Artificial Noise for In-Home PLC Networks Under the Presence of PLC and Wireless Eavesdroppers

Mateus de L. Filomeno
Electrical Engineering Department
Federal University of Juiz de Fora
Juiz de Fora, Brazil
mateus.lima@engenharia.ufjf.br

Gustavo M. Campos
Electrical Engineering Department
Federal University of Juiz de Fora
Juiz de Fora, Brazil
gustavo.moraes@engenharia.ufjf.br

Ândrei Camponogara
Electrical Engineering Department
Federal University of Paraná
Curitiba, Brazil
andrei.camponogara@ufpr.br

Pedro H. Sartorello
Electrical Engineering Department
Federal University of Paraná
Curitiba, Brazil
pedro.sartorello@ufpr.br

Moisés V. Ribeiro
Electrical Engineering Department
Federal University of Juiz de Fora
Juiz de Fora, Brazil
mribeiro@engenharia.ufjf.br

2023 Symposium on Internet of Things (SIoT) | 979-8-3503-2943-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/SIOT60039.2023.10389936

***Abstract*—This paper investigates if an artificial noise designed based on the degrees of freedom of the cyclic prefix can increase the security of in-home power line communication (PLC) networks for Internet of Things applications. The artificial noise is generated to impair the decoding capacity of diverse eavesdroppers, which can be PLC or wireless nodes, while not affecting the communication between two PLC nodes. We carefully describe the artificial noise design and derive expressions for the signal-to-noise ratio of the legitimate receiver and eavesdroppers. Numerical results derived from measured data show that the considered artificial noise technique is more effective in the most threatening scenarios of PLC networks, which refer to those with PLC eavesdroppers close to the legitimate transmitter.**

***Index Terms*—artificial noise, hybrid communication, physical layer security, power line communication.**

I. Introduction

The Internet of Things (IoT) has emerged as a revolutionary paradigm, driving innovation across diverse sectors and offering unprecedented opportunities to create a sustainable and connected world. As the number of IoT devices continues to explode, the need for efficient and reliable communication technologies becomes increasingly critical. Power line communication (PLC) offers a compelling solution to address this challenge by utilizing existing electric power systems infrastructure for data transmission between IoT devices, promoting ubiquitous connectivity, and optimizing energy consumption [1].

On the other hand, security and privacy concerns arise due to the broadcast nature of electric power systems. Furthermore, power lines are electromagnetically unshielded so that a wireless device near them can overhear PLC signals [2]. This raises the possibility of eavesdropping a private information by malicious PLC or wireless devices. Cryptography is usually the first option to overcome this issue; however, it requires the exchange of encryption keys and consequently additional processing, hardware resources, and overhead for IoT devices. In this context, physical layer security (PLS) has emerged as an alternative strategy, leveraging communication media properties and thus not requiring encryption key exchange to enhance information security. In other words, PLS aims at capitalizing on diversity across time, frequency, or space domains to increase information security [3].

Focusing on single-input single-output (SISO) communication scenarios, PLS has been investigated for PLC-only networks [3]–[6], where legitimate nodes and eavesdroppers are connected through power lines, and PLC hybrid networks [7]–[9], where legitimate nodes communicate through power lines and the eavesdropper is a wireless device. To evaluate the impact of a PLC eavesdropper, the authors of [3] and [4] considered measurement data, whereas statistical models were adopted in [5]. These works demonstrate using different criteria and scenarios that, due to the existing correlation between the involved channels, a PLC eavesdropper can threaten the security of the information exchange, indicating that PLS solutions should be investigated. Regarding the cases where the eavesdropper is a wireless device, Camponogara *et al.* [7]–[9] studied distinct metrics and scenarios, including one with colluding eavesdroppers. In this case, the channels of the eavesdropper and the legitimate receiver can be assumed to be less correlated or even uncorrelated from each other [9]. Notwithstanding, the obtained results also pointed out emerging demands for the enhancement of PLS approaches to bolster security.

The literature has clearly stated the need for PLS techniques that increase the security of a PLC network for IoT applications. In this context, a practical approach to achieving secure communication is the injection of artificial noise (AN). It is intelligently generated to not degrade the signal-to-noise-ratio

This research was supported in part by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) under Grant 001, Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) under grants 404068/2020-0 and 314741/2020-8, Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) under grants APQ-03609-17 and TEC-PPM 00787-18, and Instituto Nacional de Energia Elétrica (INERGE).

(SNR) of the legitimate receiver, yet effectively disrupts the SNR of any passive eavesdropper nearby. Salem *et al.* [6] considered an AN injection in a PLC network and demonstrated that it could significantly help in reducing the negative impacts introduced by a PLC eavesdropper. The authors, on the other hand, considered a complex cooperative scenario with reduced spectral efficiency, where relay nodes should be always available.

Therefore, an alternative and simpler approach should be evaluated for increasing the security of PLC networks. In [10], the authors, considering a SISO-based orthogonal frequency-division multiplexing (OFDM) system, investigated the use of the degrees of freedom introduced by the cyclic prefix (CP) to design the AN. The proposed technique does not require relay-assisted communication while not degrading the spectral efficiency significantly. Nonetheless, the effectiveness of this technique can vary depending on the communication environment, such as signal propagation, interference, and noise levels. Consequently, to provide consistent security guarantees across different scenarios, this specific technique should be carefully analyzed.

Notably, the AN generated based on the degrees of freedom of CP has not yet been assessed in the context of PLC networks for IoT applications. To fill this research gap, the present paper evaluates whether this technique can enhance the security of in-home PLC systems under the presence of passive eavesdroppers that can be PLC or wireless devices. In this paper, we meticulously outline the design of the AN and formulate expressions to determine the SNRs for both the legitimate receiver (PLC node) and eavesdroppers (PLC or wireless nodes). Also, it presents a numerical analysis obtained from realistic measurements considering different positions of the eavesdroppers and amounts of power allocated to the AN. This analysis addresses the most critical scenario for security and the effectiveness of the AN injection.

Notation: Throughout this paper, $\mathbb{E}\{\cdot\}$ is the expectation operator, $\mathrm{Tr}(\cdot)$ denotes the trace operator, and $\mathrm{diag}\{\cdot\}$ returns a diagonal matrix keeping the main diagonal of the input matrix. Also, $(\cdot)^\dagger$ and $(\cdot)^\mathrm{T}$ are the conjugate transpose and transpose operators, respectively. Furthermore, $\mathbf{0}_{a\times b}$ stands for an $(a\times b)$-size matrix of zeros, $\mathbf{I}_a$ represents an a-size identity matrix, and $\mathbf{F} \in \mathbb{C}^{N\times N}$ denotes the normalized version of the N-length discrete Fourier transform (DFT) matrix.

II. System Model

Let us assume the system model illustrated in Fig. 1. It is a PLC network scenario composed of a legitimate transmitter—namely Alice—and a legitimate receiver—namely Bob—which communicate through the electric power system. In this scenario, there are also K_p PLC eavesdroppers that receive signals from Alice through the electric power systems and K_w wireless eavesdroppers that receive signals from Alice through the air based on the hybrid PLC-wireless communication (WLC) channels [2]. PLC and wireless eavesdroppers can be in different positions and, for the sake of simplicity, they will be generally called Eve throughout this section. Furthermore,

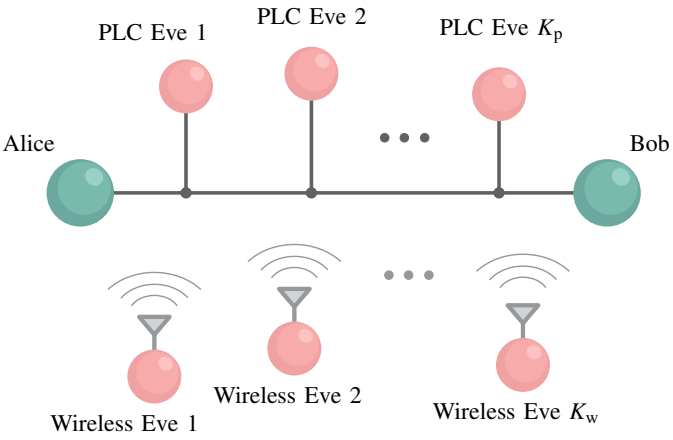

Fig. 1: Assumed PLC network scenario.

all nodes communicate using the Hermitian symmetric OFDM scheme, also known as discrete multitone modulation, detailed below.

Let $\mathbf{X}_i \in \mathbb{C}^{N\times 1}$ be the i^th OFDM transmitted information block, in the discrete-frequency domain, whose elements obey the Hermitian symmetry for baseband transmission. In this sense, $\mathbb{E}\{\mathbf{X}_i\} = \mathbf{0}_{N\times 1}$, $\forall i$, and $\mathbb{E}\{\mathbf{X}_i\mathbf{X}_i^\dagger\} = \mathbf{\Lambda}_{\sigma_\mathbf{x}^2}$, $\forall i$, is a diagonal matrix that stands for the autocorrelation matrix of the transmitted symbols, such that $\mathrm{Tr}(\mathbf{\Lambda}_{\sigma_\mathbf{x}^2}) = P_\mathbf{x}N$, with $P_\mathbf{x}$ being the total power assigned to the transmitted information block. In the discrete-time domain, the real-valued transmitted information block may be represented as

$$\mathbf{x}_i = \mathbf{\Psi}_\mathrm{T}\mathbf{F}^\dagger\mathbf{X}_i, \tag{1}$$

where the matrix $\mathbf{\Psi}_\mathrm{T} = [\mathbf{E}^\mathrm{T}_{N_\mathrm{cp}\times N}\mathbf{I}_N]^\mathrm{T}$ is responsible for the CP insertion, with N_cp indicating the CP-length and $\mathbf{E}_{N_\mathrm{cp}\times N} = [\mathbf{0}_{N_\mathrm{cp}\times(N-N_\mathrm{cp})}\mathbf{I}_{N_\mathrm{cp}}]$. The legitimate node sends the information block $\mathbf{x}_i$ plus an AN block $\mathbf{a}_i \in \mathbb{R}^{(N+N_\mathrm{cp})\times 1}$, in which $\mathbb{E}\{\mathbf{a}_i\} = \mathbf{0}_{(N+N_\mathrm{cp})\times 1}$, $\forall i$, and $\mathbb{E}\{\mathbf{a}_i\mathbf{a}_i^\dagger\} = \mathbf{R}_\mathbf{aa}$, $\forall i$, is the AN autocorrelation matrix, such that $\mathrm{Tr}(\mathbf{R}_\mathbf{aa}) = P_\mathbf{a}(N + N_\mathrm{cp})$, in which $P_\mathbf{a}$ is the total power assigned to the AN. The total transmission power is therefore $P_\mathrm{T} = P_\mathbf{x} + P_\mathbf{a}$.

The overall built block, i.e., information plus AN, is transmitted through a broadcast channel, which has a coherence time longer than the built block time interval so that it can be modeled as a linear time-invariant (LTI) system. Through this broadcast channel, the transmitted block reaches Bob and Eve, denoted by "b" and "e", respectively. If we assume that $l \in \{\mathrm{b}, \mathrm{e}\}$ and $\{h^l[n]\}_{n=0}^{L_l-1}$ represents the coefficients of the channel impulse response (CIR) between Alice and Bob or Eve, with L_l denoting the CIR length, the Toeplitz channel

matrix [10] associated with the l^{th} user can be defined as

$$\mathbf{H}^l = \begin{bmatrix} h^l[0] & 0 & 0 & \cdots & \cdots & 0 & 0 \\ h^l[1] & h^l[0] & 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ h^l[L_l-1] & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & h^l[0] & 0 \\ 0 & \cdots & 0 & h^l[L_l-1] & \cdots & h^l[1] & h^l[0] \end{bmatrix} \tag{2}$$

For baseband transmission, $\mathbf{H}^l \in \mathbb{R}^{(N+N_{\text{cp}})\times(N+N_{\text{cp}})}$. Note that $\mathbf{C}^l_{\mathbf{H}} = \mathbf{\Psi}_{\text{R}}\mathbf{H}^l\mathbf{\Psi}_{\text{T}} \in \mathbb{R}^{N\times N}$ is a circulant matrix whose first column has the CIR coefficients of the l^{th} user followed by zeros, and $\mathbf{\Lambda}^l_{\mathbf{H}} = \mathbf{F}\mathbf{C}^l_{\mathbf{H}}\mathbf{F}^\dagger \in \mathbb{C}^{N\times N}$ is a diagonal matrix with the channel frequency response of the l^{th} user at the main diagonal.

At the l^{th} user, the i^{th} discrete-time domain received block can be written as

$$\mathbf{y}^l_i = \mathbf{H}^l(\mathbf{x}_i + \mathbf{a}_i) + \mathbf{w}^l_i, \qquad \forall l \in \{\text{b}, \text{e}\}, \tag{3}$$

in which $\mathbf{w}^l_i \in \mathbb{R}^{(N+N_{\text{cp}})\times 1}$ indicates the additive noise vector affecting the i^{th} block and l^{th} user. The l^{th} user then carries out on $\mathbf{y}^l_i$ the inverse operations of those performed at Alice. As a result, the i^{th} block received by the l^{th} user can be expressed in the discrete-frequency domain as

$$\begin{aligned} \mathbf{Y}^l_i &= \mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{y}^l_i \\ &= \mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{H}^l\mathbf{x}_i + \mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{H}^l\mathbf{a}_i + \mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{w}^l_i \\ &= \mathbf{\Lambda}^l_{\mathbf{H}}\mathbf{X}_i + \mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{H}^l\mathbf{a}_i + \mathbf{W}^l_i, \end{aligned} \tag{4}$$

with the matrix $\mathbf{\Psi}_{\text{R}} = [\mathbf{0}_{N\times N_{\text{cp}}}\mathbf{I}_N]$ being responsible for the CP removal and $\mathbf{W}^l_i = \mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{w}^l_i$ indicating the discrete-frequency domain additive noise block, with $\mathbb{E}\{\mathbf{W}^l_i\} = \mathbf{0}_{(N+N_{\text{cp}})\times 1}$, $\forall i$, and $\mathbb{E}\{\mathbf{W}^l_i(\mathbf{W}^l_i)^\dagger\} = \mathbf{\Lambda}^l_{\sigma^2_{\text{w}}}$, $\forall i$, such that $\text{Tr}(\mathbf{\Lambda}^l_{\sigma^2_{\text{w}}}) = P_{\mathbf{W}^l}(N + N_{\text{cp}})$, with $P_{\mathbf{W}^l}$ denoting the total noise power at the l^{th} user.

III. Artificial Noise Based on CP Degrees of Freedom

The AN should be developed to worsen Eve's SNR but not Bob's. In this section, we describe an AN design to achieve this end based on the degrees of freedom introduced by the CP [10]. Also, the resulting SNRs at the legitimate and eavesdropper users are presented.

A. Artificial noise design

First, Alice has to design $\mathbf{a}_i$ to achieve a null signal when convolved with Bob's channel, which should not occur regarding Eve's. Mathematically, she could search for $\mathbf{a}_i$ such that $\mathbf{H}^{\text{b}}\mathbf{a}_i = \mathbf{0}_{(N+N_{\text{cp}})\times 1}$. However, $\mathbf{H}^{\text{b}}$ is a full rank square matrix, which has null space full of zeros, i.e., $\mathbf{a}_i = \mathbf{0}_{(N+N_{\text{cp}})\times 1}$. This solution is not desired since it does not detriment Eve's SNR. A possible alternative would be to design the AN in a different stage, e.g., using matrices $\mathbf{C}^{\text{b}}_{\mathbf{H}}$ or $\mathbf{\Lambda}^{\text{b}}_{\mathbf{H}}$. Notwithstanding, these matrices equally have full rank, thus preventing their application in the AN design.

To avoid the aforementioned problems, the authors of [10] exploited the degrees of freedom introduced by the CP, therefore using the matrix $\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}} \in \mathbb{R}^{N\times(N+N_{\text{cp}})}$. According to [10], $\mathbf{a}_i = \mathbf{V}^{\text{b}}_{\text{null}}\mathbf{d}_i$, such that $\mathbf{d}_i \in \mathbb{R}^{N_{\text{cp}}\times 1}$ is a vector of independent Gaussian random variables while $\mathbf{V}^{\text{b}}_{\text{null}} \in \mathbb{R}^{(N+N_{\text{cp}})\times N_{\text{cp}}}$ defines the right null space of $\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}}$, i.e.,

$$\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}}\mathbf{V}^{\text{b}}_{\text{null}} = \mathbf{0}_{N\times N_{\text{cp}}}. \tag{5}$$

Note that only $\mathbf{d}_i$ and $\mathbf{V}^{\text{b}}_{\text{null}}$ have to be found in order to design $\mathbf{a}_i$. The first can be obtained from any discrete random variable generator, while the second is yielded from the singular value decomposition (SVD). Based on the SVD, we can write

$$\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}} = \mathbf{U}^{\text{b}}\mathbf{\Sigma}^{\text{b}}(\mathbf{V}^{\text{b}})^{\text{T}}, \tag{6}$$

where $\mathbf{\Sigma}^{\text{b}} \in \mathbb{R}^{N\times(N+N_{\text{cp}})}$ is rectangular diagonal matrix with the singular values of $\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}}$, $\mathbf{U}^{\text{b}} \in \mathbb{R}^{N\times N}$ includes the left range and left null spaces of $\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}}$, and $\mathbf{V}^{\text{b}} \in \mathbb{R}^{(N+N_{\text{cp}})\times(N+N_{\text{cp}})}$ holds the right range and right null spaces of $\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}}$. The right null space of $\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{b}}$ will be defined by the N_{cp} last columns of $\mathbf{V}^{\text{b}}$. Therefore, we have

$$\mathbf{V}^{\text{b}}_{\text{null}} = \mathbf{V}^{\text{b}}[\mathbf{0}_{N_{\text{cp}}\times N}\mathbf{I}_{N_{\text{cp}}}]^{\text{T}}. \tag{7}$$

B. Signal-to-noise ratio

Assuming the AN is designed as in the previous subsection, the discrete-frequency domain representation of the i^{th} block received by Bob and Eve will be respectively given by

$$\mathbf{Y}^{\text{b}}_i = \mathbf{\Lambda}^{\text{b}}_{\mathbf{H}}\mathbf{X}_i + \mathbf{W}^{\text{b}}_i \tag{8}$$

and

$$\mathbf{Y}^{\text{e}}_i = \mathbf{\Lambda}^{\text{e}}_{\mathbf{H}}\mathbf{X}_i + \mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{e}}\mathbf{a}_i + \mathbf{W}^{\text{e}}_i. \tag{9}$$

Therefore, the resulting received block by Eve has a further noise term, i.e, $\mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{e}}\mathbf{a}_i$, that will detriment its SNR.

To yield the SNR, we can compute the portion of the total received energy related to the information block divided by the portion of the total received energy related to noise. Moreover, we can extract these energy terms from the main diagonal of the autocorrelation matrix associated with each of them. Based on (8), the SNR at Bob in the discrete-frequency domain can be written as the diagonal matrix that follows:

$$\begin{aligned} \mathbf{\Lambda}^{\text{b}}_{\gamma} &= \frac{\text{diag}\{\mathbb{E}\{(\mathbf{\Lambda}^{\text{b}}_{\mathbf{H}}\mathbf{X}_i)(\mathbf{\Lambda}^{\text{b}}_{\mathbf{H}}\mathbf{X}_i)^\dagger\}\}}{\text{diag}\{\mathbb{E}\{\mathbf{W}^{\text{b}}_i(\mathbf{W}^{\text{b}}_i)^\dagger\}\}} \\ &= \frac{\text{diag}\{\mathbf{\Lambda}^{\text{b}}_{\mathbf{H}}\mathbb{E}\{\mathbf{X}_i\mathbf{X}_i^\dagger\}\mathbf{\Lambda}^{\text{b}^\dagger}_{\mathbf{H}}\}}{\text{diag}\{\mathbb{E}\{\mathbf{W}^{\text{b}}_i(\mathbf{W}^{\text{b}}_i)^\dagger\}\}} \\ &= \frac{\mathbf{\Lambda}_{\sigma^2_{\text{x}}\mathbf{\Lambda}^{\text{b}}_{|\mathbf{H}|^2}}}{\mathbf{\Lambda}^{\text{b}}_{\sigma^2_{\text{w}}}}. \end{aligned} \tag{10}$$

At Eve, the SNR in the discrete-frequency domain can be similarly computed, despite there being two noise terms. It is therefore given by:

$$\mathbf{\Lambda}^{\text{e}}_{\gamma} = \frac{\text{diag}\{\mathbb{E}\{(\mathbf{\Lambda}^{\text{e}}_{\mathbf{H}}\mathbf{X}_i)(\mathbf{\Lambda}^{\text{e}}_{\mathbf{H}}\mathbf{X}_i)^\dagger\}\}}{\text{diag}\{\mathbb{E}\{(\mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{e}}\mathbf{a}_i + \mathbf{W}^{\text{e}}_i)(\mathbf{F}\mathbf{\Psi}_{\text{R}}\mathbf{H}^{\text{e}}\mathbf{a}_i + \mathbf{W}^{\text{e}}_i)^\dagger\}\}}. \tag{11}$$

At this point, we should observe that the noise term related to the AN, i.e., $\mathbf{F}\boldsymbol{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{e}}\mathbf{a}_i$, is independent of the natural noise term observed at Eve, i.e., $\mathbf{W}^{\mathrm{e}}$. Therefore, the autocorrelation matrix of the total resulting noise at Eve, which is in the denominator of (11), can be described as

$$\begin{aligned}\mathbf{R}^{\mathrm{e}}_{\mathrm{noise}} &= \mathbb{E}\{(\mathbf{F}\boldsymbol{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{e}}\mathbf{a}_i + \mathbf{W}^{\mathrm{e}}_i)(\mathbf{F}\boldsymbol{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{e}}\mathbf{a}_i + \mathbf{W}^{\mathrm{e}}_i)^{\dagger}\} \\ &= \mathbb{E}\{(\mathbf{F}\boldsymbol{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{e}}\mathbf{a}_i)(\mathbf{F}\boldsymbol{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{e}}\mathbf{a}_i)^{\dagger} + (\mathbf{W}^{\mathrm{e}}_i)(\mathbf{W}^{\mathrm{e}}_i)^{\dagger}\} \\ &= \mathbf{F}\boldsymbol{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{e}}\mathbf{R}_{\mathbf{aa}}\mathbf{H}^{\mathrm{e}\dagger}\boldsymbol{\Psi}^{\dagger}_{\mathrm{R}}\mathbf{F}^{\dagger} + \boldsymbol{\Lambda}^{\mathrm{e}}_{\sigma^2_{\mathbf{W}}} \\ &= \mathbf{R}^{\mathrm{e}}_{\mathrm{an}} + \boldsymbol{\Lambda}^{\mathrm{e}}_{\sigma^2_{\mathbf{W}}}, \end{aligned} \tag{12}$$

where $\mathbf{R}^{\mathrm{e}}_{\mathrm{an}} = \mathbf{F}\boldsymbol{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{e}}\mathbf{R}_{\mathbf{aa}}\mathbf{H}^{\mathrm{e}\dagger}\boldsymbol{\Psi}^{\dagger}_{\mathrm{R}}\mathbf{F}^{\dagger}$ is the autocorrelation matrix of the noise portion associated with the AN at Eve. Finally, Eve's SNR in the discrete-frequency domain can be obtained from the following diagonal matrix:

$$\boldsymbol{\Lambda}^{\mathrm{e}}_{\gamma} = \frac{\boldsymbol{\Lambda}_{\sigma^2_{\mathbf{x}}}\boldsymbol{\Lambda}^{\mathrm{e}}_{|\mathbf{H}|^2}}{\boldsymbol{\Lambda}^{\mathrm{e}}_{\sigma^2_{\mathrm{an}}} + \boldsymbol{\Lambda}^{\mathrm{e}}_{\sigma^2_{\mathbf{W}}}}, \tag{13}$$

in which $\boldsymbol{\Lambda}^{\mathrm{e}}_{\sigma^2_{\mathrm{an}}} = \mathrm{diag}\{\mathbf{R}^{\mathrm{e}}_{\mathrm{an}}\}$.

Comparing (10) with (13), the extra noise term of the AN implies an additional term in the denominator of Eve's SNR. In the next section, we numerically evaluate the impact of this extra noise term on the performance of Bob and Eve (PLC and hybrid) in two distinct configurations (i.e., Eve close to Alice and Eve close to Bob).

IV. Numerical Analysis

In this section, we evaluate the performance of the AN injection to increase the security of in-home PLC networks that face a potential threat from PLC or wireless eavesdroppers. The CIRs of the Alice-Bob link and the Alive-Eve link (when Eve is a PLC node) are obtained from the measurement campaign in [11]. The CIR of the Alive-Eve link (when Eve is a wireless node) derive from the measurement campaign of hybrid PLC-WLC channels reported in [2]. Two scenarios are addressed for each type of eavesdropper: one for Eve near Alice, namely short-path (SP), and another for Eve near Bob, namely long-path (LP).

The analysis considers bit error rate (BER) values of Bob and Eve as a function of total transmission power (P_{T}). To do so, Monte Carlo simulations with the transmission of 2^{17} bits modulated in 4-order quadrature amplitude modulation (4-QAM) are carried out. In this regard, an OFDM scheme with $N = 4096$ and $N_{\mathrm{cp}} = 512$ samples is treated. The numerical approach for the total transmission power P_{T} is such that $P_{\mathbf{x}} = (1-\alpha)P_{\mathrm{T}}$ and $P_{\mathbf{a}} = \alpha P_{\mathrm{T}}$, with $\alpha \in [0, 1]$. We assume uniform power allocation, thus $\boldsymbol{\Lambda}_{\sigma^2_{\mathbf{x}}} = \mathbf{I}_N P_{\mathbf{x}}/N$ and $\boldsymbol{\Lambda}_{\sigma^2_{\mathbf{a}}} = \mathbf{I}_N P_{\mathbf{a}}/(N + N_{\mathrm{cp}})$. Additionally, PLC nodes experience additive colored Gaussian noise with a spectral density equal to $1/f$, while wireless nodes experience additive white gaussian noise (AWGN). To be fair, $P_{\mathrm{w}} = 10^{-8}$ [12] is assumed for all nodes.

Figs. 2 and 3 show the BER of Bob and Eve (PLC), considering different values of α. First, Fig. 2 considers Eve near Alice, i.e., SP. For $\alpha = 0$ (no AN injection), Eve's BER is naturally lower than Bob's. However, as the AN power increases, Bob's BER slightly increases since the total available power has to be divided into signal and AN. On the other hand, the AN severely impacts Eve's BER so that it is higher than Bob's for $P_{\mathrm{T}} > 6$ dBm if $\alpha = 0.3$ and for $P_{\mathrm{T}} \geq -10$ dBm if $\alpha = 0.9$. Meanwhile, Fig. 3 shows the results for Eve close to Bob, i.e., LP. In this scenario, Bob's BER is lower than Eve's if $\alpha = 0$, i.e., Bob's channel is inherently better than Eve's. As α increases, the BER values of Bob and Eve also increase, with a more noticeable deterioration for Eve. Nonetheless, the impact of the AN is less expressive for Eve close to Bob.

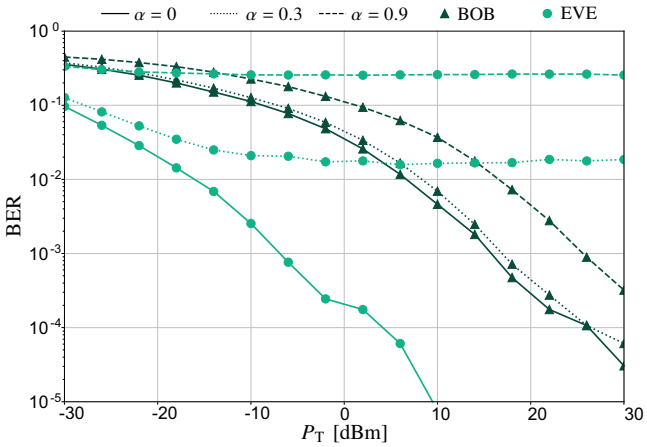

Fig. 2: BER vs P_{T} for Eve (PLC) and Bob under distinct α values for SP scenario.

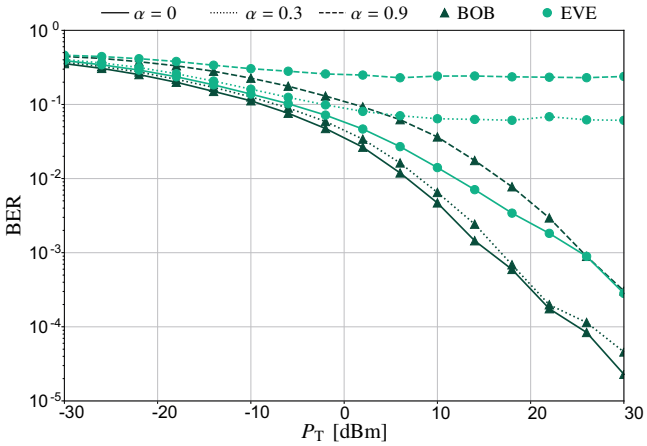

Fig. 3: BER vs P_{T} for Eve (PLC) and Bob under distinct α values for LP scenario.

In Figs. 4 and 5, we examine the effect of a wireless eavesdropper on the PLC network. Therefore, the Alice-Bob link is kept while the Alice-Eve link changes to the hybrid PLC-WLC channel. Fig. 4 shows the results for the SP scenario. Note that in the absence of AN ($\alpha = 0$), Eve's BER is slightly lower than Bob's for $P_{\mathrm{T}} < 10$ dBm. However, Bob's BER becomes smaller than Eve's for $P_{\mathrm{T}} > 2$ dBm if $\alpha = 0.3$

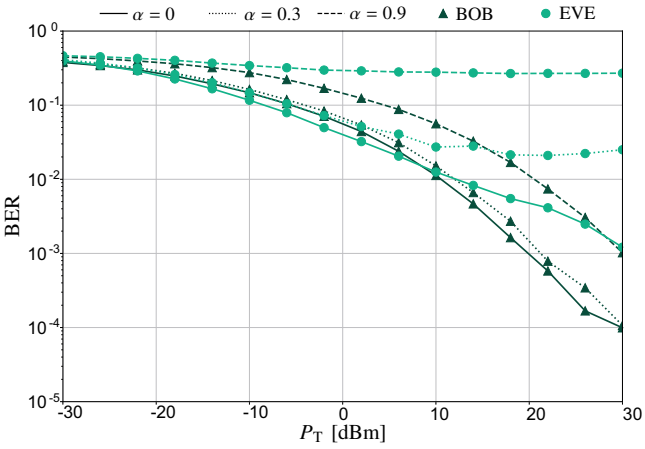

Fig. 4: BER vs P_T for Eve (wireless) and Bob under distinct α values for SP scenario.

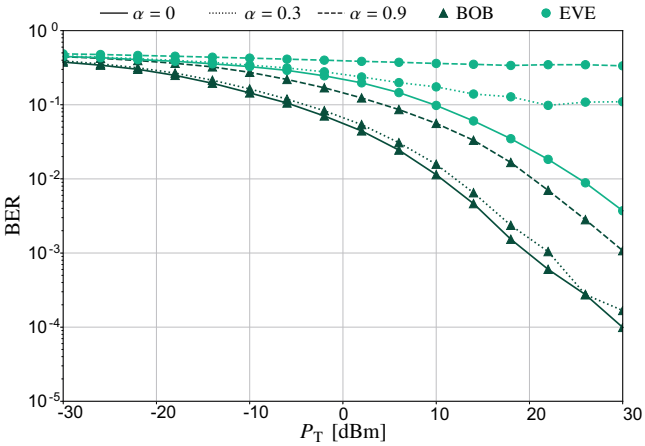

Fig. 5: BER vs P_T for Eve (wireless) and Bob under distinct α values for LP scenario.

and for any value of P_T if $\alpha = 0.9$. Changing the analyses to the LP scenario, displayed in Fig. 5, note that Eve's BER is higher than Bob's for all simulated values of α, i.e, Eve's BER is worst than Bob's regardless of the amount of power allocated to the AN. Therefore, when Eve (wireless) is closer to Alice there is a drop in the system's security, but the system security is enhanced as the eavesdropper moves away from the transmitter.

Overall, the obtained results show that PLC eavesdroppers are more dangerous to the security of an in-home PLC network than wireless ones, which is due to both the correlation of PLC channels for near nodes and the lowest channel attenuation associated with PLC eavesdropper. When the PLC network is in the presence of a wireless eavesdropper, the AN is less efficient because of the channel attenuation related to the eavesdroppers. Moreover, the AN is most advantageous for a PLC eavesdropper in the SP scenario. Therefore, the analyzed technique is quite useful in the most threatening scenario for the PLS of the PLC network—see Fig. 2 for $\alpha = 0$.

V. Conclusions

From a perspective of information security, this paper has investigated the effects of introducing an artificial noise, designed based on the degrees of freedom of the CP, to in-home PLC systems in the presence of PLC and wireless eavesdroppers. The numerical analysis, in terms of BER, indicates that the artificial noise can degrade the performance of a passive eavesdropper located in proximity to the legitimate transmitter, leading to an elevated BER for the eavesdropper. However, when the eavesdropper is closer to the legitimate receiver (thus relatively far from the legitimate transmitter), the effectiveness of the artificial noise diminishes, causing only a minor increase in the eavesdropper's BER. Also, a comparison among the considered eavesdroppers shows that the PLC eavesdropper is potentially a more significant threat to the in-home PLC network. Furthermore, when a PLC eavesdropper is near the legitimate transmitter, the eavesdropper naturally achieves a low value of BER (no artificial noise injection). Fortunately, this is the scenario where artificial noise injection is more effective. As future work, we mention a statistical analysis of the artificial noise injection technique, considering more data and other noise types, as well as the investigation of other techniques.

References

[1] L. de M. B. A. Dib, V. Fernandes, M. de L. Filomeno, and M. V. Ribeiro, "Hybrid PLC/wireless communication for smart grids and internet of things applications," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 655–667, 2018.

[2] T. R. Oliveira, F. J. A. Andrade, A. M. Picorone, H. A. Latchman, S. L. Netto, and M. V. Ribeiro, "Characterization of hybrid communication channel in indoor scenario," *J. Commun. Inf. Syst.*, vol. 31, no. 1, pp. 224–235, Sept. 2016.

[3] A. Pittolo and A. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Commun.*, vol. 8, pp. 1239–1247, May 2014.

[4] Â. Camponogara, H. V. Poor, and M. V. Ribeiro, "Physical layer security of in-home PLC systems: Analysis based on a measurement campaign," *IEEE Syst. J.*, vol. 15, no. 1, pp. 617–628, Mar. 2021.

[5] V. Mohan, A. Mathur, V. Aishwarya, and S. Bhargav, "Secrecy analysis of PLC system with channel gain and impulsive noise," in *Proc. IEEE Veh. Technol. Conf.*, 2019, pp. 1–6.

[6] A. Salem, K. A. Hamdi, and E. Alsusa, "Physical layer security over correlated log-normal cooperative power line communication channels," *IEEE Access*, vol. 5, pp. 13 909–13 921, 2017.

[7] Â. Camponogara, H. V. Poor, and M. V. Ribeiro, "PLC systems under the presence of a malicious wireless communication device: Physical layer security analyses," *IEEE Syst. J.*, vol. 14, no. 4, pp. 4901–4910, Dec. 2020.

[8] Â. Camponogara and M. V. Ribeiro, "The effective secrecy throughput for the hybrid wiretap channel," *J. Commun. Inf. Syst.*, vol. 36, no. 1, pp. 44–51, Feb. 2021.

[9] Â. Camponogara, R. D. Souza, and M. V. Ribeiro, "The effective secrecy throughput of a broadband power line communication system under the presence of colluding wireless eavesdroppers," *IEEE Access*, vol. 10, pp. 85 019–85 029, 2022.

[10] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 6, pp. 2717–2729, June 2013.

[11] M. S. P. Facina, H. A. Latchman, H. V. Poor, and M. V. Ribeiro, "Cooperative in-home power line communication: Analyses based on a measurement campaign," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 778–789, Feb. 2016.

[12] G. Prasad, L. Lampe, and S. Shekhar, "In-band full duplex broadband power line communications," *IEEE Trans. Commun.*, vol. 64, no. 9, pp. 3915–3931, Sept. 2016.