Effective Secrecy Throughput in PLC Systems Threatened by a Wireless Eavesdropper: A Practical Perspective

Álvaro G. S. Correia, Ândrei Camponogara, and Moisés V. Ribeiro

***Abstract*— This paper advances the investigation of physical layer security of broadband and indoor power line communication (PLC) system when a malicious wireless communication (WLC) device tries to eavesdrop upon private messages exchanged between two PLC devices. To do so, numerical results related to the effective secrecy throughput and the corresponding wiretap code rates for distinct positions of the malicious WLC device are provided for three different frequency bands, $1.7-30$ MHz, $1.7-50$ MHz, and $1.7-86$ MHz under the power masks defined by the IEEE 1901 $13-29$ and ITU-T G.9964 standards.**

***Keywords*— Physical layer security, wireless communication, power line communication, effective secrecy throughput.**

I. Introduction

Over the years, power line communication (PLC) has become a well-established technology with applications in indoor (e.g., houses and commercial buildings), outdoor (low-, medium-, and high-voltage), and in-vehicles (e.g., cars, airplanes, trains, ships, and spacecraft) electric power systems [1]. The main advantages of PLC technology are easy installation in low-voltage electric power circuits and low implementation cost since the data communication infrastructure is already available. However, as electric power systems are only designed for delivery energy, data carrying signals suffer with attenuation as distance and frequency increase due to the use of non-ideal cables; multipath effects caused by impedance mismatching at load and branching connection points; impulsive noise generated by switching devices; time-varying behavior due to the dynamic of loads connected to the electric power systems; interference signals from other telecommunication systems, which operate in the same frequency band, since electric power systems are mainly composed of unshielded power cables [2], [3].

In this way, the broadcast propagation of data carrying signals in electric power systems and leakage of these signals into the air due to the use of unshielded power cables constitute two serious security breaches in PLC systems. In fact, malicious PLC and wireless communication (WLC) devices connected to and close to power lines, respectively, can overhear private information of a PLC system operating in it. One way to deal with the presence of those eavesdroppers is using the knowledge of the PLC channel for guaranteeing that eavesdroppers can not decode private messages from the PLC system. This approach is known as physical layer security (PLS). In this regard, there have been a few studies in the literature that investigate security at the physical layer in PLC systems [4]–[7].

Camponogara *et al.* [4] studied the PLS of a broadband in-home PLC system eavesdropped by a passive and malicious PLC device. Numerical results showed the level of vulnerability of this system for three distinct frequency bands. Similarly, [5] investigated the PLS of a cooperative relaying PLC system which uses artificial noise to guarantee secrecy in the presence of a PLC eavesdropper. In [6], the authors analyzed the achievable secrecy rate related to PLC systems under the presence of a WLC eavesdropper. To do so, a data set constituted of channel estimates and additive noise measures obtained in a measurement campaign was considered. Also, Camponogara *et al.* [7] studied the effective secrecy throughput (EST) along with the corresponding wiretap code rates for an in-home and broadband PLC system, when WLC, PLC, and hybrid PLC/WLC eavesdroppers overhear private information from this system.

Aiming to attach the studies regarding the PLS in in-home and broadband PLC systems threatened by a WLC eavesdropper toward a more practical scenario, this study investigates the ESTs and their respective wiretap codes under the power masks defined by the IEEE 1901 $13-29$ [8] and ITU-T G.9964 [9] standards, which is a severe constraint that practical PLC devices needs to agree with. Furthermore, in addition to the frequency band investigated earlier in [6], [7] ($1.7-86$ MHz), the frequency bands $1.7-30$ MHz and $1.7-50$ MHz are assessed. As in [6], [7], the numerical results are provided by using a data set composed of channel frequency response (CFR) estimates and additive noise measures obtained in a measurement campaign reported in [2].

The rest of this paper is organized as follows: Section II details the system model; Section III deduces mathematical expressions for evaluating the EST; Section IV shows the numerical results; and, finally, Section V some concluding remarks are presented.

This study was supported in part by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) - finance code 001, Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq), Instituto Nacional de Energia Elétrica (INERGE), and Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG).

Álvaro G. S. Correia and Moisés V. Ribeiro are with the Department of Electrical Engineering, Federal University of Juiz de Fora, Juiz de Fora, MG, Brazil (e-mails: {alvaro.guilherme, mribeiro}@engenharia.ufjf.br).

Ândrei Camponogara is with the Department of Electrical Engineering, Federal University of Paraná, Curitiba, PR, Brazil (e-mail:andrei.camponogara@ufpr.br).

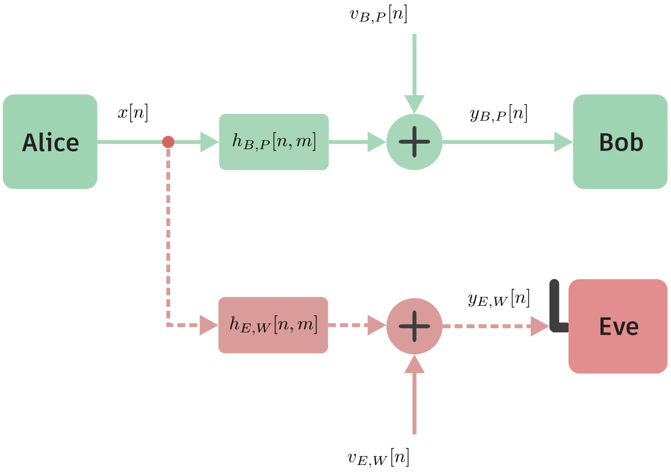


Fig. 1. Block diagram of the hybrid PLC/WLC wiretap channel model. The continuous line represent the PLC channel and the dashed line denotes the hybrid PLC-WLC channel.

II. System Model

Let Fig. 1 illustrate the wiretap channel model considered in this paper, where a transmitter (Alice) wants to send a private message to a legitimate receiver (Bob), keeping it a secret from a passive eavesdropper (Eve), which is a malicious WLC device located in the vicinity of Alice or Bob. According to [10], [11] the hybrid PLC-WLC channels can entirely characterize the wireless propagation of the radiated PLC signal (the link between Alice and Eve). Usually, Eve must be located nearby the electric power circuit, as [11] argued that for Eve to wirelessly overhear the private messages a distance up to 6 m from the power cable is required.

Based on this information, we consider that $\{h_l[n,m]\}$ denotes the discrete-time version of the time-varying channels associated with the link between Alice and the l^{th} receiver where $l \in \{B,E\}$ indicates Bob and Eve. Importantly, the link between Alice and Bob is represented by the PLC channel and the link between Alice and Eve is represented by the hybrid PLC-WLC channel. Then, the discrete-time representation of the received signal at the l^{th} receiver can be expressed as

$$y_l[n] = \sum_{m=-\infty}^{\infty} x[m]h_l[n,m] + v_l[n], \tag{1}$$

where $\{x[n]\}$ is the sequence of infinite numbers of symbols of length N (N-block symbols) that was transmitted; $h_l[n,m]$ is the linear and time-varying channel impulse response (CIR); $\{v_l[n]\}$ it presents the additive noise sequence; and $\{x[n]\}$ and $\{v_l[n]\}$ are independent and wide-sense stationary random processes.

The PLC and hybrid PLC-WLC channels are assumed to be linear and time-invariant during the time interval that corresponds to an N-block symbol. In such time interval, the discrete-time CIR is time-invariant. Consequently, it can be denoted by $\{h_l[n]\}_{n=0}^{L_l-1}$, with L_l being the CIR length associated with the link between Alice and the l^{th} receiver. The vector representation of the discrete-time version of such channels during one N-block symbol is $\mathbf{h}_l = [h_l[0], h_l[1], \cdots, h_l[L_l - 1]]^T$ whereas $\mathbf{H}_l = [H_l[0], H_l[1], \cdots, H_l[N-1]]^T$ is the vector representation in the discrete-frequency domain, where in

$$\mathbf{H}_l = \mathcal{F}\begin{bmatrix}\mathbf{h}_l \\ \mathbf{0}_{N-L_l}\end{bmatrix} \tag{2}$$

and N denotes the number of subchannels. Note that the diagonal matrices $\mathbf{\Lambda}_{\mathcal{H}_l} = \text{diag}\{H_l[0], H_l[1], \cdots, H_l[N-1]\}$ and $\mathbf{\Lambda}_{|\mathcal{H}_l|^2} = \text{diag}\{|H_l[0]|^2, |H_l[1]|^2, \cdots, |H_l[N-1]^2|\}$ will be used.

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

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

where $\mathbf{\Lambda}_P = \text{diag}\{P[0], P[1], \cdots, P[N-1]\}$ is the matrix representation of the power allocated in the frequency domain, $\text{tr}(\mathbf{\Lambda}_P) = P_T$ is the total transmission power, and $[\cdot]^\dagger$ is the Hermitian operator. Moreover, $\mathbf{V}_l \in \mathbb{C}^{N\times 1}$ is the vector representation of the additive noise in the discrete-frequency domain such that

$$\mathbb{E}\{\mathbf{V}_l\} = \mathbf{0}_{N\times 1} \quad \text{and} \quad \mathbb{E}\{\mathbf{V}_l\mathbf{V}_l^\dagger\} = N\mathbf{\Lambda}_{P_{V_l}} \tag{4}$$

where $\mathbf{\Lambda}_{P_{V_l}} = \text{diag}\{P_{V_l}[0], P_{V_l}[1], \cdots, P_{V_l}[N-1]\}$ and $P_{V_l}[k]$ is the additive noise power in the k^{th} sub-channel.

III. Effective Secrecy Throughput

The PLC and hybrid PLC-WLC channels are considered N-block linear Gaussian channels with finite memory (i.e., $L_{\max} = \max L_l$). It is well-known that inter-block interference caused by CIR memory and correlated noises make achievable data rate hard to be computed. In order to overcome this problem, [12] showed that the N-block circular Gaussian relay channel (CGRC) totally removes the inter-block interference if $N \gg L_{\max}$. In this way, as linear Gaussian relay channel (LGRC) tends to N-CGRC as $N \to \infty$, N-CGRC channels model PLC and hybrid PLC-WLC ones since $N \to \infty$.

The received N-block symbol at Bob or Eve is expressed as

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

Thus, the respective signal-noise ratio (SNR) is given by

$$\begin{aligned}\mathbf{\Lambda}_{\gamma_l} &= \frac{\mathbf{\Lambda}_{\mathcal{H}_l}\mathbb{E}[\mathbf{X}\mathbf{X}^\dagger]\mathbf{\Lambda}_{\mathcal{H}_l}^\dagger}{\mathbb{E}\{\mathbf{V}_l\mathbf{V}_l^\dagger\}} \\ &= \mathbf{\Lambda}_P\mathbf{\Lambda}_{|\mathcal{H}_l|^2}\mathbf{\Lambda}_{P_{V_l}}^{-1}\end{aligned} \tag{6}$$

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

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

subjected to $\text{tr}(\Lambda_P) \leq P_T$, and the capacity between Alice and Eve can be expressed as

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

If the channel state informations (CSIs) of Bob and Eve are available at Alice, then perfect secrecy can be achieved since she knows C_B and C_E [13], [14]. From a wiretap code design perspective, the conformity with the reliability and secrecy constraints imposes the wiretap codes R_B and R_E be designed such that $R_B \leq C_B$ and $R_E > C_E$ hold [13], [14], where $R_E = R_B - R$ is the redundancy rate used to confuse Eve, R_B is the codeword rate, and R is the secrecy rate. However, in practical scenarios, Eve is a passive device and, consequently, $R_E > C_E$ can not be guaranteed. In this regard, [13], [14] introduced a novel framework to estimate R_B and R_E based on the EST.

The secrecy outage probability can be represented as

$$\begin{aligned}\mathcal{O}_s(R_E) &= \mathbb{P}\{R_E < C_E\} \\ &= \mathbb{P}\{2^{R_E N} < \det(\mathbf{I}_N + \mathbf{\Lambda}_{\gamma_E})\}, \end{aligned} \tag{9}$$

whereas the reliability outage probability can be expressed

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

As a result, the EST is given by

$$\Psi(R_E, R_B) = (R_B - R_E)[1 - \mathcal{O}_r(R_B)][1 - \mathcal{O}_s(R_E)], \tag{11}$$

where $(R_B - R_E)$ estimates the target secrecy rate R since $[1 - \mathcal{O}_r(R_B)][1 - \mathcal{O}_s(R_E)]$ demonstrates the probability that the information is securely transmitted to Bob from Alice. $\Psi(R_E, R_B)$ shows the average secrecy rate at which private messages are transmitted from Alice to Bob without Eve decoding the information. Lastly, the constraints $R_B > 0$ and $0 < R_E < R_B$ apply to (11) and, as a consequence, $\Psi(R_E, R_B) \geq 0$.

In this study, two situations are adopted to calculate the EST:

- *Situation #1*: Alice is aware of C_B but does not know C_E. Thus, $R_B = C_B$ is considered and, as a consequence, $\mathcal{O}_r(R_B) = 0$. Under this assumption, the EST can be rewritten as

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

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

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

  Hence, the maximum EST is $\Psi^*_1 = \Psi_1(R^*_{E,1})$.
- *Situation #2*: In this case, Alice has no knowledge of C_E or C_B. Therefore, the EST is given by

  $$\Psi_2(R_E, R_B) = (R_B - R_E)[1 - \mathcal{O}_r(R_B)][1 - \mathcal{O}_s(R_E)]. \tag{14}$$

  The codeword and redundancy rates that 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 EST is $\Psi^*_2 = \Psi_2(R^*_{B,2}, R^*_{E,2})$.

TABLE I

STATISTICS OF THE NORMALIZED SNRS FOUND FOR THE PLC, HYBRID SP, AND HYBRID LP CHANNELS IN DECIBELS

Channel	Minimum	Mean	Maximum	SD
PLC	65.7	79.2	84.1	7.91
Hybrid SP	64.0	73.8	80.0	7.35
Hybrid LP	53.5	64.0	72.62	6.47

IV. NUMERICAL RESULTS

This section presents numerical results of EST and the respective wiretap code rates for the hybrid wiretap channel model assuming that Eve is passive, i.e., Alice does not have Eve's CSI. Also, three distinct frequency bands are adopted: $1.7 - 30$ MHz, $1.7 - 50$ MHz, and $1.7 - 86$ MHz, which are denoted as F_{30}, F_{50}, and F_{86}, respectively.

Furthermore, in order to provide a more practical perspective than in [7], it is considered a comparison between the following power masks:

- *Power Mask #1* (IEEE 1901 $13 - 29$): in this case, the power mask defined in IEEE 1901 Standard is applied to the transmit PLC signal. Consequently, for the frequency range $1.7 - 1.8$ MHz, a power spectral density (PSD) of -85 dBm/Hz is considered while for $1.8 - 50$ MHz the PSDs of -85 dBm/Hz and -55 dBm/Hz are switched, respectively. Note that, IEEE 1901 Standard does not define a PSD for $50 - 86$ MHz.
- *Power Mask #2* (ITU-T G.9964): in this mask, the pattern is a little different from the previous one. For the frequency range $1.7 - 2$ MHz, it is used a PSD of -85 dBm/Hz while, for $2 - 30$ MHz, it is adopted a PSD of -50 dBm/Hz. Finally, for the frequency band $30 - 86$ MHz, it is indicated a PSD of -85 dBm/Hz.

Regarding the hybrid wiretap channel model, two cases are analyzed [7]:

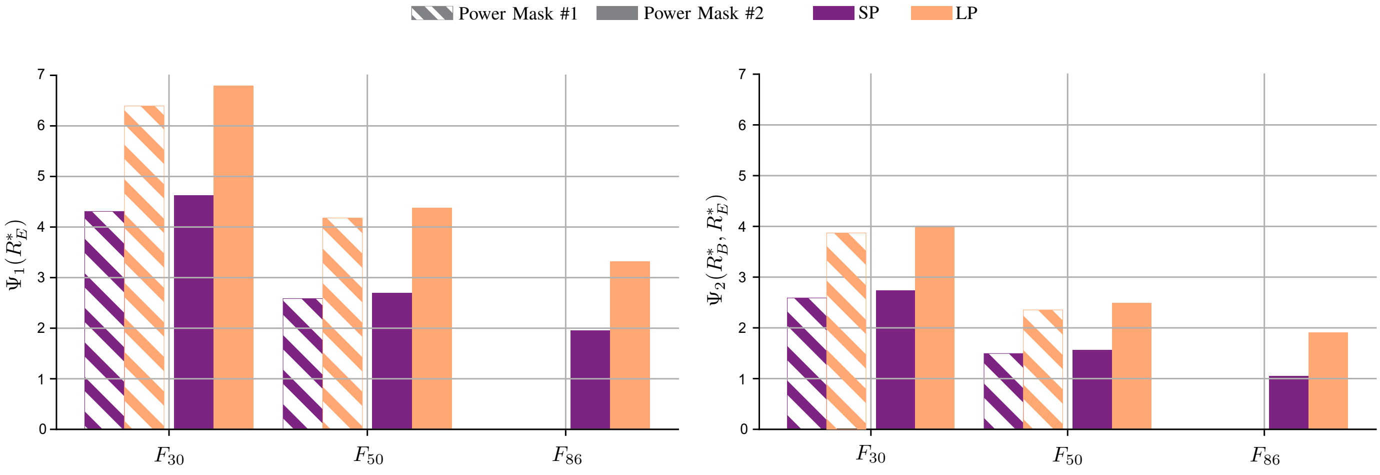
- *Short-Path (SP)*: Eve is close to Alice (less than 2 m) and far from Bob (between 2 and 6 m).
- *Long-Path (LP)*: Eve is close to Bob (less than 2 m) and far from Alice (between 2 and 6 m).

Based on the CFR estimates, Table I shows the minimum, mean, maximum, and standard deviation (SD) of normalized signal-noise ratio (nSNR) values in decibels (dB) for the PLC, hybrid SP, and hybrid LP channels. According to [15], the nSNR multichannel parameter can be expressed as

$$\bar{\gamma}_l = \det(\mathbf{I}_N + \mathbf{\Lambda}_{|\mathcal{H}_l|^2} \mathbf{\Lambda}^{-1}_{P_{V_l}})^{1/N} - 1 \tag{16}$$

Analyzing Table I, it can be seen that the values of nSNR when Eve is closer to Alice (i.e., SP channels) are higher than when she is farther away (i.e., LP channels).

Figs. 2(a) and (b) show Ψ^*_1 and Ψ^*_2 for the frequency bands F_{30}, F_{50}, and F_{86} considering SP and LP scenarios and comparing the two analyzed masks. In this figure, we can see an improvement in the situation #1 compared to the situation #2 due to the knowledge of Bob's CSI. Note that Ψ^*_1 and Ψ^*_2 decrease as the frequency band increases. Also, SP channels yields lower values of Ψ^*_1 and Ψ^*_2 than LP



(a)

(b)

Fig. 2. EST for situations #1 and #2 in terms of the frequency bands F_{30}, F_{50}, and F_{86}

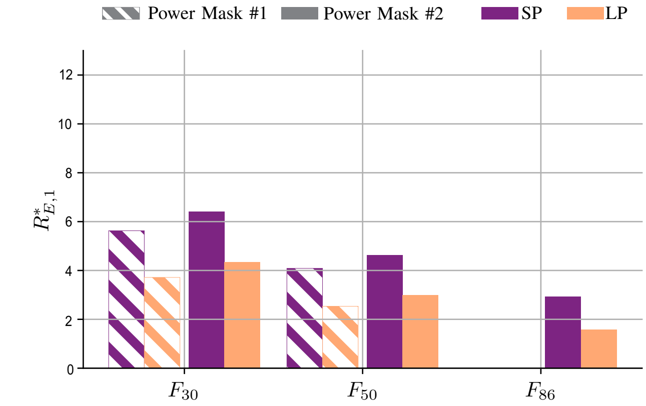


Fig. 3. Redundancy rate for situation #1, $R_{E,1}^*$, in terms of the frequency bands F_{30}, F_{50}, and F_{86}

channels for the chosen frequency bands. To illustrate how the power masks impact the PLS, Fig. 2 shows that the Power Mask #2 has slightly higher EST values than the Power Mask #1. For instance, for the SP scenario and F_{30}, the values of $\Psi_1^* = 4.31$ bps/Hz and $\Psi_2^* = 2.59$ bps/Hz are observed for the Power Mask #1, while the values of $\Psi_1^* = 4.62$ bps/Hz and $\Psi_2^* = 2.73$ bps/Hz are found for the Power Mask #2.

Figs. 3 and 4(a)-(b) show the wiretap codes $R_{E,1}^*$ and $(R_{B,2}^*, R_{E,2}^*)$ respectively for the frequency bands F_{30}, F_{50}, and F_{86}. Also, it is considered the SP and LP scenarios and the Power Mask #1 and #2. Note that the SP scenario offers higher values of wiretap code rates than the LP scenario, with the exception of F_{86}, see Fig. 4(a). Furthermore, the values of $R_{E,1}^*$, $R_{B,2}^*$, and $R_{E,2}^*$ also decrease as the frequency band increases. Regarding the adopted power masks, as expected, one can see that the Power Mask #2 provides the best results. In particular, for the situation #1, the SP scenario, and the frequency band F_{30}, one can find $R_{E,1}^* = 5.63$ bps/Hz and 6.42 bps/Hz by applying the Power Mask #1 and the Power Mask #2, respectively. Still in situation #1, the SP scenario, and F_{30}, the values of $R_{B,2}^* = 11.26$ bps/Hz and $R_{E,2}^* = 5.94$ bps/Hz are obtained for the Power Mask #1 while the values of $R_{B,2}^* = 12.31$ bps/Hz and $R_{E,2}^* = 6.75$ bps/Hz are found for the Power Mask #2.

Overall, the attained results show that security at the physical layer level can be achieved for the SP and LP scenarios by applying the chosen power masks if the respective wiretap code rates are used. Also, the numerical results show that the power mask for the ITU-T G.9964 yields slightly better results then its counterpart from the IEEE 1901 $13-29$, which also provides satisfactory secrecy results.

V. Conclusion

This paper has discussed the EST and the corresponding wiretap code rates for a PLC system under the presence of a passive WLC eavesdropper, which is capable of overhearing private messages sent by a PLC transmitter to an intended PLC receiver. Aims at bringing a more practical perspective, the EST and the respective wiretap code rates have been evaluated for the ITU-T G.9964 and IEEE 1901 $13-29$ power masks in three distinct frequency bands: $1.7-30$ MHz, $1.7-50$ MHz, and $1.7-86$ MHz.

The numerical results have shown that lower values of EST are achieved when Eve is close to Alice compared to the scenarios in which Eve is close to Bob. Moreover, we can see that both EST and wiretap code rates values decrease as the frequency band increases. Also, the ITU-T G.9964 power mask have provided better results than the IEEE 1901 $13-29$ power mask. Last but not the least, the analysis of the wiretap code rates to mitigate the threat of a WLC eavesdropper to PLC systems under the use of the ITU-T G.9964 and IEEE 1901 $13-29$ power masks for different frequency bands was performed.

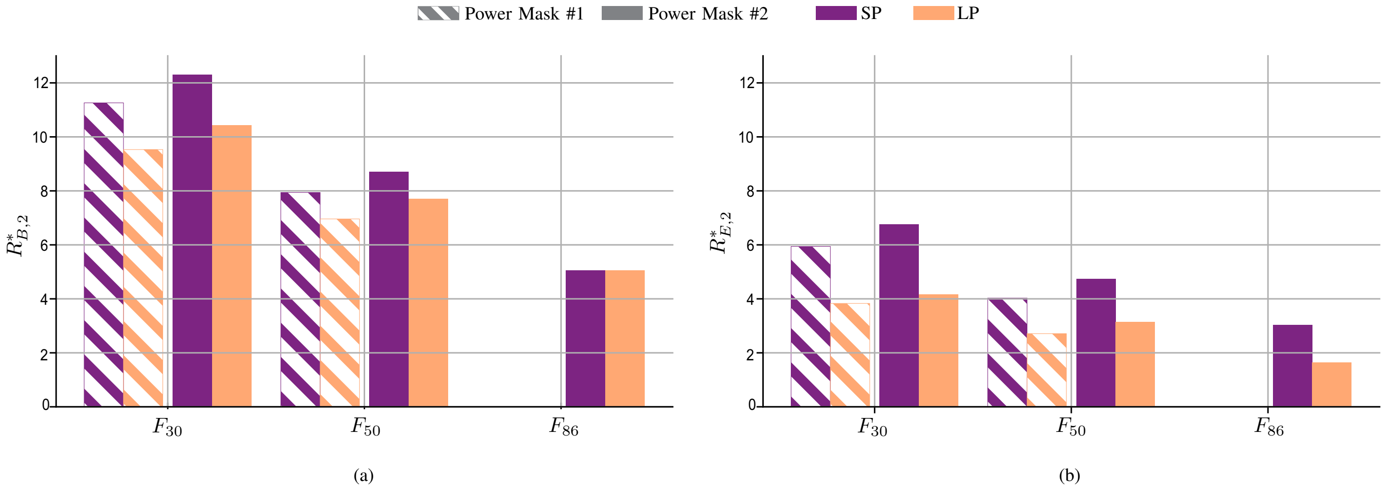


Fig. 4. Wiretap code rates in situation #2, $R^*_{B,2}$ and $R^*_{E,2}$, in terms of the frequency bands F_{30}, F_{50}, and F_{86}

References

[1] A. Camponogara, T. R. Oliveira, R. Machado, W. A. Finamore, and M. V. Ribeiro, “Measurement and characterization of power lines of aircraft flight test instrumentation,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1550–1560, 2019.

[2] 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,” *Electric Power Systems Research*, vol. 150, pp. 188–197, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378779617302006

[3] G. Huang, D. Akopian, and C. L. P. Chen, “Measurement and characterization of channel delays for broadband power line communications,” *IEEE Transactions on Instrumentation and Measurement*, vol. 63, no. 11, pp. 2583–2590, 2014.

[4] A. Camponogara, H. V. Poor, and M. V. Ribeiro, “Physical layer security of in-home PLC systems: Analysis based on a measurement campaign,” *IEEE Systems Journal*, vol. 15, no. 1, pp. 617–628, 2021.

[5] 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 *IEEE International Symposium on Power Line Communications and its Applications*, 2016, pp. 185–189.

[6] 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, 2020.

[7] A. Camponogara and M. V. 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. [Online]. Available: https://jcis.sbrt.org.br/jcis/article/view/750

[8] *IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications*, 1st ed., IEEE Communications Society, 3 Park Avenue, New York, NY 10016-5997, 9 2010.

[9] *Unified high-speed wireline-based home networking transceivers – Power spectral density specification*, G.9964 ed., ITU-T Telecommunication Standardization Sector of ITU, 12 2011.

[10] T. R. Oliveira, C. A. G. Marques, M. S. Pereira, S. L. Netto, and M. V. Ribeiro, “The characterization of hybrid PLC-wireless channels: A preliminary analysis,” in *2013 IEEE 17th International Symposium on Power Line Communications and Its Applications*, 2013, pp. 98–102.

[11] T. R. Oliveira, F. Andrade, A. A. M. Picorone, H. Latchman, S. Netto, and M. V. Ribeiro, “Characterization of hybrid communication channel in indoor scenario,” *Journal of Communication and Information Systems*, vol. 31, no. 1, Sep. 2016. [Online]. Available: https://jcis.sbrt.org.br/jcis/article/view/397

[12] A. Goldsmith and M. Effros, “The capacity region of broadcast channels with intersymbol interference and colored Gaussian noise,” *IEEE Transactions on Information Theory*, vol. 47, no. 1, pp. 219–240, 2001.

[13] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, “On the target secrecy rate for SISOME wiretap channels,” in *IEEE International Conference on Communications*, 2014, pp. 987–992.

[14] S. Yan, N. Yang, G. Geraci, R. Malaney, and J. Yuan, “Optimization of code rates in SISOME wiretap channels,” *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6377–6388, 2015.

[15] J. M. Cioffi. (2018) Chapter 4: Multi-channel modulation.