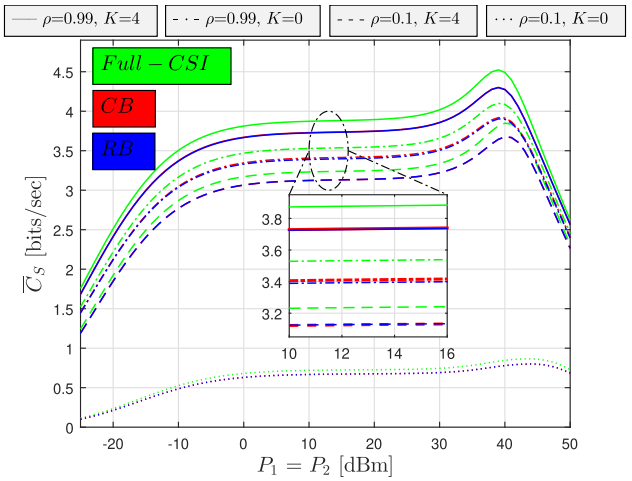

FIGURE 3. Average secrecy capacity under different beamforming strategies.

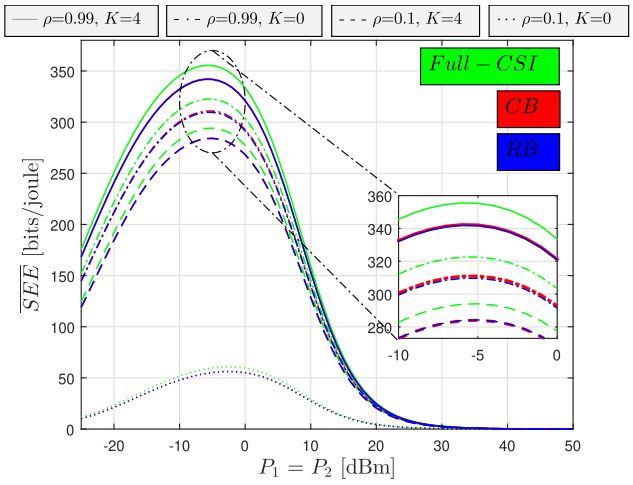

FIGURE 4. Average secrecy energy efficiency under different beamforming strategies.

estimation error. The path loss is expressed in dB as $PL = PL_0 - 10\gamma \log_{10}(d)$, where d is the link distance and PL_0 is the fixed loss at a reference distance of 1 meter. PL_0 is given by $PL_0 = 20\log_{10}(\lambda/4\pi)$, where λ is the signal wavelength. The parameters of the nonlinear EH are set as $a = 150$, $b = 0.014$ and $P_s = 0.024$ W [38].

Figures 3 and 4 illustrate the performance of the different beamforming schemes in terms of the average secrecy capacity and secrecy energy efficiency, respectively. We notice that, even though full-CSI availability allows for a better performance, the degradation of the no-CSI based schemes is not dramatical in all instances. We also see that the overall performance is degraded for lower values of ρ, which is coherent with the fact that beamforming quality for the MRT scheme is degraded due to channel aging. This effect is less pronounced in the presence of a dominant LOS component. In these figures, the benefits of energy-information channel correlation on both metrics can be appreciated. As is stated by [17, Eq. 13], this benefit is more significant in Rayleigh channels ($K = 0$), meanwhile, in LOS channels ($K = 4$) the effect is reduced. It can be observed in Figure 3 that $\overline{C}_S$ is approximately invariant when the transmitted power ($P_1 = P_2$) varies from 0 to 30 dBm. In this case, an increment of P_1 is reflected on a large energy harvested to be employed during phase 2. On the other hand, a large value of P_2 will increase the jamming signal over RX and degrade its SNR (Eq. 12). However, due to the imperfect self-interference cancellation, a large P_2 will also affect the SNR of the desired user (PB) (Eq. 11). In this range of transmitted power, both effects are balanced, and the secrecy capacity will remain almost constant. The peaky behavior around 40 dBm is due to an increase in the energy conversion efficiency due to the nonlinear characteristic of the energy harvester (8). For the case of $\overline{\text{SEE}}$, we can see that a transmitted power around 0 dBm provides the best results. In this metric, an increment of P_2 above 0 dBm is reflected in large power consumption while the secrecy capacity is kept invariant (see Figure 3). These results motivate the necessity of optimizing the power transmitted at each phase in order to exploit the benefits of the proposed systems. This issue will be addressed in the following sections.

On the other hand, these results also suggest that having CSI knowledge for the eavesdropper's link (PB-RX) does not provide a major benefit, compared to the case of no-CSI. Hence, the simplest beamforming architecture, i.e., random beamforming, will be considered in the analysis.

V. POWER ALLOCATION AND TIME-SPLITTING STRATEGIES

According to the results in the previous section, choosing a RB strategy is a recommended option that simplifies system design while eliminating the need of eavesdropper's CSI knowledge at the PB. With this in mind, the optimization problems in Section III-A may be redefined as:

- **S2: Secrecy Capacity Maximization**. The secrecy capacity maximization problem with RB is defined as:

$$(S2): \max_{P_1,P_2,\theta} C_s \quad \text{s.t. } P_1, P_2 \leq P_{max}, \quad 0 < \theta < 1. \tag{22}$$

- **J2: Secrecy Energy Efficiency Maximization**. The secrecy energy efficiency maximization problem with RB is formulated as:

$$(J2): \max_{P_1,P_2,\theta} SEE \quad \text{s.t. } P_1, P_2 \leq P_{max}, \quad 0 < \theta < 1. \tag{23}$$

Contrary to other works [39], these optimization problems cannot be solved using the typical local solvers (i.e. like `fmincon` in Matlab) due to the non-convex nature of the problem. In this case, to obtain the values of P_1, P_2 and θ that jointly optimize the performance metric of interest, it is necessary to use a solver which allows a global search.

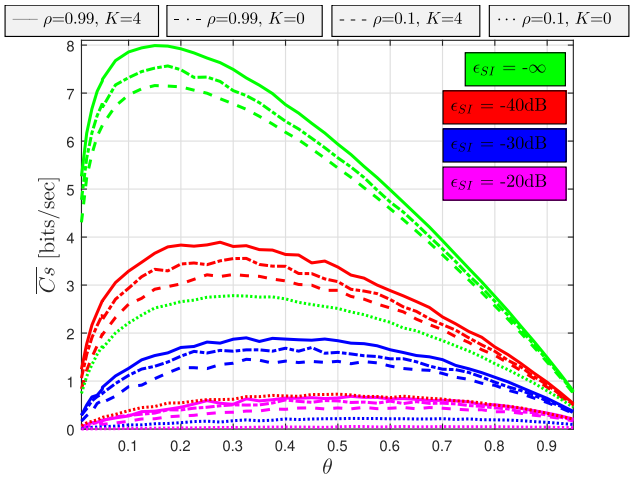

FIGURE 5. Average secrecy capacity of EH-PB link as a function of θ, for $P_1 = P_2 = 0$ dBm. $\rho = 0.1$ and 0.99, $K = 0$ and 4, and ϵ_{SI} takes different values.

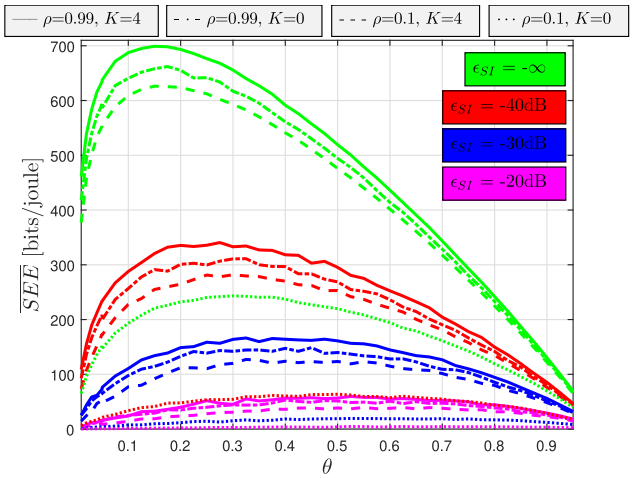

FIGURE 6. Average secrecy energy efficiency of EH-PB link as a function of θ, for $P_1 = P_2 = 0$ dBm. $\rho = 0.1$ and 0.99, $K = 0$ and 4, and ϵ_{SI} takes different values.

In this sense, some algorithms, namely the *GlobalSearch*, the *MultiStart* and the *Genetic Algorithm*, were employed in order to double-check the correctness of the global solution. We will later see that in the presence of residual self-interference in the PB full-duplex operation, the value of θ can be set to a fixed value and then optimize the values of P_1, P_2 to balance the effects of jamming and self-interference. Because of the multiple interplays between the parameters of the system model, we will first analyze the effect of θ (for a fixed transmit power) and P_1, P_2 (for a fixed time-splitting ratio).

A. EFFECT OF TIME-SPLITTING RATIO

We first evaluate the impact of the time-splitting ratio on the secrecy performance metrics, when a fixed transmit power at the PB is considered. For the sake of simplicity, the same parameter values as in Section IV.D are considered. We also assume $P_1 = P_2 = 0$ dBm, and the SI channel estimation error ϵ_{SI} takes different values, in order to account for dissimilar SI cancellation performances. Again, NLOS/LOS set-ups and extreme conditions for the correlation parameter ρ are also considered.

Figures 5 and 6 show the evolution of the secrecy performance metrics as a function of θ. In the absence of SI channel estimation error, we see that both secrecy metrics have an optimal value of θ for which performance is maximized. This also happens when imperfect SI cancellation is considered, since a finite ϵ_{SI} has a flattening effect on the secrecy metrics. This suggests that a close to optimal operation can be achieved for a certain range of θ values, both in terms of average secrecy capacity and energy efficiency, and regardless of the NLOS/LOS condition and the value of ρ.

We also see that high correlation values have a two-fold benefit in system performance: energy beamforming in phase 1 is barely degraded in the absence of channel aging, and the average received power at the PB during phase 2 is also increased thanks to the correlation between the energy and information links [16].

B. EFFECT OF POWER ALLOCATION IN PHASES 1 AND 2

Our aim now is to understand the effect of power allocation for the energy transmission and jamming phases on the secure system performance. The time-splitting factor is now fixed to $\theta = 1/3$, and the rest of parameters are similar to those in the previous figures. Figures 7 and 8 show the evolution of the secrecy performance metrics as a function of the jamming power P_2, for a given energy transmission power $P_1 = 0$ dBm, and different NLOS/LOS, correlation and SI cancellation conditions. In the absence of SI, increasing the jamming power improves the average secrecy capacity, although such improvement saturates when the jamming signal arriving at the eavesdropper is sufficiently large. However, as the imperfect SI cancellation becomes noticeable, the degradation in terms of self-interference due to the increase of the jamming power is the dominant effect, and further increasing the jamming power turns out to be detrimental. With regard to the average secrecy energy efficiency, we see than in all instances, there is a maximum value of P_2 that maximizes the secrecy energy efficiency: this value is reduced as ϵ_{SI} grows.

We observe that the maximization of both metrics is not reached for the same value of P_2. However, the values of P_2 that maximize both performance metrics are reasonably close; this suggests that in practical systems, i.e., in the presence of a finite ϵ_{SI}, it is possible to obtain a good secrecy performance without a major degradation of energy efficiency. In general, the amount of residual self-interference and the saturation of the non-linear EH limit the performance of our system when P_1 and P_2 vary. Hence, the trade-off between security and energy efficiency maximization needs to be further evaluated. It can be observed, throughout Figures 5 to 8, that in NLOS channels the gain due to channel

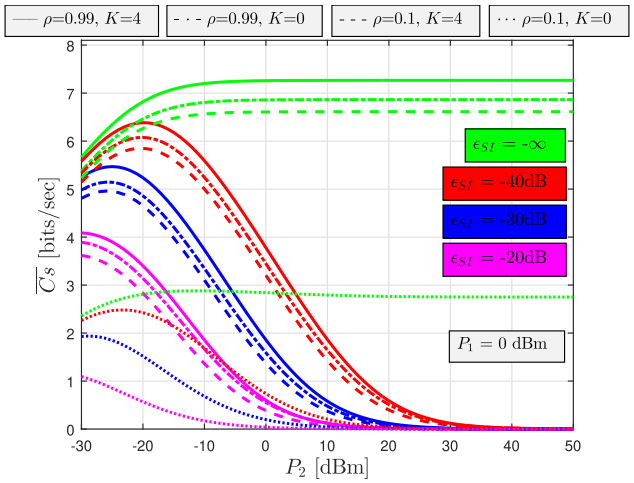

FIGURE 7. Average secrecy capacity of EH-PB link as a function of P_2 (varying from −30 to 50 dBm). $P_1 = 0$ dBm, $\rho = 0.1$ and 0.99, $K = 0$ and 4, and ϵ_{SI} takes different values.

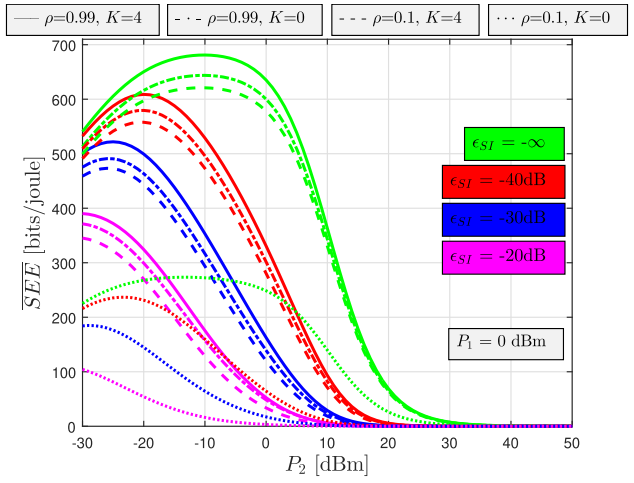

FIGURE 8. Average secrecy energy efficiency of EH-PB link as a function of P_2 (varying from −30 to 50 dBm). $P_1 = 0$ dBm, $\rho = 0.1$ and 0.99, $K = 0$ and 4, and ϵ_{SI} takes different values.

correlation is even more pronounced than the gain obtained in LOS channels.

C. JOINT OPTIMIZATION OF POWER ALLOCATION AND TIME-SPLITTING RATIO

After evaluating the individual effects of the power allocation and time-splitting ratio parameters, in this subsection we address the optimization problems S2 and J2, to determine the optimal set of P_1, P_2 and θ that maximize the secrecy and energy efficiency performances.

With this objective, we choose an optimization technique based on the *Genetic Algorithm (GA)*. The GA is a heuristic method for solving both constrained and unconstrained optimization problems that are not well suited for standard optimization algorithms. We choose the GA due to its ability to solve problems of highly nonlinear objective functions that have several local extreme values. This is the case of our scenario where conventional optimization functions return a

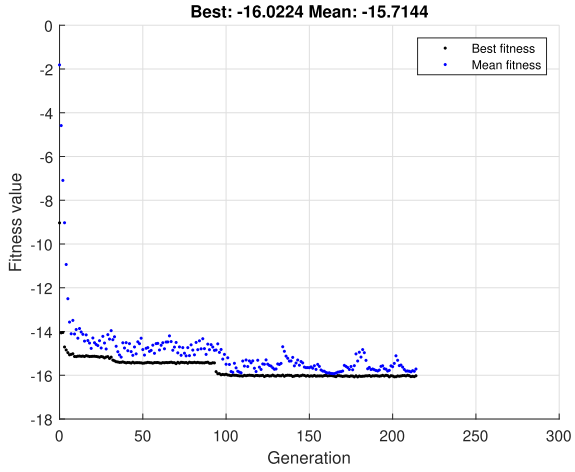

FIGURE 9. Value of objective function versus the number of iterations of the genetic algorithm.

local minimum point. The GA has the capacity to overcome this deficiency.

We also tested several global optimization algorithms such as *PatternSearch*, *MultiStart*, and *GlobalSearch*. However, the best results in terms of convergence were observed when using *Genetic Algorithm (GA)*. This is exemplified in Figure 9, where the value of the utility function (the fitness value) versus the number of iterations (generations) is represented, for the maximization of $\overline{C}_S$. We see that, on average, the algorithm converges in around 150-250 iterations. A similar behavior is obtained when the goal is maximizing the $\overline{\text{SEE}}$, although it's not explicitly shown here for the sake of compactness.

The pseudocode used for the optimization of both $\overline{C}_S$ and $\overline{\text{SEE}}$ is shown in Algorithm 1. The algorithm stops if *(i)* the average relative change in the best fitness function value, represented by $\overline{\Delta}(FitVal_{\text{Best}})$, is less than or equal to the given tolerance (ε_0) or *(ii)* the number of iterations, represented by $n°It$, is larger than a predefined value ($I_{\max}$).

The good results obtained with the GA, which avoid the convergence at local minimum points, are obtained at the cost of higher implementation complexity. However, this issue is out of the scope of our work, and the development of simplified algorithms to solve the optimization problem are left for future research activities. The optimum performance values are illustrated in Figures 10, 11, 12 and 13, as a function of the SI channel estimation error.

In figures 10 and 12, we observe that the optimal value of P_1 it is reasonably flat regardless of the value of ϵ_{SI}. Conversely, the optimal value of P_2 is decreased as the SI channel estimation error grows for both secrecy performance metrics: reducing the jamming power reduces self interference, and also improves energy efficiency. In figures 11 and 13, we can observe that the optimal time-switching ratio that maximizes both performance metrics is always confined in $\theta \approx 0.05$, regardless of the value of ϵ_{SI}.[3] The optimization curves are

[3]This value of $\theta \approx 0.05$ is in concordance with those reported considering the case of power splitting implementation [40].

Algorithm 1 Genetic Algorithm for $\overline{C}_S$ / $\overline{\text{SEE}}$ Maximization

Define:
- number of design variables (P_1, P_2, θ);
- population size;
- maximum number of iterations ($It_{\max}$);
- tolerance (ε_0);
- range values for P_1, P_2 and θ;

Generate:
- the initial population randomly;

Apply:
- the fitness function to each member of the population;

while $\overline{\Delta}(FitVal_{Best}) > \varepsilon_0$ ***or*** $n°It < I_{max}$ **do**
- **Select:**
  - the members of the population that will be crossed in the next generation;
- **Make:**
  - the migration of the best individuals from one subpopulation replacing the worst individuals in another subpopulation;
- **Make:**
  - the crossover combining two individuals to form a crossover child for the next generation;
- **Apply:**
  - the fitness function to each member of the population;
- **Make:**
  - the replacement by the best individuals to make up the population of the next generation;

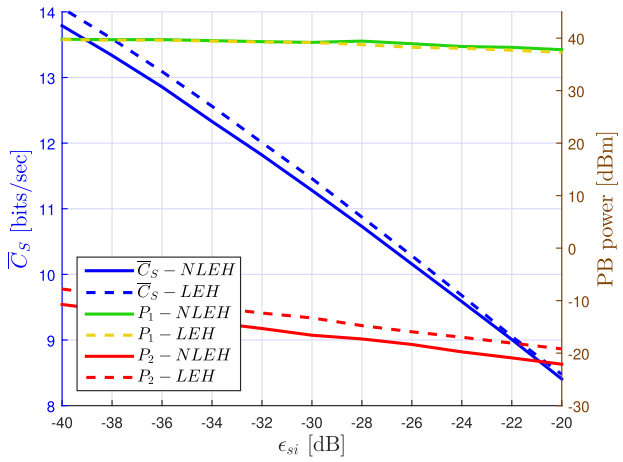

FIGURE 10. Average secrecy capacity optimizations for linear and nonlinear EH. P_1 and P_2 evolution with $\rho = 0.99$ and $K = 4$.

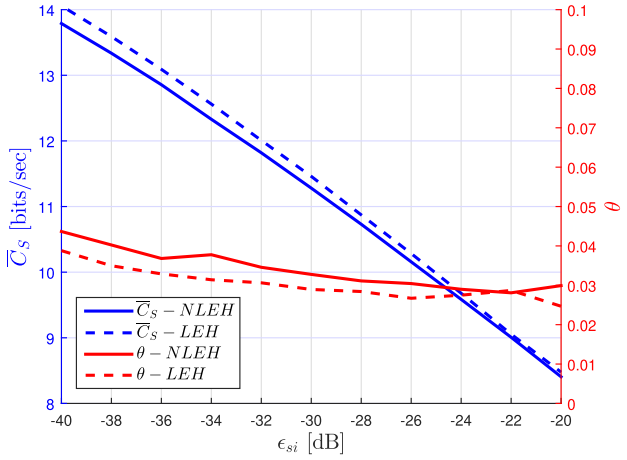

FIGURE 11. Average secrecy capacity optimizations for linear and nonlinear EH. θ evolution with $\rho = 0.99$ and $K = 4$.

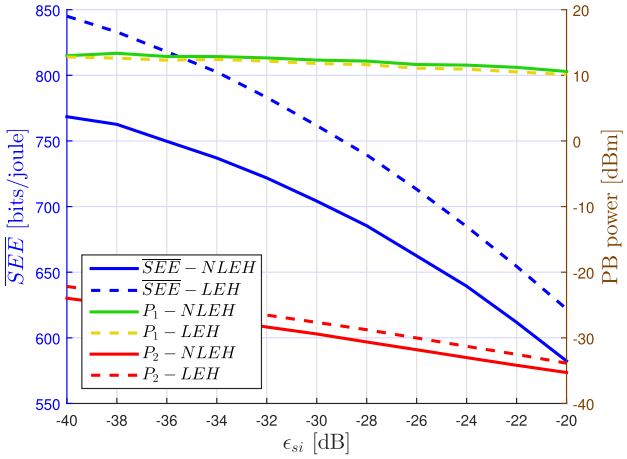

FIGURE 12. Average secrecy energy efficiency optimizations for linear and nonlinear EH. P_1 and P_2 evolution with $\rho = 0.99$ and $K = 4$.

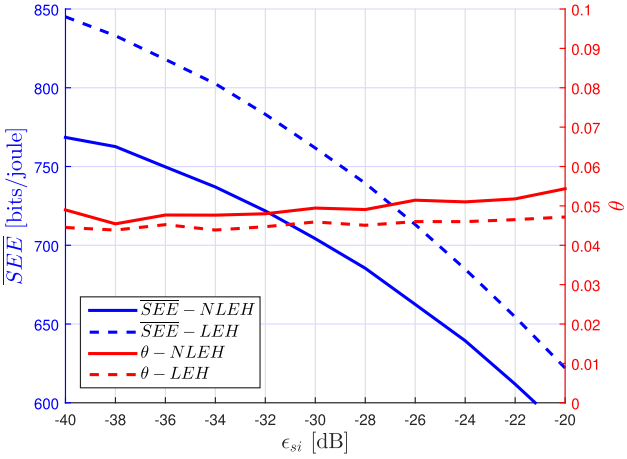

FIGURE 13. Average secrecy energy efficiency optimizations for linear and nonlinear EH. θ evolution with $\rho = 0.99$ and $K = 4$.

obtained considering linear and non-linear energy harvesters. It can be observed that the time-splitting factor is not affected by the type of harvester. Moreover, secrecy capacity and transmitted power are also slightly affected when linear and nonlinear harvesters are considered. On the other hand, the nonlinear harvester affects the secrecy energy efficiency, and its effect is even more pronounced when a good level of

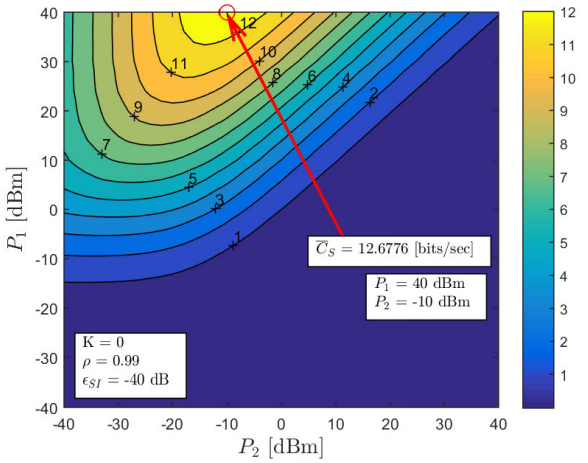

FIGURE 14. Average secrecy capacity of EH-PB link as a function of P_1 and P_2 (both varying from -40 to 40 dBm). $\rho = 0.99$, $K = 0$, and $\epsilon_{SI} = -40$ dB.

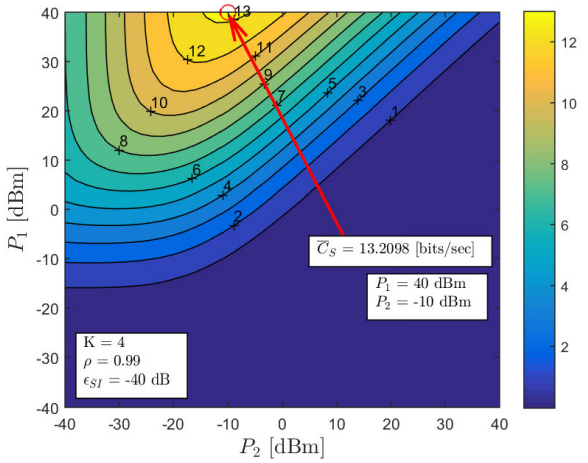

FIGURE 15. Average secrecy capacity of EH-PB link as a function of P_1 and P_2 (both varying from -40 to 40 dBm). $\rho = 0.99$, $K = 4$, and $\epsilon_{SI} = -40$ dB.

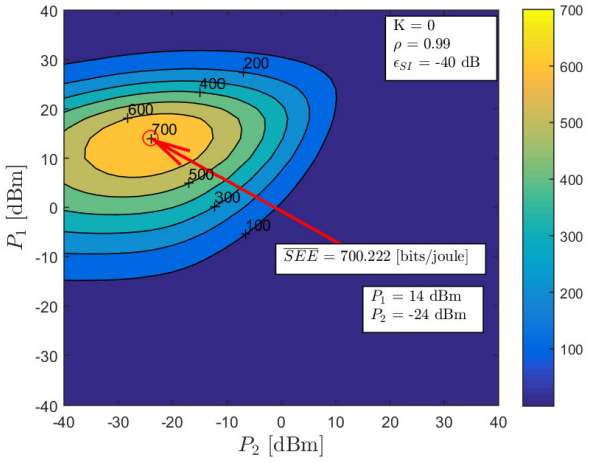

FIGURE 16. Average secrecy energy efficiency of EH-PB link as a function of P_1 and P_2 (both varying from -40 to 40 dBm). $\rho = 0.99$, $K = 0$, and $\epsilon_{SI} = -40$ dB.

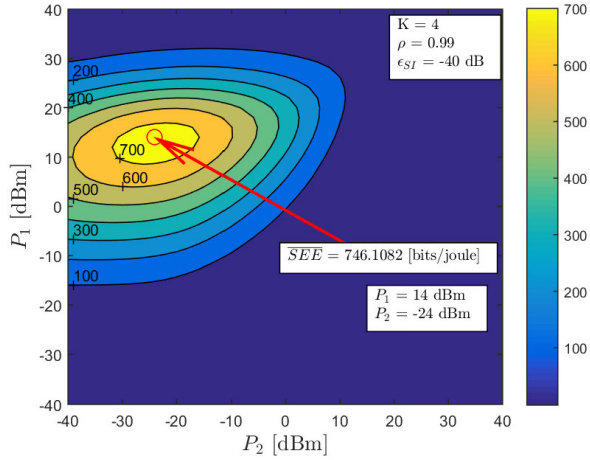

FIGURE 17. Average secrecy energy efficiency of EH-PB link as a function of P_1 and P_2 (both varying from -40 to 40 dBm). $\rho = 0.99$, $K = 4$, and $\epsilon_{SI} = -40$ dB.

self-interference cancellation is considered, as is illustrated in Figures 12 and 13.

In the following simulations, θ is fixed to 0.05 that is a reasonable value that optimize both metrics. With this consideration, we now visualize the effect of varying P_1 and P_2 in Figures 14, 15, 16 and 17. A moderate SI level is assumed, i.e. $\epsilon_{\text{SI}} = -40$ dB. It is evident that the best results in terms of $\overline{C}_S$ are obtained for large TX power at phase 1, $P_1 = 38 - 40$ dBm, whereas the jamming signal powered needs to be lowered (P_2) when the PB acts as a friendly jammer. On the other hand, the best result for the $\overline{\text{SEE}}$ is reached when the PB operates with power levels around 10 dBm during phase 1, and -30 dBm during phase 2. Hence, the effects of saturation at the EH and the residual self-interference are better highlighted when the $\overline{\text{SEE}}$ is under consideration.

D. FULL-DUPLEX VS HALF-DUPLEX OPERATION

In this section it is evaluated the performance of a PB operating in full-duplex mode with non-ideal self-interference cancellation (i.e., through channel estimation error ϵ_{SI}), and compare its performance with a PB that only operates in half-duplex mode. In this case, during phase 2 the PB only operate as a receiver (jamming signal is not transmitted). The transmitted power at phase 1 is settled to $P_1 = 20$ dBm. This value is a good compromise between the power required to maximize the secrecy capacity (around 40 dBm) and the energy efficiency that requires a transmitted power of 14 dBm.

We consider a scenario with Rayleigh channel ($K = 0$) for the cases of low and high correlation between energy and information channels. Secrecy capacity and secrecy energy efficiency results are illustrated in Figures 18, 19, 20 and 21, respectively. In these figures, two different regions can be identified: *a)* a region where FD outperforms HD operation, and *b)* a region where HD outperforms FD operation. These regions are delimited by the results obtained operating in HD mode. As expected, the performance of FD and HD

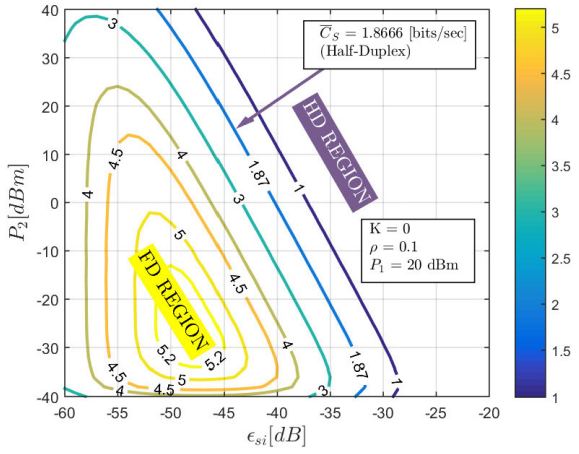

FIGURE 18. Average secrecy capacity: Full-duplex vs. half-duplex operation, as a function of ϵ_{SI} and P_2. $\rho = 0.1$, $K = 0$, $P_1 = 20$ dBm, and $\theta = 0.05$.

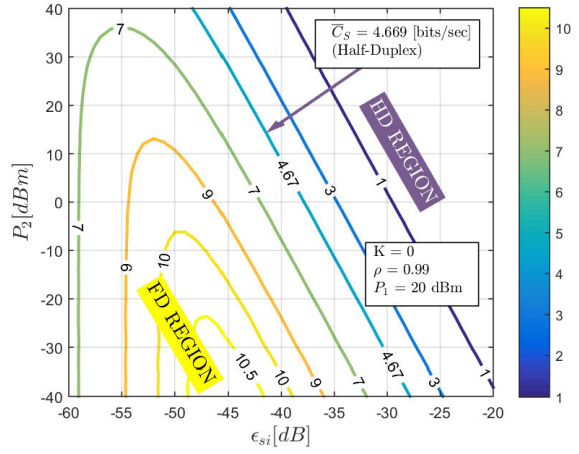

FIGURE 19. Average secrecy capacity: Full-duplex vs. half-duplex operation, as a function of ϵ_{SI} and P_2. $\rho = 0.99$, $K = 0$, $P_1 = 20$ dBm, and $\theta = 0.05$.

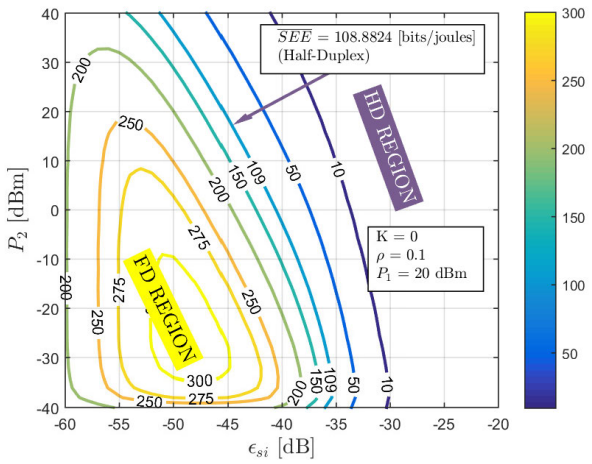

FIGURE 20. Average secrecy energy efficiency: Full-duplex vs. half-duplex operation, as a function of ϵ_{SI} and P_2. $\rho = 0.1$, $K = 0$, $P_1 = 20$ dBm, and $\theta = 0.05$.

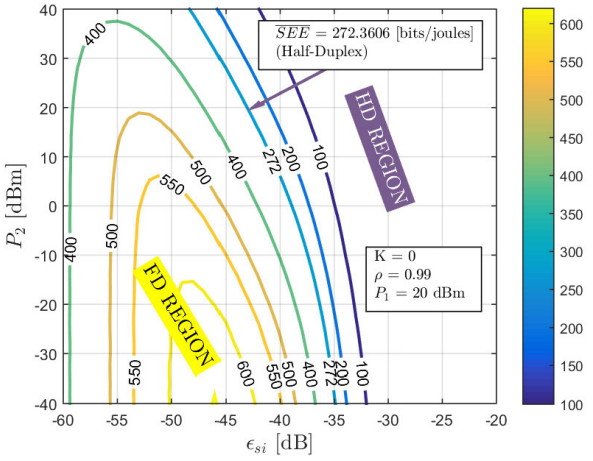

FIGURE 21. Average secrecy energy efficiency: Full-duplex vs. half-duplex operation, as a function of ϵ_{SI} and P_2. $\rho = 0.99$, $K = 0$, $P_1 = 20$ dBm, and $\theta = 0.05$.

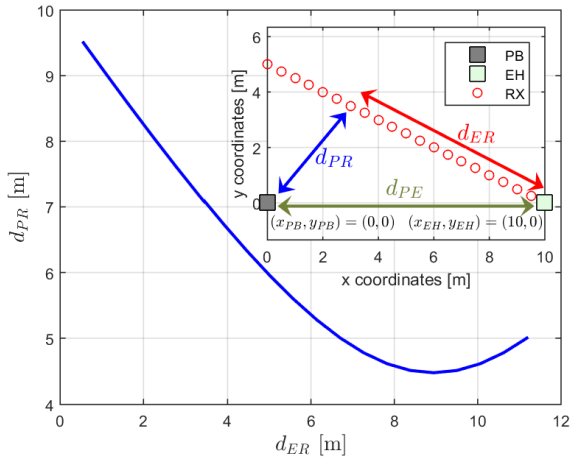

FIGURE 22. Locations of PB (gray marker), EH (green marker) and RX (red markers), and distance from the RX to EH and PB.

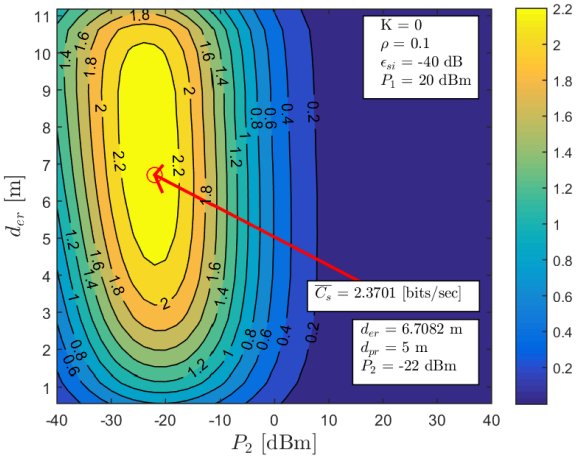

FIGURE 23. Average secrecy capacity as a function of P_2 and d_{ER}. $K = 0$, $\rho = 0.1$, $P_1 = 20$ dBm, $\epsilon_{SI} = -40$ dB, and $\theta = 0.05$.

techniques is governed by the residual self-interference level. A PB with FD capacity outperforms a PB operating in HD mode when moderate levels of SI channel estimation error are considered ($\epsilon_{SI} < -30$ dB). We also observe that the power

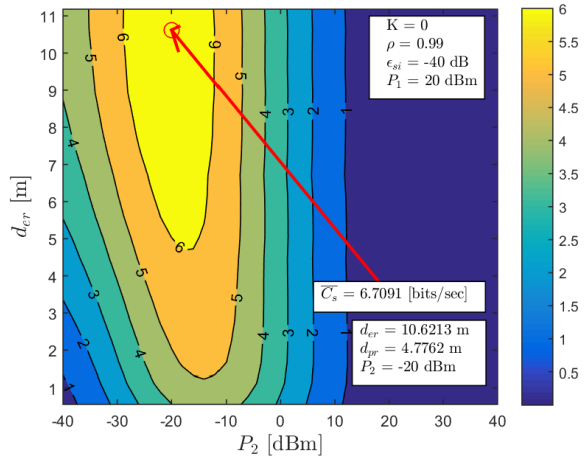

FIGURE 24. Average secrecy capacity as a function of P_2 and d_{ER}. $K = 0$, $\rho = 0.99$, $P_1 = 20$ dBm, $\epsilon_{SI} = -40$ dB, and $\theta = 0.05$.

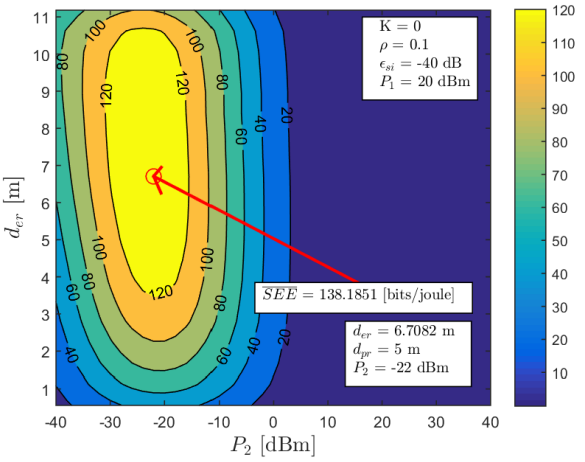

FIGURE 25. Average secrecy energy efficiency as a function of P_2 and d_{ER}. $K = 0$, $\rho = 0.1$, $P_1 = 20$ dBm, $\epsilon_{SI} = -40$ dB, and $\theta = 0.05$.

of the jamming signal needs to be properly tuned in order to reach a good trade-off between secrecy capacity and energy efficiency.

E. EFFECT OF VARYING RX LOCATION

Finally, we evaluate the secrecy performance metrics when varying the position of the eavesdropper (RX) with respect to the EH and the PB, as is illustrated in Figure 22. The transmitted power at phase 1 is settled to $P_1 = 20$ dBm, and the jamming power P_2 varies from -40 to 40 dBm. We consider an scenario with Rayleigh channel ($K = 0$) for the cases of low and high correlation between energy and information channels and the set of general evaluation parameters remain unchanged.

In the new scenario, the PB is placed at the coordinates $(x_{\text{PB}}, y_{\text{PB}}) = (0, 0)$ and the EH is located at $(x_{\text{EH}}, y_{\text{EH}}) = (10, 0)$. Initially RX is placed at $(x_{\text{RX}}, y_{\text{RX}}) = (0, 5)$, and its displacement of RX is expressed by $y_{\text{RX}} = 5 - 0.5\, x_{\text{RX}}$ with $0 \leq x_{\text{RX}} < 10$ meters. As the position of RX is changed, this induces a variation of d_{ER} (distance between EH to RX) and d_{PR} (distance between PB to RX) (see Figure 22) that modify the overall system performance. The location of each element and the different positions of the eavesdropper RX are illustrated in figure 22.

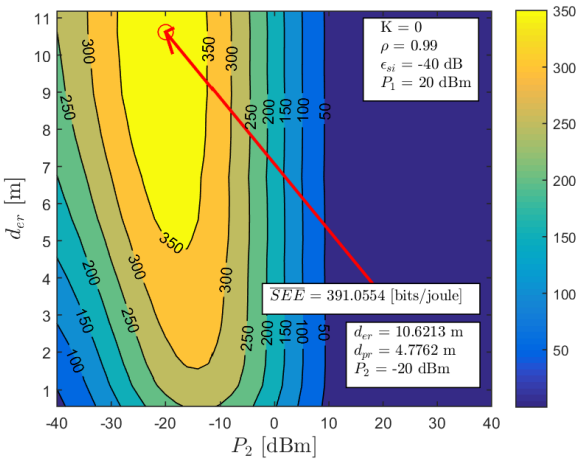

FIGURE 26. Average secrecy energy efficiency as a function of P_2 and d_{ER}. $K = 0$, $\rho = 0.99$, $P_1 = 20$ dBm, $\epsilon_{SI} = -40$ dB, and $\theta = 0.05$.

We observe that the best results for the $\overline{C}_S$ and the $\overline{\text{SEE}}$ are obtained when the eavesdropper (RX) is closer to the PB, which corresponds to a higher degradation of the EH-RX link. In this case, the jamming signal affects severely the capacity of the eavesdropper (RX), increasing the secrecy capacity of the system. Moreover, when RX is near to the PB, lower jamming signal power is required to degraded the SNR at RX increasing the energy efficiency of the link. These results can be seen in Figures 23, 24, 25 and 26. We also see that $\overline{C}_S$ and $\overline{\text{SEE}}$ reach the maximum value at identical locations of RX, $d_{\text{ER}} = 6.71$ meters, $d_{\text{PR}} = 5$ meters (channel with low-correlation, $\rho = 0.1$) with a jamming signal $P_2 = -22$ dBm, and $d_{\text{ER}} = 10.62$ meters, $d_{\text{PR}} = 4.78$ meters (channel with high-correlation, $\rho = 0.99$), with a jamming power of $P_2 = -20$ dBm.

VI. CONCLUDING REMARKS

We addressed the design of practical secure full-duplex wireless powered communication systems, by taking into account relevant key aspects such as EH non-linearity, link correlation, channel aging, CSI availability, or imperfect self-interference cancellation. Several key conclusions and design recommendations can be extracted from our work: *i)* the implementation of a FD-PB that operates as a friendly jammer outperforms conventional HD-PB and gives a good balance between system security and energy efficiency. *ii)* correlation between energy and information channels cannot be neglected, and is beneficial for physical layer security. This effect is even more pronounced when NLOS channels are under consideration. *iii)* high-complexity optimization techniques can be avoided when practical aspects as those listed above are considered. *iv)* performance degradation due to non-optimal jamming beamforming design under Eve's CSI lack of knowledge is minor, and *v)* the selection of the

time switching ratio for SWIPT is not critical within a certain range, and its value can be fixed in most scenarios. Future research activities in this line are: the study of scenarios with random mobility, the derivation of analytical expressions for the secrecy performance metrics, and the development of specific solutions of the highly-complex optimization problem identified in this scenario.

REFERENCES

[1] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IoT) technologies, applications and challenges," in *Proc. IEEE Smart Energy Grid Eng. (SEGE)*, Aug. 2016, pp. 381–385.

[2] R. Zhang and C. K. Ho, "MIMO broadcasting for simultaneous wireless information and power transfer," *IEEE Trans. Wireless Commun.*, vol. 12, no. 5, pp. 1989–2001, May 2013.

[3] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electron.*, vol. 3, no. 1, pp. 20–29, Jan. 2020.

[4] D. Xu and H. Zhu, "Secure transmission for SWIPT IoT systems with full-duplex IoT devices," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10915–10933, Dec. 2019.

[5] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8169–8181, Oct. 2019.

[6] G. de Meulenaer, F. Gosset, F.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *Proc. IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun.*, Oct. 2008, pp. 580–585.

[7] L. Sun and Q. Du, "A review of physical layer security techniques for Internet of Things: Challenges and solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[9] J. Zhang, S. Rajendran, Z. Sun, R. Woods, and L. Hanzo, "Physical layer security for the Internet of Things: Authentication and key generation," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 92–98, Oct. 2019.

[10] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[11] Y. Liu, J. Xu, and R. Zhang, "Exploiting interference for secrecy wireless information and power transfer," *IEEE Wireless Commun.*, vol. 25, no. 1, pp. 133–139, Feb. 2018.

[12] L. Tang and Q. Li, "Wireless power transfer and cooperative jamming for secrecy throughput maximization," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 556–559, Oct. 2016.

[13] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[14] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[15] E. Boshkovska, D. W. K. Ng, N. Zlatanov, and R. Schober, "Practical non-linear energy harvesting model and resource allocation for SWIPT systems," *IEEE Commun. Lett.*, vol. 19, no. 12, pp. 2082–2085, Dec. 2015.

[16] J. Matez-Bandera, P. Ramirez-Espinosa, J. Vega-Sanchez, and F. Lopez-Martinez, "Effect of correlation on the capacity of backscatter communication systems," *Electron. Lett.*, vol. 56, no. 14, pp. 716–719, 2020.

[17] A. Tarrías-Muñoz, J. L. Matez-Bandera, P. Ramírez-Espinosa, and F. J. López-Martínez, "Effect of correlation between information and energy links in secure wireless powered communications," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3780–3789, 2021.

[18] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[19] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Energy efficiency of confidential multi-antenna systems with artificial noise and statistical CSI," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1462–1477, Dec. 2016.

[20] N. Zlatanov, Z. Hadzi-Velkov, and D. W. K. Ng, "Asymptotically optimal power allocation for wireless powered communication network with non-orthogonal multiple access," in *Wireless Power Transfer Algorithms, Technologies and Applications in Ad Hoc Communication Networks*. Cham, Switzerland: Springer, 2016, pp. 231–251.

[21] I. Nikoloska, N. Zlatanov, Z. Hadzi-Velkov, and R. Zhang, "On the secrecy capacity of a full-duplex wirelessly powered communication system," *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5424–5439, Nov. 2019.

[22] J. Tang, L. Jiao, K. Zeng, H. Wen, and K.-Y. Qin, "Physical layer secure MIMO communications against eavesdroppers with arbitrary number of antennas," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 466–481, 2021.

[23] K. T. Truong and R. W. Heath, Jr., "Effects of channel aging in massive MIMO systems," *J. Commun. Netw.*, vol. 15, no. 4, pp. 338–351, 2013.

[24] L. N. Ribeiro, S. Schwarz, A. L. F. de Almeida, and M. Haardt, "Low-complexity massive MIMO tensor precoding," in *Proc. 54th Asilomar Conf. Signals, Syst., Comput.*, Nov. 2020, pp. 348–355.

[25] J. Tang, H. Wen, H. Song, T. Zhang, and K. Qin, "On the security–reliability and secrecy throughput of random mobile user in Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10635–10649, Oct. 2020.

[26] O. S. Badarneh, D. B. Da Costa, and P. H. J. Nardelli, "Wireless-powered communication networks with random mobility," *IEEE Access*, vol. 7, pp. 166476–166492, 2019.

[27] K. Xu, M. Zhang, J. Liu, N. Sha, W. Xie, and L. Chen, "SWIPT in mMIMO system with non-linear energy-harvesting terminals: Protocol design and performance optimization," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, Dec. 2019, Art. no. 72.

[28] M. Alageli, A. Ikhlef, and J. Chambers, "SWIPT massive MIMO systems with active eavesdropping," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 1, pp. 233–247, Jan. 2019.

[29] A. Zappone, P.-H. Lin, and E. A. Jorswieck, "Secrecy and energy efficiency in MIMO-ME systems," in *Proc. IEEE 16th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Jun. 2015, pp. 380–384.

[30] S. Morosi, L. Mucchi, D. Marabissi, M. Dolfi, and K. Marini, "On the trade-off between secrecy and energy-efficiency in multi-layer cellular networks," in *Proc. IEEE 5th Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2019, pp. 132–137.

[31] X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Commun. Lett.*, vol. 17, no. 4, pp. 637–640, Apr. 2013.

[32] T. Q. Duong, X. Zhou, and H. V. Poor, *Trusted Communications with Physical Layer Security for 5G and Beyond*. London, U.K.: Institution of Engineering and Technology, 2017.

[33] H. A. Suraweera, I. Krikidis, G. Zheng, C. Yuen, and P. J. Smith, "Low-complexity end-to-end performance optimization in MIMO full-duplex relay systems," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 913–927, Feb. 2014.

[34] T. Riihonen, S. Werner, and R. Wichman, "Spatial loop interference suppression in full-duplex MIMO relays," in *Proc. Conf. Rec. 43rd Asilomar Conf. Signals, Syst. Comput.*, 2009, pp. 1508–1512.

[35] Z. Mobini, M. Mohammadi, B. K. Chalise, H. A. Suraweera, and Z. Ding, "Beamforming design and performance analysis of full-duplex cooperative NOMA systems," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3295–3311, Jun. 2019.

[36] V. Tarokh, Y.-S. Choi, and S. Alamouti, "Complementary beamforming," in *Proc. IEEE 58th Veh. Technol. Conf. (VTC -Fall)*, vol. 5, Oct. 2003, pp. 3136–3140.

[37] X. Jiang, C. Zhong, Z. Zhang, and G. K. Karagiannidis, "Power beacon assisted wiretap channels with jamming," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8353–8367, Dec. 2016.

[38] 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.

[39] X. Zhang, Y. Qi, and M. Vaezi, "A rotation-based method for precoding in Gaussian MIMOME channels," *IEEE Trans. Commun.*, vol. 69, no. 2, pp. 1189–1200, Feb. 2021.

[40] Z. Hu, C. Yuan, and F. Gao, "Maximizing harvested energy for full-duplex SWIPT system with power splitting," *IEEE Access*, vol. 5, pp. 24975–24987, 2017.

SANTIAGO FERNÁNDEZ received the B.Sc. degree in electronic engineering from the Universidad Nacional del Sur (UNS), Bahía Blanca, Argentina, in 2016, where he is currently pursuing the Ph.D. degree in engineering with the Signal Processing and Communication Laboratory. His research interests include digital communications, digital signal processing, wireless communication, simultaneous wireless information and power transfer, IoT systems, and 5G and resource-efficient wireless communications and networks.

F. JAVIER LÓPEZ-MARTÍNEZ (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in telecommunication engineering from the University of Malaga, Spain, in 2005 and 2010, respectively. He was an Associate Researcher with the Communication Engineering Department, University of Malaga, from 2005 to 2012. He was a Marie Curie Postdoctoral Fellow with the Wireless Systems Laboratory, Stanford University, from 2012 to 2014, and the University of Malaga, from 2014 to 2015. He was a Visiting Researcher with the University College London, in 2010, and Queen's University Belfast, in 2018. Since 2015, he has been a Faculty Member with the Communication Engineering Department, University of Malaga, where he is currently an Associate Professor. His research interests include a diverse set of topics in the wide areas of communication theory and wireless communications, including stochastic processes, wireless channel modeling, physical layer security, and wireless powered communications. He received several research awards, including the best paper award from the Communication Theory Symposium at the IEEE GLOBECOM 2013, the IEEE COMMUNICATIONS LETTERS Exemplary Reviewer Certificate, in 2014 and 2019, and the IEEE TRANSACTIONS ON COMMUNICATIONS Exemplary Reviewer Certificate, in 2014, 2016, and 2019. He is an Editor of the IEEE TRANSACTIONS ON COMMUNICATIONS in the area of wireless communications.

FERNANDO H. GREGORIO received the B.Sc. degree from Universidad Tecnologica Nacional (UTN), Bahía Blanca, Argentina, the M.Sc. degree in electrical engineering from the Universidad Nacional del Sur (UNS), Bahía Blanca, and the D.Sc. degree in electrical engineering from the Helsinki University of Technology (HUT), Espoo, Finland, in 2007. Since 2008, he has been with the Departamento de Ingenieria Eléctrica y Computadoras, UNS. He is currently a Senior Researcher with the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina. His research interests include power amplifier nonlinearities and RF imperfection in MIMO–OFDM systems and multiuser communications.

JUAN E. COUSSEAU (Senior Member, IEEE) received the B.Sc. degree in electrical engineering from the Universidad Nacional del Sur (UNS), Bahía Blanca, Argentina, in 1983, and the M.Sc. and Ph.D. degrees in electrical engineering from the COPPE/Universidade Federal do Rio de Janeiro (UFRJ), Brazil, in 1989 and 1993, respectively. Since 1984, he has been with the undergraduate Departamento de Ingenieria Eléctrica y Computadoras, UNS. He is currently a Senior Researcher of the National Scientific and Technical Research Council (CONICET), Argentina. He has been involved in scientific and industry projects with research groups from Argentina, Brazil, Spain, USA, Finland, and South Africa. He is also a Coordinator of the Signal Processing and Communication Laboratory (LaPSyC), UNS. His research interests include adaptive and statistical signal processing with application to modern broadband wireless communications. He was the IEEE Circuits and Systems Chair of the Argentine Chapter, from 1997 to 2000, and a member of the Executive Committee of the IEEE Circuits and Systems Society, from 2000 to 2001 (the Vice President for Region 9). He participates in the IEEE Signal Processing Society Distinguished Lecturer Program 2006. He is currently the Director of the Instituto de Investigaciones en Ingeniería Eléctrica—Alfredo Desages, CONICET—UNS.