Assessment of an Artificial Noise Scheme in PLC Systems under the Presence of a Passive WLC Eavesdropper

Pedro H. Sartorello, Gustavo M. Campos, Mateus de L. Filomeno, Moisés V. Ribeiro, and Ândrei Camponogara

Abstract— **This study investigates the information security in a discrete multitone-based power line communication (PLC) system when a wireless communication eavesdropper tries to obtain private information, and the PLC transmitter combats it with an artificial noise scheme designed to degrade the eavesdropper's signal-to-noise ratio only. The numerical results showed that the artificial noise significantly degrades the eavesdropper's bit error rate (BER) compared to the legitimate receiver's BER.**

Keywords— **Artificial noise, physical layer security, power line communication**

I. Introduction

Power line communication (PLC) has become a well-established technology with various applications in outdoor (medium- and low-voltage) and indoor (homes and commercial buildings) electric power grids [1]. Nonetheless, as PLC is inherently broadcast, information security is a big concern since any malicious PLC device connected to the electric power grid, in which the PLC system operates, could access private information. Moreover, most electric power grids are composed of unshielded power lines, and consequently, information-carrying signals traveling over them radiate electromagnetic fields that are sensed by a malicious wireless communication (WLC) device close enough to the electric power grid [2]. Aiming to circumvent this problem, the physical layer security (PLS) has been investigated as an alternative to increasing security and privacy.

Camponogara *et al.* [2] investigated the PLS in terms of secrecy outage probability in a PLC system when a legitimate PLC transmitter sends private information to a legitimate PLC receiver while a passive WLC eavesdropper overhears it. Next, considering this scenario, the authors in [3] presented the wiretap code rates required to maximize the effective secrecy throughput. In [4], the authors proposed an artificial noise scheme to increase the PLS in visible light communication (VLC) wiretap systems by degrading the signal-to-noise ratio (SNR) of a malicious VLC device. The main idea is to use the degree of freedom added to the channel convolution matrix by the cyclic prefix in an orthogonal frequency-division multiplexing (OFDM)-based VLC system to generate the artificial noise.

Considering the scenario addressed in [2], this study aims at assessing the bit error rates (BERs) at the legitimate PLC receiver, and the PLC eavesdropper when the artificial noise detailed in [4] is used by the PLC transmitter. To do so, channel estimates obtained in the measurement campaign addressed in [1] are considered to perform numerical simulations.

II. System Model

Let us evaluate information security in a discrete multitone modulation (DMT)-based PLC system where a PLC transmitter (Alice) sends private information to a legitimate PLC receiver (Bob) in the presence of a passive WLC eavesdropper (Eve). To prevent Eve from decoding the private messages, Alice designs and transmits an artificial noise spanned in the null space of Bob's channel along with the communication signal. In this way, the vector representation of the received signals at the output of Bob and Eve's channels can be expressed as

$$\mathbf{y}_l = \boldsymbol{\mathcal{H}}_l(\mathbf{T}_{\mathrm{CP}}\mathbf{x} + \mathbf{a}) + \mathbf{v}_l \tag{1}$$

in which $\mathbf{x} \in \mathbb{R}^{N\times 1}$ is a DMT block symbol transmitted by Alice to Bob, with $\mathbf{x} = \mathbf{F}^{\dagger}\mathbf{X}$, $\mathbf{F}$ denotes the normalized N-size discrete Fourier transform (DFT) matrix, $\mathbf{X} \in \mathbb{C}^{N\times 1}$ being the DMT symbol block in the frequency domain obeying the Hermitian symmetric property, and $(\cdot)^{\dagger}$ denoting the Hermitian transpose operator. Also, $E\{\mathbf{X}\} = 0$ and $E\{\mathbf{X}\mathbf{X}^{\dagger}\} = \sigma_X^2\mathbf{I}_N$, where $\mathbf{I}_a$ is the $(a \times a)$-size identity matrix. The power used to transmit private messages is $P_X = \mathrm{Tr}(\sigma_X^2\mathbf{I}_N)/N$, with $\mathrm{Tr}(\cdot)$ denoting the trace operator. Moreover, $\mathbf{T}_{\mathrm{CP}} = [\mathbf{E}_{(N+N_{\mathrm{CP}})\times N_{\mathrm{CP}}}\ \mathbf{I}_N]^T$ and $\mathbf{E}_{(N+N_{\mathrm{CP}})\times N_{\mathrm{CP}}} = [\mathbf{0}_{N_{\mathrm{CP}}\times(N-N_{\mathrm{CP}})}\ \mathbf{I}_{N_{\mathrm{CP}}}]^T$ is responsible for appending the cyclic prefix with length N_{CP} at the beginning of $\mathbf{x}$. Also, $\mathbf{a} \in \mathbb{R}^{(N+N_{\mathrm{CP}})\times 1}$ denotes the artificial noise and $\mathbf{v}_l \sim \mathcal{N}(0,\ \sigma_l^2\mathbf{I}_{N+N_{\mathrm{CP}}})$ represents the additive noise. Notice that both noises are assumed to be independent of $\mathbf{x}$ and each other. Furthermore, $\boldsymbol{\mathcal{H}}_l$ is a Toeplitz matrix [4] associated with the channel impulse response $\mathbf{h}_l \in \mathbb{R}^{L_h\times 1}$, which is obtained from the link between Alice and the l^{th} receiver with $l \in \{B, E\}$ and B and E representing respectively Bob and Eve. Additionally, one assumes that the time-interval duration of $\mathbf{x}$

Pedro H. Sartorello e Ândrei Camponogara, Department of Electrical Engineering, Federal University of Paraná, Curitiba-PR, e-mail: {pedro.sartorello, andrei.camponogara}@ufpr.br

Gustavo M. Campos, Mateus de L. Filomeno, and Moisés V. Ribeiro; Federal University of Juiz de Fora (UFJF); e-mail addresses: {gustavo.moraes, mateus.lima, mribeiro}@engenharia.ufjf.br.

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, TEC-PPM 00787-18, and APQ-04623-22, and Instituto Nacional de Energia Elétrica (INERGE).

is shorter than the coherence time of $\mathbf{h}_l$, which is considered time-invariant during one block symbol interval.

The received signal in the frequency domain at the input of Bob and Eve can respectively be expressed as

$$\mathbf{Y}_{\mathrm{B}} = \mathbf{F}\mathbf{R}_{\mathrm{CP}}\boldsymbol{\mathcal{H}}_{\mathrm{B}}\mathbf{T}_{\mathrm{CP}}\mathbf{F}^{\dagger}\mathbf{X} + \mathbf{F}\mathbf{R}_{\mathrm{CP}}\mathbf{v}_{\mathrm{B}} \tag{2}$$

and

$$\mathbf{Y}_{\mathrm{E}} = \mathbf{F}\mathbf{R}_{\mathrm{CP}}\boldsymbol{\mathcal{H}}_{\mathrm{E}}\mathbf{T}_{\mathrm{CP}}\mathbf{F}^{\dagger}\mathbf{X} + \mathbf{F}\mathbf{R}_{\mathrm{CP}}\boldsymbol{\mathcal{H}}_{\mathrm{E}}\mathbf{a} + \mathbf{F}\mathbf{R}_{\mathrm{CP}}\mathbf{v}_{\mathrm{E}}, \tag{3}$$

where $\mathbf{R}_{\mathrm{CP}} = [\mathbf{0}_{N\times N_{\mathrm{CP}}}\ \mathbf{I}_N]$ is responsible for removing the cyclic prefix. Note that differently from Bob, the received symbols at Eve are degraded by $\mathbf{F}\mathbf{R}_{\mathrm{CP}}\boldsymbol{\mathcal{H}}_{\mathrm{E}}\mathbf{a}$ due to the artificial noise. In the next sections, it is described the design of $\mathbf{a}$ and its impact is analyzed in terms of BER.

III. The Artificial Noise Design

The artificial noise $\mathbf{a} \in \mathbb{R}^{(N+N_{\mathrm{CP}})\times 1}$ is responsible for degrading Eve's SNR and can be designed as [4]

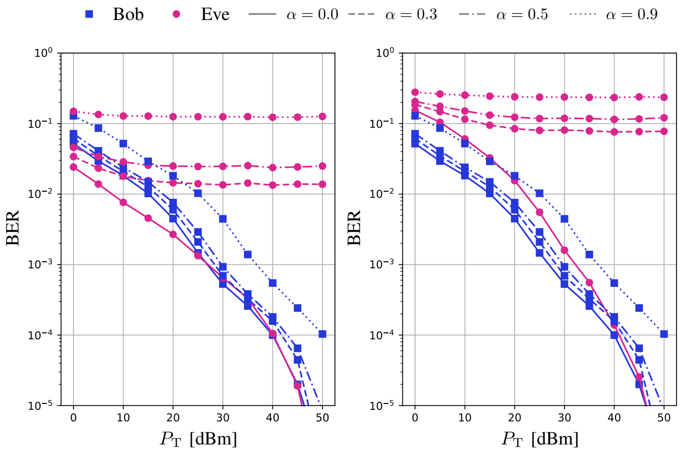
$$\mathbf{a} = \boldsymbol{\mathcal{G}}\mathbf{a}',$$

where $\mathbf{a}' \sim \mathcal{N}(0, \sigma_a^2\mathbf{I}_{N_{\mathrm{CP}}})$ and $\boldsymbol{\mathcal{G}} \in \mathbb{R}^{(N+N_{\mathrm{CP}})\times N_{\mathrm{CP}}}$ is the artificial noise precoding matrix that projects $\mathbf{a}'$ in the null space of the matrix $\mathbf{R}_{\mathrm{CP}}\boldsymbol{\mathcal{H}}_{\mathrm{B}}$, and can be expressed as $\boldsymbol{\mathcal{G}} = \boldsymbol{\mathcal{H}}_{\mathrm{B}}^{-1}[\mathbf{I}_{N_{\mathrm{CP}}}\ \mathbf{0}_{N_{\mathrm{CP}}\times 2N}]^T$. Note that the total transmission power available at Alice is P_{T}. To degrade Eve's SNR in respect to Bob, Alice uses $P_a = \alpha P_{\mathrm{T}}$ to transmit the artificial noise along with the private messages where $0 \leq \alpha \leq 1$, while $P_X = (1-\alpha)P_{\mathrm{T}}$ is used to transmit the private messages to Bob.

IV. Numerical Results

This section analyzes the information security in a DMT-based PLC system when Alice combats Eve using an artificial noise scheme designed to compromise Eve's SNR only. Then, by means of Monte Carlo simulation, the BERs at Bob and Eve are evaluated. To do so, one assumes that Alice transmits 1000 DMT symbol blocks built with 4-quadrature amplitude modulation (QAM) symbols, $N = 2048$, and $N_{\mathrm{CP}} = 512$. Moreover, the Alice-Bob and Alice-Eve links are represented by the PLC and the hybrid PLC-WLC channel estimates (frequency band $1.7-100$ MHz) collected in the measurement campaign discussed in [1]. The noise is assumed to be additive white Gaussian noise (AWGN) with the power of 10^{-8} W. Lastly, two simulation scenarios are adopted: (i) Eve is situated less than 2 meters from Alice, named short-path (SP); and (ii) Eve is located between 2 and 6 meters from Alice, named long-path (LP).

Figs. 1(a) and (b) show the BER×P_{T} curves of Bob and Eve for $\alpha = 0,\ 0.3,\ 0.5$, and 0.9 considering respectively the SP and LP scenarios. Note that when there is no artificial noise, i.e., $\alpha = 0$, Eve's BER is lower than Bob's BER in the SP scenario, see Fig. 1(a). On the other hand, in the LP scenario, Eve's BER is higher than Bob's BER, see Fig. 1(b). Nonetheless, as α increases, Eve's BER is degraded significantly with respect to Bob's BER, showing a constant behavior as P_{T} increases. Note that the best results are found in the LP scenario. For instance, in Fig. 1(b), one sees that the minimum values found of Eve's BER are around 0.08, 0.12, and 0.26 for $\alpha = 0.3,\ 0.5$, and 0.9, respectively.



(a)

(b)

Fig. 1. BER×P_{T} for distinct distances between Eve and Alice and $\alpha = 0.0,\ 0.3,\ 0.5$, and 0.9. (a) Short-path scenario. (b) Long-path scenario.

V. Conclusion

This study has investigated information security in a DMT-based PLC system with a WLC eavesdropper (Eve). In this regard, Monte Carlo simulations assessed the BER at Bob (PLC receiver) and Eve when Alice uses an artificial noise scheme to degrade Eve's SNR. In particular, the additive noise uses additional degrees of freedom introduced by the cyclic prefix in Bob's channel. Moreover, to generate the numerical results, two scenarios have been considered: (i) Eve is close to Alice (SP), and (ii) Eve is situated far from Alice (LP). Additionally, real channel estimates obtained from a measurement campaign have been adopted.

The numerical results have shown that the artificial noise scheme increases Eve's BER significantly compared to Bob's BER, even in the worst scenario, i.e., the SP one. This outcome supports previous findings in the literature that highlight the artificial noise scheme's efficiency in compromising Eve's SNR. However, this advantage comes at a cost, as a portion of the total transmission power is allocated to the artificial noise, decreasing the system's data rate.

References

[1] 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," *Journal of Communication and Information Systems*, vol. 31, no. 1, pp. 224–235, Sep. 2016.

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

[3] A. Camponogara and M. Ribeiro, "The effective secrecy throughput for the hybrid wiretap channel," *Journal of Communication and Information Systems*, vol. 36, no. 1, pp. 44–51, Feb. 2021.

[4] F. Yang, K. Zhang, Y. Zhai, J. Quan, and Y. Dong, "Artificial noise design in time domain for indoor SISO DCO-OFDM VLC wiretap systems," *Journal of Lightwave Technology*, vol. 39, no. 20, pp. 6450–6458, Oct. 2021.