The Effective Secrecy Throughput for the Hybrid PLC/WLC Wiretap Channel: Analysis Based on a Measurement Campaign

Ândrei Camponogara and Moisés Vidal Ribeiro

***Abstract*—This study investigates the physical layer security (PLS) of an in-home and broadband power line communication (PLC) system under the presence of a hybrid PLC/wireless communication (WLC) eavesdropper. Also, we compare the security threats suffered by a in-home and broadband PLC system due to the presence of WLC, PLC, and hybrid PLC/WLC eavesdroppers. In this regard, we evaluate the effective secrecy throughput and corresponding wiretap code rates by using a real data set composed of channel estimates and measured additive noises. Considering all investigated scenarios, numerical results show that a hybrid PLC/WLC eavesdropper represents the main security threat to in-home and broadband PLC systems because it combines private information simultaneously eavesdropped from the power line and the air, which constitutes a remarkable advantage in comparison to the sole use of PLC or WLC eavesdropper.**

***Index Terms*—Physical layer security, power line communication, wireless communication, effective secrecy throughput, passive eavesdropping.**

I. Introduction

RECENTLY, power line communications (PLC) technologies have been extensively studied because of the existing channel resources in indoor (e.g., houses and commercial buildings), outdoor (low- and medium-voltages), and in-vehicle (e.g., cars, ships, trains, spacecraft, and aircraft) electric power grids [1]–[7], which can be useful for emerging applications such as internet of things (IoT) and industry 4.0. However, electric power systems were not conceived to transmit information-carrying signals (PLC signals) and several contributions have pointed out that these systems constitute harsh communication media [8]–[13]. Essentially, PLC signals may suffer attenuation related to node-to-node distance and frequencies increase and coupling losses at the connection points between PLC modems and power cables. Also, the intersymbol interference caused by impedance mismatching between power cables and loads degrades those signals while the high-power impulsive noises generated by the dynamics of electric loads and the interference from wireless communications (WLC) systems[1], which operates in the same frequency range, introduces additional degradation to the PLC signals. Despite all the drawbacks mentioned above, researches on PLC technologies have advanced. Nowadays, there are worldwide standards and several private protocols in the market [14].

The broadcast nature of electric power systems and the widespread use of electromagnetically unshielded power cables in these systems raise the attention to the security of carrying-data signal transmitted by PLC technologies. A malicious PLC or WLC device located nearby a PLC system can eavesdrop on private messages transmitted through this system [15], [16], and the parallel combination of these devices, which gives rise to the hybrid PLC/WLC device, constitute a powerful source of security breach. In this sense, a few studies have investigated physical layer security (PLS) [17] in PLC systems when the transmitter knows the complete channel state information (CSI) of a malicious device [15], [18]–[21] or not [16], [22]–[25].

In [15], the authors analyzed the achievable secrecy rate related to in-home and broadband PLC systems under the presence of a malicious PLC device when a data set constituted of PLC channel measures was taken into account. Also, [18] investigated the achievable secrecy rate for a multiple-input multiple-output (MIMO) broadband PLC system considering distinct distances between a PLC transmitter and a PLC receiver while [20] discussed PLS of a MIMO broadband PLC system when a legitimate PLC receiver uses jamming signals for degrading the signal-to-noise ratio (SNR) of a PLC eavesdropper. Moreover, [21] analyzed the ergodic achievable rate and secrecy outage probability metrics for low-bit-rate hybrid PLC/WLC wiretap channels and their incomplete versions.

Furthermore, [19] focused on an artificial noise scheme to improve the average secrecy capacity in cooperative relaying PLC systems when quasi-static and flat log-normal fading channels represent PLC channels. Soon after, [22] assessed the average secrecy capacity and the secrecy outage probability for PLC and hybrid PLC/WLC single relay channels using the same channel model. [23] considered an artificial noise scheme to improve the PLS of a hybrid PLC/WLC system in the presence of a WLC or a PLC eavesdropper. Next, the achievable secrecy rate, secrecy outage probability, and strictly positive secrecy capacity metrics were evaluated for a broadband PLC system impaired by impulsive noise [24]. Furthermore, [16] introduced the hybrid wiretap channel model to evaluate the ergodic achievable secrecy rate and the secrecy outage probability of an in-home and broadband PLC

The authors would like to thank CAPES (Finance Code 001), CNPq, INERGE, and FAPEMIG for their financial support.

Ândrei Camponogara and Moisés V. Ribeiro are with the Department of Electrical Engineering, Federal University of Juiz de Fora, Juiz de Fora, MG, Brazil (e-mails: andrei.camponogara@engenharia.ufjf.br and mribeiro@engenharia.ufjf.br).

Digital Object Identifier: 10.14209/jcis.2021.4

[1] This interference is due to the use of electromagnetically unshielded power cables in electric power systems.

system threatened by the presence of a malicious WLC device. Lastly, [25] assessed the PLS in terms of ergodic achievable secrecy rate, secrecy outage probability, and effective secrecy throughput of an in-home and broadband PLC system under the presence of a malicious PLC device located in distinct positions relative to the PLC transmitter and the PLC receiver. The authors also provided the wiretap code rates for achieving the optimal effective secrecy throughput.

Aiming to offer complementary and useful insights about the PLS of an in-home and broadband PLC system and relying on the findings reported in [26], [27], this study analyzes the effective secrecy throughput and its respective wiretap code rates when a PLC system is threatened by a passive hybrid PLC/WLC eavesdropper. This type of eavesdropper is the most powerful because it can overhear private information simultaneously through the PLC and hybrid PLC-WLC channels[2]. Giving a practical perspective for this investigation, the frequency band $1.7-86$ MHz (in agreement with the ITU-T Rec. G.9964) and a data set composed of channel frequency response (CFR) estimates and measured additive noises are taken into account.

Numerical results about effective secrecy throughput and its respective wiretap code rates based on the use of PLC and hybrid PLC-WLC channel estimates and measured additive noises are reported. To do so, we consider two distinct sets of relative positions of transmitter, receiver and eavesdropper; distinct levels of the total transmission power, which cover practical (i.e., $[0, 30]$ dBm); a comparison with the cases in which the passive eavesdropper is a WLC device and a PLC device [16], [25], which constitute the two reduced version of a hybrid PLC-WLC eavesdropper. The attained results show that a hybrid PLC/WLC eavesdropper can produce the most dangerous security attack at the physical layer level of in-home and broadband PLC systems. A remarkable result is that, when the hybrid PLC/WLC eavesdropper is near the PLC transmitter, the values of effective secrecy throughput are equal to zero when the total transmission power is higher than -10 dBm.

The rest of this paper is organized as follows: Section II details the problem formulation; Section III deduces the mathematical expression for evaluating the effective secrecy throughput; Section IV shows the numerical results; and, finally, Section V draws some concluding remarks.

Notation: Lower-case and upper-case boldface symbols denote vectors in the discrete-time and -frequency domains, respectively. $\mathcal{F}$ is the N-size and normalized discrete-time Fourier transform (DFT) matrix. $\mathbf{0}_{N\times 1}$ is the N-length column vector of zeros. $\mathbf{I}_N$ is the $N \times N$ identity matrix. $\det(\mathbf{\Lambda}_D)$ denotes the determinant of the matrix $\mathbf{\Lambda}_D$. $h(\cdot)$ refers to the entropy function. $|\cdot|$ denotes the modulus operator. $\mathbb{E}[\cdot]$ is the expectation operator. $\{\cdot\}^T$ denotes the transpose operator. $\{\cdot\}^\dagger$ is the Hermitian operator. $\mathrm{tr}(\cdot)$ is the trace operator. $\mathbb{P}\{c < d\}$ means the probability that c is less than d. $\max[b]^+ = \max(0, b)$.

II. Problem Formulation

In the classical wiretap channel, an eavesdropper (Eve) tries to overhear private information exchanged between a transmitter (Alice) and a legitimate receiver (Bob). Following the PLS approach, the secrecy capacity (C_S) is a natural parameter to quantify secrecy at the physical layer level. If complete CSIs of Bob and Eve are available to Alice, then perfect secrecy can be attained since Alice knows the channel capacities related to Bob (C_B) and Eve (C_E) [28], [29]. From the perspective of wiretap code design, the following requirements have to be addressed for achieving perfect secrecy:

- *Reliability constraint*: The error probability of Bob must decrease as the code length increases.
- *Secrecy constraint*: The equivocation rate of Eve must increase as the wiretap code length increases.

Also, a wiretap code consists of the following rates:

- Rate of transmitted codewords, $R_B \in \mathbb{R}_+$;
- Target secrecy rate, $R \in \mathbb{R}_+$.

Based on these information, let us assume that $R_E = R_B - R$ is the redundancy rate used to confuse Eve. To fulfill both reliability and secrecy constraints, $R_B \leq C_B$ and $R_E > C_E$ must be satisfied [26], [27]. The maximum R, i.e., $C_S = C_B - C_E$, can be reached since C_B and C_E are known.

In a practical scenario, Eve is a passive device; i.e., she does not transmit any information to Alice. Consequently, Eve's CSI knowledge is unavailable to Alice and then $R_E > C_E$ may not be fulfilled. In this sense, the secrecy outage probability $P_S(R) = \mathbb{P}(C_S > R)$ is an useful parameter to measure secrecy at the physical layer level; however, $P_S(R)$ does not separate reliability and secrecy requirements. To deal with this problem, [26], [27] introduced a novel framework to estimate R_B and R_E based on the effective secrecy throughput.

To exploit the use of the effective secrecy throughput in PLC systems threatened by a hybrid PLC/WLC eavesdropper, Fig. 1 shows the block diagram of the hybrid PLC/WLC wiretap channel model. This channel model represents the scenario where a PLC transmitter, Alice (A), sends private messages to an intended PLC receiver, Bob (B), while a malicious hybrid PLC/WLC device, Eve (E), simultaneously eavesdrops on the private messages through both power line and wireless media. Note that Eve is capable of overhearing private messages through a physical connection to the electric power circuit and, at the same time, sensing the electromagnetic field radiated by the PLC signal, which carries private messages, traveling over electromagnetically unshielded power lines. In this regard, Fig. 2 shows an illustration of a scenario in which Eve is a hybrid PLC/WLC device designed to eavesdrop on private messages sent by Alice to Bob. In general, Eve must be located nearby the electric power circuit, in which the PLC system operates, because [30] reported that a distance of up to 6 m from the power cable allows Eve to wirelessly overhear the private messages.

Regarding the hybrid PLC/WLC wiretap channel model, the Alice-Eve link, which is defined between the PLC and WLC

[2] The hybrid PLC-WLC channel refers to the data communication medium between a PLC device and a WLC device operating in the same frequency band. In this case, a WLC receiver is near an electric power grid, in which a PLC system operates, and, as a consequence, can sense the electromagnetic field radiated by a PLC signal traveling over electromagnetically unshielded power cables.

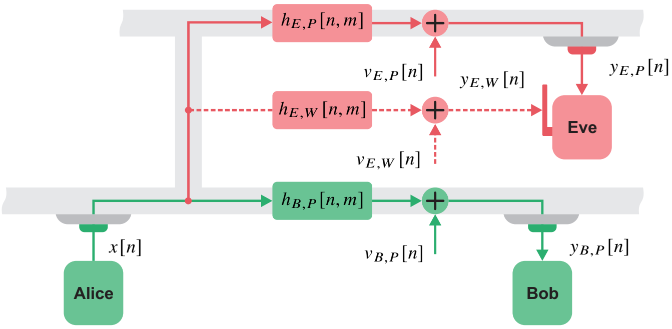


Fig. 1: Block diagram of the hybrid PLC/WLC wiretap channel model. The dashed line denotes the hybrid PLC-WLC channel while the continuous lines represent the PLC channel.

devices, is well-modeled by so-called in-home and broadband hybrid PLC-WLC channels [30]. In addition, the Alice-Bob and Alice-Eve links, which are defined over electric power circuits, are well-modeled by in-home and broadband PLC channels [2].

Based on these considerations, we assume that $\{h_{l,q}[n,m]\}$ denotes the discrete-time version of the time-varying channels associated with the link between Alice and the l^{th} receiver in the q^{th} data communication medium, where $l \in \{B, E\}$ denotes Bob and Eve, respectively, while $q \in \{P, W\}$ represents the power lines and wireless media, respectively. Then the discrete-time representation of the received signal at the l^{th} receiver through the q^{th} medium can be expressed as

$$y_{l,q}[n] = \sum_{m=-\infty}^{\infty} x[m] h_{l,q}[n,m] + v_{l,q}[n], \tag{1}$$

where $\{x[n]\}$ is the transmitted sequence that is constituted by an infinite number of N-length symbols (N-block symbols); $h_{l,q}[n,m]$ is the linear and time-varying channel impulse response (CIR); $\{v_{l,q}[n]\}$ denotes the additive noise sequence; and $\{x[n]\}$ and $\{v_{l,q}[n]\}$ are independent and wide-sense stationary random processes.

The PLC and hybrid PLC-WLC channels are considered to be linear and time-invariant during a time interval corresponding to an N-block symbol. In this way, the discrete-time CIR is denoted by $\{\mathrm{h}_{l,q}[n]\}_{n=0}^{L_{l,q}-1}$, in which $L_{l,q}$ denotes the length of CIR associated with the link between Alice and the l^{th} receiver and the q^{th} medium. The vector representation of the discrete-time version of such channels during one N-block symbol is $\mathbf{h}_{l,q} = [\mathrm{h}_{l,q}[0], \mathrm{h}_{l,q}[1], \ldots, \mathrm{h}_{l,q}[L_{l,q}-1]]^T$ whereas $\mathbf{H}_{l,q} = [H_{l,q}[0], H_{l,q}[1], \ldots, H_{l,q}[N-1]]^T$ denotes its vector representation in the frequency domain, where

$$\mathbf{H}_{l,q} = \mathcal{F} \begin{bmatrix} \mathbf{h}_{l,q} \\ \mathbf{0}_{N-L_{l,q}} \end{bmatrix} \tag{2}$$

and N denotes the number of sub-channels. Hereafter the diagonal matrices $\mathbf{\Lambda}_{\mathcal{H}_{l,q}} = \mathrm{diag}\left\{H_{l,q}[0], H_{l,q}[1], \ldots, H_{l,q}[N-1]\right\}$ and $\mathbf{\Lambda}_{|\mathcal{H}_{l,q}|^2} = \mathrm{diag}\{|H_{l,q}[0]|^2, |H_{l,q}[1]|^2, \cdots, |H_{l,q}[N-1]|^2\}$ will be used.

Moreover, the vectorial representation of the N-block symbol, in the frequency domain, is $\mathbf{X} \in \mathbb{C}^{N\times 1}$ under the assumption that

$$\mathbb{E}\{\mathbf{X}\} = \mathbf{0}_{N\times 1} \quad \text{and} \quad \mathbb{E}\left\{\mathbf{X}\mathbf{X}^\dagger\right\} = N\mathbf{\Lambda}_P, \tag{3}$$

where $\mathbf{\Lambda}_P = \mathrm{diag}\{P[0], P[1], \ldots, P[N-1]\}$ is the matrix representation of the power allocated in the frequency domain and $\mathrm{tr}(\mathbf{\Lambda}_P) = P_T$ is the total transmission power. Furthermore, $\mathbf{V}_{l,q} \in \mathbb{C}^{N\times 1}$ is the vector representation of the additive noise, in the frequency domain, such that

$$\mathbb{E}\left\{\mathbf{V}_{l,q}\right\} = \mathbf{0}_{N\times 1} \quad \text{and} \quad \mathbb{E}\left\{\mathbf{V}_{l,q}\mathbf{V}_{l,q}^\dagger\right\} = N\mathbf{\Lambda}_{P_{V_{l,q}}}, \tag{4}$$

where $\mathbf{\Lambda}_{P_{V_{l,q}}} = \mathrm{diag}\left\{P_{V_{l,q}}[0], P_{V_{l,q}}[1], \ldots, P_{V_{l,q}}[N-1]\right\}$ and $P_{V_{l,q}}[k]$ is the additive noise power in the k^{th} sub-channel.

Based on the formulation above, the following two questions arise: *Can a broadband in-home PLC system securely transmit information under the presence of a malicious hybrid PLC/WLC device? How do wiretap code rates (R_B and R_E) behave when P_T changes?*

III. Effective Secrecy Throughput

Following [31], PLC and hybrid PLC-WLC channels are assumed to be N-block linear Gaussian channels with finite memory (i.e., $L_{\max} = \max L_{l,q}$). It is well-established that the inter-block interference caused by the memory of CIRs and the correlated noises make the assessment of the achievable data rate a harsh task to be accomplished [32]. To overcome such a problem, [32] showed that the N-block circular Gaussian relay channel (CGRC) completely remove the inter-block interference if $N \gg L_{\max}$; therefore, as linear Gaussian relay channel (LGRC) tends to N-CGRC as $N \rightarrow \infty$, N-CGRC channels model PLC and hybrid PLC-WLC ones since $N \rightarrow \infty$.

The received N-block symbol at the l^{th} receiver through the q^{th} medium can be expressed as

$$\mathbf{Y}_{l,q} = \mathbf{\Lambda}_{\mathcal{H}_{l,q}}\mathbf{X} + \mathbf{V}_{l,q}. \tag{5}$$

Then the respective SNR is given by

$$\begin{aligned} \mathbf{\Lambda}_{\gamma_{l,q}} &= \frac{\mathbf{\Lambda}_{\mathcal{H}_{l,q}}\mathbb{E}[\mathbf{X}\mathbf{X}^\dagger]\mathbf{\Lambda}_{\mathcal{H}_{l,q}}^\dagger}{\mathbb{E}\left\{\mathbf{V}_{l,q}\mathbf{V}_{l,q}^\dagger\right\}} \\ &= \mathbf{\Lambda}_P\mathbf{\Lambda}_{|\mathcal{H}_{l,q}|^2}\mathbf{\Lambda}_{P_{V_{l,q}}}^{-1}. \end{aligned} \tag{6}$$

Consequently, the channel capacity between Alice and Bob can be expressed as

$$C_B = \max_{\mathbf{\Lambda}_P} \frac{1}{N}\log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}\right)\right] \quad [\text{bps/Hz}], \tag{7}$$

subjected to $\mathbf{tr}(\mathbf{\Lambda}_P) \leq P_T$, and the capacity between Alice and Eve can be written as

$$C_E = \frac{1}{N}\log_2\left[\det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_{E,P}} + \mathbf{\Lambda}_{\gamma_{E,W}}\right)\right] \quad [\text{bps/Hz}], \tag{8}$$

since we assumed that Eve makes use of the maximal-ratio combining (MRC) technique. Note that the $\mathbf{\Lambda}_P$ values used in C_E are the ones used for maximizing C_B.

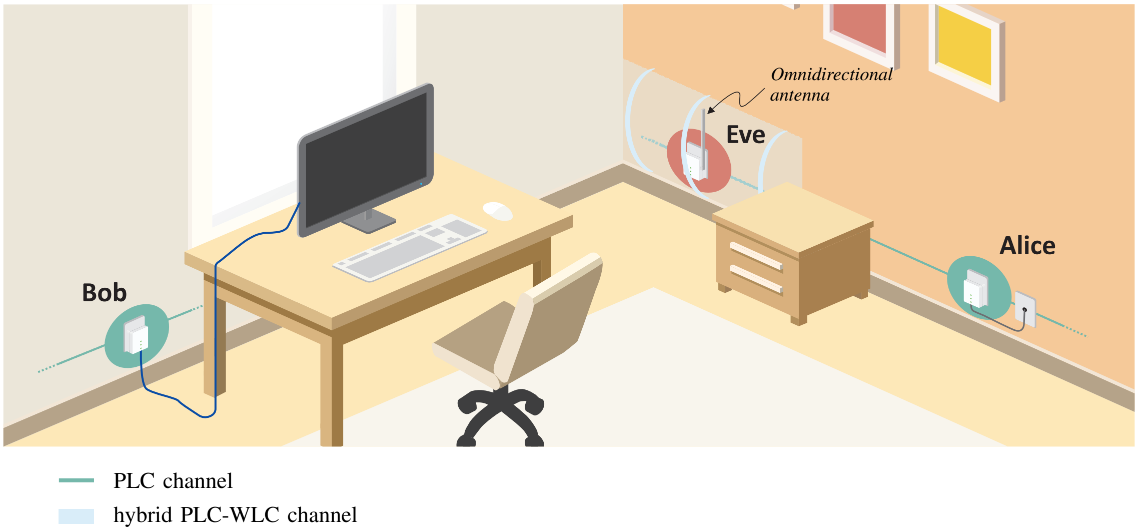


Fig. 2: Illustration of broadband data communication between two PLC devices (Alice and Bob) under the presence of a hybrid PLC/WLC eavesdropper (Eve).

Following [27], the secrecy outage probability can be expressed as

$$\begin{aligned} O_s(R_E) &= \mathbb{P}\left\{R_E < C_E\right\} \\ &= \mathbb{P}\left\{2^{R_E N} < \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_{E,P}} + \mathbf{\Lambda}_{\gamma_{E,W}}\right)\right\}, \end{aligned} \tag{9}$$

whereas the reliability outage probability is given by

$$\begin{aligned} O_r(R_B) &= \mathbb{P}\left\{R_B > C_B\right\} \\ &= \mathbb{P}\left\{2^{R_B N} > \det\left(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_B}\right)\right\}. \end{aligned} \tag{10}$$

Therefore, the effective secrecy throughput can be given by [27]

$$\Psi(R_E, R_B) = (R_B - R_E)[1 - O_r(R_B)][1 - O_s(R_E)], \tag{11}$$

where $(R_B - R_E)$ quantifies the target secrecy rate R whereas $[1 - O_r(R_B)][1 - O_s(R_E))]$ informs the probability that the information is securely transmitted from Alice to Bob. Thus, $\Psi(R_E, R_B)$ tells the average secrecy rate at which the private messages are transmitted from Alice to Bob without being leaked to Eve. Finally, as stated in [27], the constraints $R_B > 0$ and $0 < R_E < R_B$ apply to (11) and, as a consequence, $\Psi(R_E, R_B) \geq 0$.

It is important to emphasize that the computation of the effective secrecy throughput is relevant in the following situations:

- *Situation #1*: Alice knows C_B (i.e., Bob's CSI is available) but she does not know C_E. In this case, following [27], $R_B = C_B$ is adopted and, as a consequence, $O_r(R_B) = 0$. Under this assumption, the effective secrecy throughput can be expressed as

  $$\Psi_1(R_E) = (C_B - R_E)[1 - O_s(R_E)]. \tag{12}$$

  Also, the maximization of (12) yields the redundancy rate, which is given by

  $$R^*_{E,1} = \underset{0<R_E<C_B}{\arg\max}\ \Psi_1(R_E). \tag{13}$$

  In consequence the maximum effective secrecy throughput is $\Psi^*_1 = \Psi_1(R^*_{E,1})$.
- *Situation #2*: Alice does not know C_B and C_E. In this case, the effective secrecy throughput is given by

  $$\Psi_2(R_E, R_B) = (R_B - R_E)[1 - O_r(R_B)][1 - O_s(R_E)]. \tag{14}$$

  The codeword and redundancy rates, which maximize (14), are expressed as

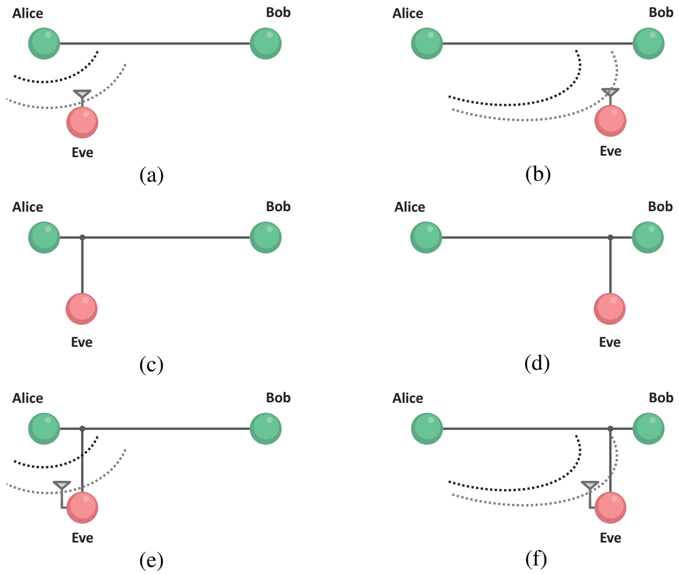
  $$(R^*_{B,2}, R^*_{E,2}) = \underset{0<R_B, 0<R_E<R_B}{\arg\max}\ \Psi_2(R_B, R_E). \tag{15}$$

  As a result, the maximum effective secrecy throughput is $\Psi^\star_2 = \Psi_2(R^*_{B,2}, R^*_{E,2})$.

IV. Numerical Results

This section assesses the effective secrecy throughput and wiretap code rates for the hybrid PLC/WLC wiretap channel model assuming that Eve is passive, i.e., Eve's CSI is not available to Alice. Also, it analyzes the situation in which Eve is a passive WLC [21] or passive PLC eavesdropper [25] since a comparison among them is important to show how dangerous a hybrid PLC/WLC eavesdropper can be. In order to simplify the numerical simulations, C_B and C_E are computed only based on the use of uniform power allocation (UA) technique since the difference in the results obtained with the optimal power allocation (OA) and UA techniques is not relevant in terms of PLS [16], [21]. In addition, $P_T \in [20, 30]$ dBm, the frequency band 1.7 – 86 MHz, and $N = 1727$ are adopted.

Furthermore, in this study, Ψ^*_1 and Ψ^*_2 are numerically computed based on CFR estimates and measured additive noises obtained from measurement campaigns carried out in several Brazilian houses [2], [30]. The CFR estimates are composed of PLC channels, which model the Alice-Bob and Alice-Eve links, and hybrid PLC-WLC channels, which represent the Alice-Eve link.



(a) (b) (c) (d) (e) (f)

Fig. 3: Illustrations of Alice, Bob, and Eve positions. (a) SP WLC eavesdropper. (b) LP WLC eavesdropper. (c) SP PLC eavesdropper. (d) LP PLC eavesdropper. (e) SP hybrid PLC/WLC eavesdropper. (f) LP hybrid PLC/WLC eavesdropper.

Moreover, two sets of Alice, Bob, and Eve positions are taken into account, named as short-path (SP) and long-path (LP), according to the following definition:

- *Short-path (SP)*: Eve is near Alice and far from Bob, see Fig. 3.
- *Long-path (LP)*: Eve is far from Alice and near Bob, see Fig. 3.

Note that, in [25], the authors referenced the SP and LP scenarios as cases #3 and #2, respectively.

Regarding the adopted data sets, Fig 4 shows the cumulative distribution functions (CDFs) of the average channel gain (ACG) for the CFR estimates related to Bob and Eve. Observe that the ACG in decibel (dB) can be expressed as

$$\bar{G}_l = 20\log_{10}\left(\frac{1}{N}\sum_{k=0}^{N-1}|H_l[k]|\right) \tag{16}$$

In Fig. 4, when 90^{th} and 10^{th} percentiles are taken into account, one can see $\bar{G}_l$ values equal to -16.8 and -27.6 dB for Bob's CFRs. Also, considering the PLC CFRs related to Eve, $\bar{G}_l$ equals to -10.2 and -16.9 dB for 90^{th} percentile are found in SP and LP scenarios, respectively, and $\bar{G}_l = -27.8$ and -16.7 dB are observed for 10^{th} percentile, respectively. Likewise, regarding the hybrid PLC-WLC CFRs, it can be seen $\bar{G}_l = -28.3$ and -36.4 dB for SP and LP scenarios, respectively, for 90^{th} percentile and $\bar{G}_l = -36.9$ and -48.8 dB, respectively, for 10^{th} percentile. In summary, taking into account the Alice-Eve links, we observe that the hybrid PLC-WLC CFRs present higher attenuation than the PLC CFRs.

A. Effective Secrecy Throughput

Considering the LP and SP scenarios, Figs. 5 and 6 show $\bar{\Psi}_1^*$ and Ψ_2^* respectively versus P_T for the cases where an in-home and broadband PLC system is threatened by hybrid PLC/WLC, PLC, and WLC eavesdroppers. In these figures, the right-side figures show zooms of the shaded parts of the left-side figures. Note that $\bar{\Psi}_1^* = \mathbb{E}\{\Psi_1^*\}$ and $\bar{\Psi}_1^*$ and $\bar{\Psi}_2^*$ increase as P_T rises and, as a consequence, situation #1 provides higher secrecy than situation #2. Furthermore, LP yields higher values of Ψ_1^* and Ψ_2^* than SP for all eavesdroppers. Also, in general, PLC eavesdroppers are more threatening to the security of an in-home and broadband PLC system than WLC ones while hybrid PLC/WLC eavesdroppers stand out as the worst security threat to an in-home and broadband PLC system. In contrast, a WLC eavesdropper close to Alice is a greater risk to the security of an in-home and broadband PLC system than a PLC or a hybrid PLC/WLC eavesdropper located far from Alice and near Bob. For instance, when $P_T = 30$ dBm, $\Psi_1^* = 2.09$ and 0.19 b/s/Hz and $\Psi_2^* = 1.40$ and 0.10 b/s/Hz are found for LP and SP scenarios when Eve is a WLC device, respectively. Also $\Psi_1^* = 0.89$ and 0.06 b/s/Hz and $\Psi_2^* = 0.39$ and 0.01 b/s/Hz are attained for LP and SP scenarios when Eve is a PLC device, respectively. Regarding the hybrid PLC/WLC eavesdroppers, one sees $\Psi_1^* = 0.37$ and 0 b/s/Hz and $\Psi_2^* = 0.15$ and 0 b/s/Hz for the LP and SP scenarios, respectively.

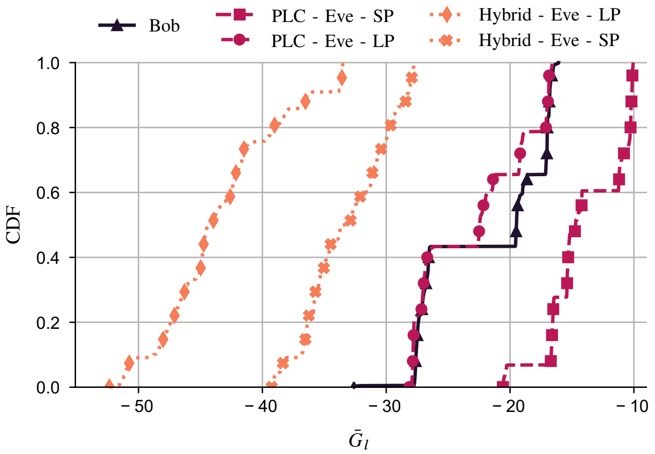


Fig. 4: Average channel gain, $\bar{G}_l$, of the PLC CFR estimates related to Bob and the hybrid PLC-WLC and PLC CFR estimates related to Eve in both SP and LP scenarios.

Therefore, the results illustrated in Figs. 5 and 6 show that the hybrid PLC/WLC eavesdropper imposes lower effective secrecy throughput than the PLC and WLC eavesdroppers on an in-home and broadband PLC system. Moreover, a WLC eavesdropper in the SP scenario may be dangerous for the PLS of an in-home and broadband PLC system. In such a case, effective secrecy throughput values lower than the ones found for the PLC and hybrid PLC/WLC eavesdroppers in the LP scenario have been observed.

B. Wiretap Code Rates

Fig. 7 shows $R_{E,1}^* \times P_T$ for the cases where an in-home and broadband PLC system is threatened by the hybrid PLC/WLC, PLC, and WLC eavesdroppers considering the LP and SP scenarios. Note that higher values of $R_{E,1}^*$ are required to achieve Ψ_1^* for SP than the ones found for LP. Also, higher

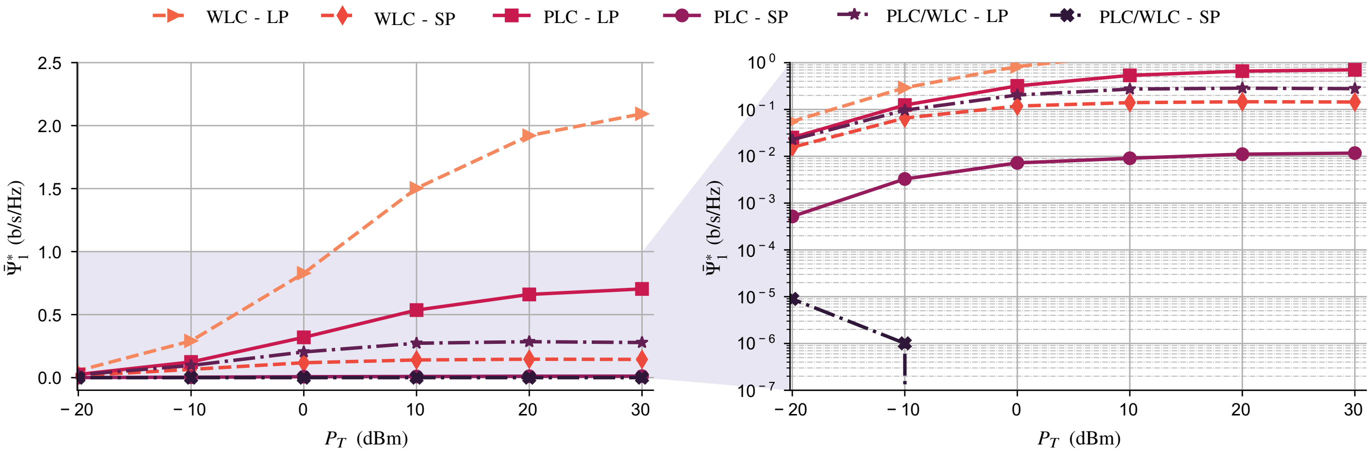


Fig. 5: Situation #1: Effective secrecy throughput, Ψ^*_1, versus total transmission power, P_T.

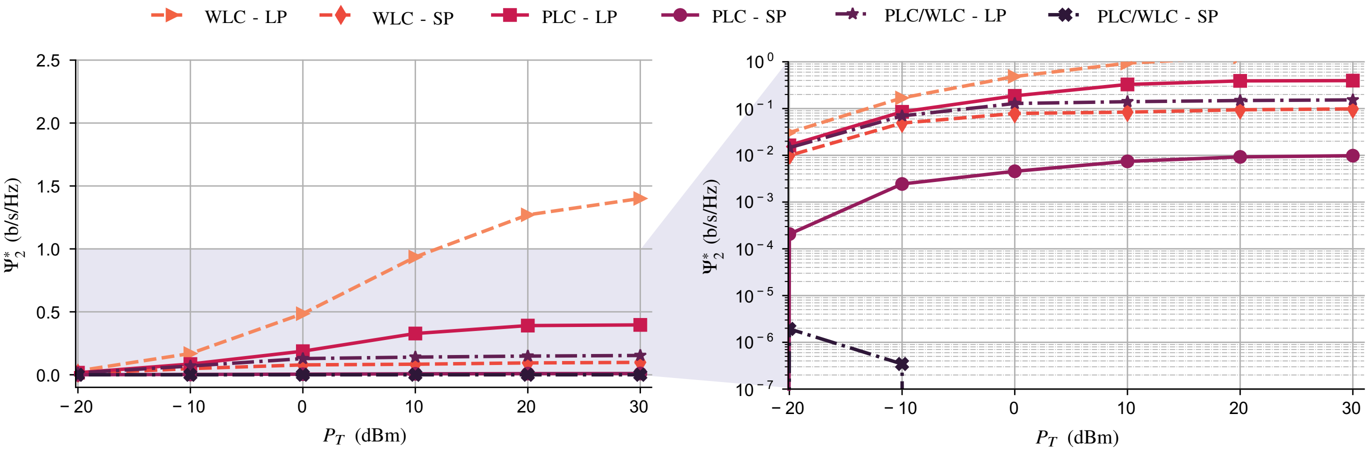


Fig. 6: Situation #2: Effective secrecy throughput, Ψ^*_2, versus total transmission power, P_T.

values of $R^*_{E,1}$ are found for the PLC eavesdropper than the ones found for the WLC eavesdropper. Furthermore, the highest values of $R^*_{E,1}$ are observed for the hybrid PLC/WLC eavesdropper. Note that for this type of eavesdropper, in the SP scenario, $R^*_{E,1}$ cannot be assessed when $P_T > -10$ since $\Psi^*_1 = 0$. In addition, it is clear that $R^*_{E,1}$ increases as P_T rises for both LP and SP scenarios for all eavesdroppers. For instance, when $P_T = 30$ dBm, $R^*_{E,1} = 6.00$ and 9.15 b/s/Hz are noticed for LP and SP scenarios when Eve is a WLC device, respectively. Also, $R^*_{E,1} = 7.92$ and 10.10 b/s/Hz are found for LP and SP channels, when Eve is a PLC device, respectively. Lastly, $R^*_E = 8.78$ b/s/Hz is found for the hybrid PLC/WLC eavesdropper in the LP scenario.

Figs. 8(a) and (b) show $R^*_{B,2}$ and $R^*_{E,2}$, respectively, versus P_T for the cases where an in-home and broadband PLC system is threatened by the hybrid PLC/WLC, PLC, and WLC eavesdroppers taking into account the LP and SP scenarios. Note that the difference between $R^*_{B,2}$ and $R^*_{E,2}$ (i.e., the target secrecy rate) increases as P_T rises for all eavesdroppers. Also, such difference is the highest for WLC eavesdroppers while is the lowest for the hybrid PLC/WLC eavesdropper. Also, observe that when $P_T > -10$ dBm it is not possible to evaluate $R^*_{B,2}$ and $R^*_{E,2}$ for the hybrid PLC/WLC eavesdropper, in the SP scenario, because Ψ^*_2 is equal to zero. Based on the adoption of $P_T = 30$ dBm, one sees $R^*_{B,2} = 8.63$ and 10.81 b/s/Hz and $R^*_{E,2} = 6.01$ and 9.74 b/s/Hz for LP and SP scenarios when Eve is a WLC device, respectively. Also, $R^*_{B,2} = 9.39$ and 10.82 b/s/Hz and $R^*_{E,2} = 7.74$ and 10.09 b/s/Hz are found for the LP and SP scenarios when Eve

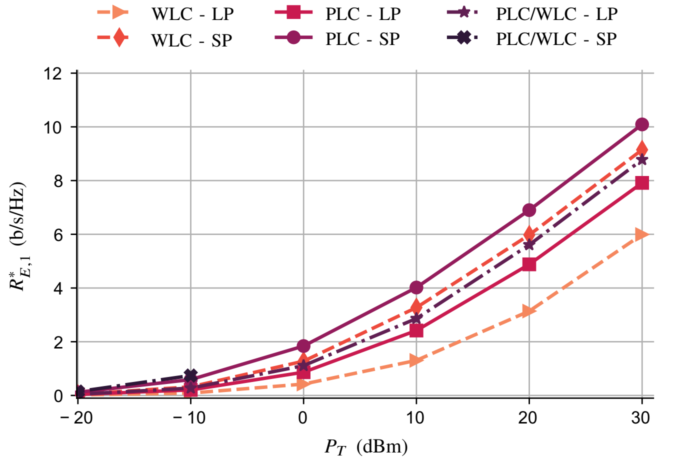
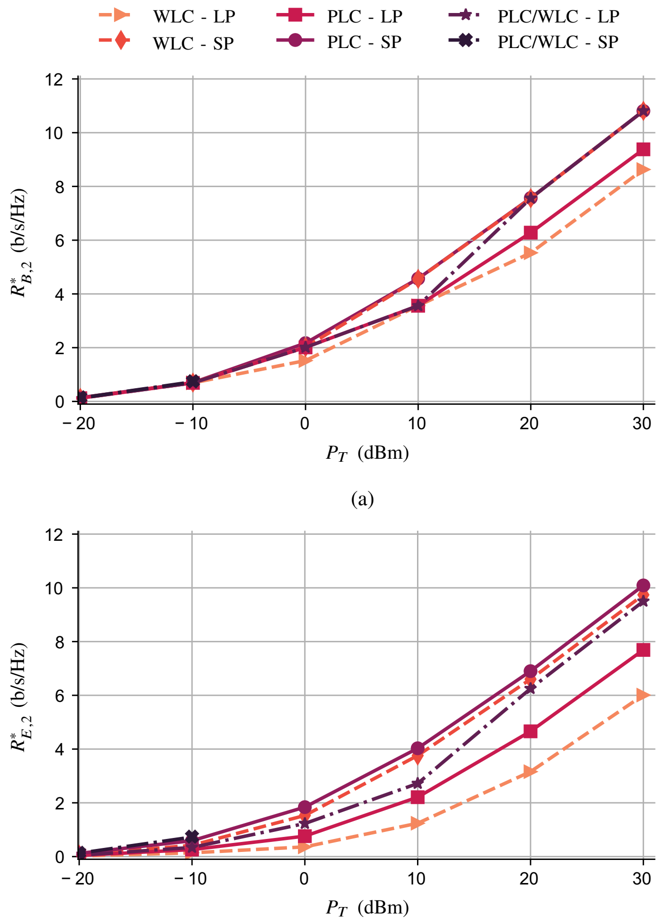


Fig. 7: Redundancy rate in situation #1, $R^*_{E,1}$, versus total transmission power, P_T.



(a)

(b)

Fig. 8: Wiretap code rates in situation #2, $R^*_{B,2}$ and $R^*_{E,2}$, versus total transmission power, P_T. (a) $R^*_{B,2} \times P_T$. (b) $R^*_{E,2} \times P_T$.

is a PLC device, respectively. Regarding the hybrid PLC/WLC eavesdropper, $R^*_{B,2} = 10.81$ b/s/Hz and $R^*_{E,2} = 9.5$ b/s/Hz are observed in the LP scenario.

Finally, numerical results show that security at the physical layer level may be achieved, on average, for an in-home and broadband PLC system in practical scenarios when the respective wiretap code rates are used, except when the hybrid PLC/WLC eavesdropper is near Alice. In this case, values of effective secrecy throughput equal zero are found for practical values of the total transmission power, i.e., $P_T \in [0, 30]$ dBm.

V. Conclusion

This study has investigated the effective secrecy throughput and the corresponding wiretap code rates of an in-home and broadband PLC system when a hybrid PLC/WLC eavesdropper overhears private messages sent from a PLC transmitter to an intended PLC receiver. Also, it has discussed performance comparison when the presence of hybrid PLC/WLC, WLC, and PLC eavesdroppers are taken into account.

Reported results showed that effective secrecy throughput values are equal to zero when a hybrid PLC/WLC eavesdropper is near Alice and the total transmission power is higher than −10 dBm. When a WLC eavesdropper is near Alice, low values of effective secrecy throughput are achieved. These values are lower than those found when the PLC or hybrid PLC/WLC eavesdroppers are far from Alice and near Bob. The comparison among the eavesdroppers showed that the hybrid PLC/WLC eavesdropper is the most powerful threat to the security of in-home and broadband PLC systems. Also, numerical results indicated that the use of electromagnetically shielded power cables can eliminate the hardness of a hybrid PLC/WLC eavesdropper; however, we point out that the costs may be economically prohibitive.

Overall, the wiretap code rates to mitigate the threat of the hybrid PLC/WLC and WLC eavesdroppers to in-home and broadband PLC systems were presented. Regarding the hybrid PLC/WLC eavesdropper, the wiretap code rates were addressed only for the case in which it is near Bob and far from Alice since the effective secrecy throughput is zero when it is close to Alice and far from Bob.

Acknowledgment

The authors also would like to thank prof. Richard D. Souza for valuable discussions on PLS.

References

[1] M. V. Ribeiro, G. R. Colen, F. V. P. Campos, Z. Quan, and H. V. Poor, "Clustered-OFDM for power line communication: When can it be beneficial?" *IET Commun.*, vol. 8, no. 13, pp. 2336–2347, Sept. 2014, doi: 10.1049/iet-com.2014.0056.

[2] 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, doi: 10.1109/TCOMM.2015.2499744.

[3] M. Mohammadi, L. Lampe, M. Lok, S. Mirabbasi, M. Mirvakili, R. Rosales, and P. Van Veen, "Measurement study and transmission for in-vehicle power line communication," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2009, pp. 73–78, doi: 10.1109/ISPLC.2009.4913407.

[4] S. Barmada, L. Bellanti, M. Raugi, and M. Tucci, "Analysis of powerline communication channels in ships," *IEEE Trans. Veh. Technol.*, vol. 59, no. 7, pp. 3161–3170, Sep. 2010, doi: 10.1109/TVT.2010.2052474.

[5] S. Barmada, A. Gaggeli, A. Musolino, R. Rizzo, M. Raugi, and M. Tucci, "Design of PLC system onboard trains: selection and analysis of the PLC channel," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Apr. 2008, pp. 13–17, doi: 10.1109/ISPLC.2008.4510391.

[6] F. Grassi, S. A. Pignari, and J. Wolf, "Channel characterization and EMC assessment of a PLC system of spacecraft DC differential power buses," *IEEE Trans. Electromag. Compat.*, vol. 53, no. 3, pp. 664–675, Aug. 2011, doi: 10.1109/TEMC.2011.2125967.

[7] A. Camponogara, T. R. Oliveira, R. Machado, and M. V. Finamore, W. A. Ribeiro, "Measurement and characterization of power lines of aircraft flight test instrumentation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 3, pp. 1550–1560, Apr. 2019, doi: 10.1109/TAES.2019.2913613.

[8] J. A. Cortés, F. J. Canete, L. Díez, and J. T. Entrambasaguas, "Characterization of the cyclic short-time variation of indoor power-line channels response," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Apr. 2005, pp. 326–330, doi: 10.1109/ISPLC.2005.1430524.

[9] J. A. Cortés, F. J. Canete, L. Díez, and J. L. G. Moreno, "On the statistical properties of indoor power line channels: Measurements and models," in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Apr. 2011, pp. 271–276, doi: 10.1109/ISPLC.2011.5764406.

[10] A. Cataliotti, V. Cosentino, and G. Di Cara, D. Tinè, "Measurement issues for the characterization of medium voltage grids communications," *IEEE Trans. Instrum. Meas.*, vol. 62, no. 8, pp. 2185–2196, Jun. 2013, doi: 10.1109/TIM.2013.2264861.

[11] G. Huang, D. Akopian, and C. L. P. Chen, "Measurement and characterization of channel delays for broadband power line communications," *IEEE Trans. Instrum. Meas.*, vol. 63, no. 11, pp. 2583–2590, May 2014, doi: 0.1109/TIM.2014.2313033.

[12] L. G. S. Costa, A. C. M. Queiroz, B. Adebisi, V. L. R. Costa, and M. V. Ribeiro, “Coupling for power line communications: A survey,” *J. Commun. Inf. Syst.*

[13] T. R. Oliveira, A. A. M. Picorone, S. L. Netto, and M. V. Ribeiro, “Characterization of Brazilian in-home power line channels for data communication,” *Elect. Power Syst. Res.*, vol. 150, pp. 188 – 197, 2017, doi: 10.1016/j.epsr.2017.05.011.

[14] R. M. de Oliveira, A. B. Vieira, H. A. Latchman, and M. V. Ribeiro, “Medium access control protocols for power line communication: A survey,” *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 920–939, Firstquarter. 2019, doi: 10.1109/COMST.2018.2865835.

[15] A. Pittolo and A. M. Tonello, “Physical layer security in power line communication networks: An emerging scenario, other than wireless,” *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, 2014.

[16] A. Camponogara, H. V. Poor, and M. V. Ribeiro, “PLC systems under the presence of a malicious wireless device: Physical layer security analyses,” *IEEE Syst. J.*, vol. 14, no. 4, pp. 4901–4910, Dec. 2020, doi: 10.1109/JSYST.2020.2969044.

[17] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Techn. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975, doi: 0.1002/j.1538-7305.1975.tb02040.x.

[18] Y. Zhuang and L. Lampe, “Physical layer security in MIMO power line communication networks,” in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2014, pp. 272–277, doi: 10.1109/ISPLC.2014.6812346.

[19] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and A. M. Tonello, “Physical layer security of cooperative relaying power-line communication systems,” in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Mar. 2016, pp. 185–189, doi: 10.1109/ISPLC.2016.7476261.

[20] G. Prasad, O. Taghizadeh, L. Lampe, and R. Mathar, “Securing MIMO power line communications with full-duplex jamming receivers,” in *Proc. IEEE Int. Symp. Power Line Commun. Appl.*, Apr. 2019, pp. 1–6, doi: 10.1109/ISPLC.2019.8693263.

[21] A. Camponogara, H. V. Poor, and M. V. Ribeiro, “The complete and incomplete low-bit-rate hybrid PLC/wireless channel models: Physical layer security analyses,” *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2760–2769, Apr. 2019, doi: 10.1109/JIOT.2018.2874377.

[22] 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, Jan. 2017, doi: 10.1109/ACCESS.2017.2729784.

[23] A. E. Shafie, M. F. Marzban, R. C. Chabaan, and N. Al-Dhahir, “An artificial-noise-aided secure scheme for hybrid parallel PLC/wireless OFDM systems,” in *Proc. IEEE Int. Conf. Commun.*, May 2018, pp. 1–6, doi: 10.1109/ICC.2018.8422901.

[24] V. Mohan, A. Mathur, V. Aishwarya, and S. Bhargav, “Secrecy analysis of PLC system with channel gain and impulsive noise,” in *Proc. IEEE Veh. Techn. Conf.*, Sep. 2019, pp. 1–6, doi: 10.1109/VTC-Fall.2019.8890986.

[25] A. 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.*, pp. 1–12, 2020, doi: 10.1109/JSYST.2020.2999487.

[26] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, “On the target secrecy rate for SISOME wiretap channels,” in *IEEE Int. Conf. Commun.*, Jun. 2014, pp. 987–992, doi: 10.1109/ICC.2014.6883448.

[27] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, “Optimization of code rates in SISOME wiretap channels,” *IEEE Internet Wireless Commun.*, vol. 14, no. 11, pp. 6377–6388, Nov. 2015, doi: 10.1109/TWC.2015.2453260.

[28] A. Jorswieck, Eduard and A. Wolf, “Resource allocation for the wire-tap multi-carrier broadcast channel,” in *Int. Conf. Telecomm.*, Jun. 2008, pp. 1–6, doi: 10.1109/ICTEL.2008.4652697.

[29] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008, doi: 10.1109/TIT.2008.921678.

[30] 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, Sep. 2016, doi: https://doi.org/10.14209/jcis.2016.20.

[31] C. Choudhuri and U. Mitra, “Capacity bound for relay channels with intersymbol interference and colored gaussian noise,” *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5639–5652, Sep. 2014, doi: 10.1109/TIT.2014.2322859.

[32] A. J. Goldsmith and M. Effros, “The capacity region of broadcast channels with intersymbol interference and colored noise,” *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 219–240, Sep. 2001, doi: 10.1109/18.904524.

Ândrei Camponogara received the B.Sc. degrees in Industrial Design and in Computer Engineering from the Federal University of Santa Maria (UFSM), RS, Brazil, in 2010 and 2014, respectively. Also, he received the M.Sc. and D.Sc. degrees in Electrical Engineering from Federal University of Juiz de Fora (UFJF), MG, Brazil in 2016 and 2020, respectively. Currently, he is a Postdoctoral research fellow at UFJF. His main interests are in power line communication, hybrid communication, digital communication, and digital signal processing.

Moisés V. Ribeiro received the B.S. degree in Electrical Engineering from the Federal University of Juiz de Fora (UFJF), MG, Brazil, and M.Sc. and D.Sc. Degrees in Electrical Engineering from the University of Campinas, SP, Brazil, in 1999, 2001, and 2005. He was a Visiting Scholar at the University of California in Santa Barbara, CA, USA, in 2004, Visiting Professor (2005-2007), and Assistant Professor (2007-2015) at UFJF. Since 2015, he has been an Associate Professor at UFJF. He is also the Director of the Brazilian National Institute of Science and Technology for Smart Grid (INERGE). He co-founded Smarti9 LTD. and Wari LTD. in 2012 and 2015, respectively. He had served as the Secretary of the IEEE ComSoc TC-PLC.

Dr. Ribeiro was the recipient of Fulbright Visiting Professorship at Stanford University, Stanford, CA, USA, in 2011, and at Princeton University, Princeton, NJ, USA, in 2012. He was the General Chair of the 2010 IEEE ISPLC, 2013 IWSGC, SBrT 2015, and a Guest Co-Editor for Special Issues in the EURASIP Journal on Advances in Signal Processing and EURASIP Journal of Electrical and Computer Engineering. He was awarded Student Awards from 2001 IEEE IECON and 2003 IEEE ISIE, Winner of 2014 I2P Global Competition, Honorable Mention in 2014 Global Venture Labs Investment Competition, 3rd Place Prêmio Mineiro de Inovação 2014, Engie Brazil Innovation Award 2016, Unicamp Inventor Award in 2017 and 2018.

Dr. Ribeiro’s research interests include signal processing, power line communication, wireless communication, computational intelligence, internet of everything. He has advised 42 graduate students in these fields and authored over 210 peer-reviewed papers and nine book chapters. He holds 13 issued/pending patents