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

Andrei 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 high-power impulsive noises generated by the dynamics of electric loads and the interference from wireless communications (WLC) systems1, 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.

Andrei 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: andreicamponogara@engenharia.ufjf.br and mriqueiro@engenharia.ufjf.br).

Digital Object Identifier: 10.14209/jcis.2021.4

1This 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

2The 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.

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...
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

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

where \( \{x[n]\} \) is the transmitted sequence that is constituted by an infinite number of \( N\)-length 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 \( \{h_{l,q}[n]\}_{n=0}^{L_{l,q}-1} \), 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

\[
h_{l,q} = [h_{l,q}[0], h_{l,q}[1], \ldots, h_{l,q}[L_{l,q} - 1]]^T
\]

where \( H_{l,q} = [H_{l,q}[0], H_{l,q}[1], \ldots, H_{l,q}[N - 1]]^T \) denotes its vector representation in the frequency domain, where

\[
H_{l,q} = \mathcal{F} \left[ h_{l,q} \right]
\]

and \( N \) denotes the number of sub-channels. Hereafter the diagonal matrices

\[
\Lambda_{H_{l,q}} = \text{diag} \left \{ H_{l,q}[0], H_{l,q}[1], \ldots, H_{l,q}[N - 1] \right \}
\]

and

\[
\Lambda_{|H_{l,q}|^2} = \text{diag} \left \{ |H_{l,q}[0]|^2, |H_{l,q}[1]|^2, \ldots, |H_{l,q}[N - 1]|^2 \right \}
\]

will be used.

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

\[
\mathbb{E}(X) = 0_{N \times 1} \text{ and } \mathbb{E}(XX^H) = NA_{P},
\]

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

\[
\mathbb{E}(V_{l,q}) = 0_{N \times 1} \text{ and } \mathbb{E}(V_{l,q}V_{l,q}^H) = NA_{P_{V_{l,q}}},
\]

where \( A_{P_{V_{l,q}}} = \text{diag} \{P_{V_{l,q}}[0], P_{V_{l,q}}[1], \ldots, P_{V_{l,q}}[N - 1]\} \) 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 \( (R_B \text{ and } R_E) \) 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 har a 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

\[
Y_{l,q} = \Lambda_{H_{l,q}} X + V_{l,q}.
\]

Then the respective SNR is given by

\[
\Lambda_{Y_{l,q}} = \frac{\Lambda_{H_{l,q}} \mathbb{E}(XX^H)^{-1} \Lambda_{H_{l,q}}^T}{\mathbb{E}(V_{l,q}V_{l,q}^H)} = \Lambda_P \Lambda_{Y_{l,q}}^{-1} \Lambda_{P_{V_{l,q}}^{-1}}.
\]

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

\[
C_B = \max_{\Lambda_P} \frac{1}{N} \log_2 \left( \text{det} \left( I_N + \Lambda_{Y_{l,q}} \right) \right) \text{ [bps/Hz]},
\]

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

\[
C_E = \frac{1}{N} \log_2 \left( \text{det} \left( I_N + \Lambda_{Y_{E,P}} + \Lambda_{Y_{E,W}} \right) \right) \text{ [bps/Hz]},
\]

since we assumed that Eve makes use of the maximal-ratio combining (MRC) technique. Note that the \( \Lambda_P \) values used in \( C_E \) are the ones used for maximizing \( C_B \).
Following [27], the secrecy outage probability can be expressed as

\[ O_s(R_E) = \mathbb{P}\{R_E < C_E\} = \mathbb{P}\{2^{R_E N} < \det(I_N + A_{Y E,P} + A_{Y E,W})\}, \quad (9) \]

whereas the reliability outage probability is given by

\[ O_r(R_B) = \mathbb{P}\{R_B > C_B\} = \mathbb{P}\{2^{R_B N} > \det(I_N + A_{Y B})\}. \quad (10) \]

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

\[ \Psi(R_E, R_B) = (R_B - R_E)[1 - O_r(R_B)][1 - O_s(R_E)], \quad (11) \]

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

\[ \Psi_1(R_E) = (C_B - R_E)[1 - O_s(R_E)]. \quad (12) \]

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

\[ R_{E,1}^* = \arg \max_{0 < R_E < C_B} \Psi_1(R_E). \quad (13) \]

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

\[ \Psi_2(R_E, R_B) = (R_B - R_E)[1 - O_r(R_B)][1 - O_s(R_E)]. \quad (14) \]

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

\[ (R_{B,2}^*, R_{E,2}^*) = \arg \max_{0 < R_B, 0 < R_E < R_B} \Psi_2(R_B, R_E). \quad (15) \]

As a result, the maximum effective secrecy throughput is \(\Psi_2^* = \Psi_2^*(R_{B,2}^*, R_{E,2}^*)\).

**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, \(P_T \in [20, 30] \text{ dBm}\), the frequency band 1.7 – 86 MHz, and \(N = 1727\) are adopted.

Furthermore, in this study, \(\Psi_1^*\) and \(\Psi_2^*\) 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.
Likewise, regarding the hybrid PLC-WLC CFRs, it can be seen that \( \bar{\Psi}_1^{\text{WLC}} \) and \( \bar{\Psi}_2^{\text{WLC}} \) are higher than \( \bar{\Psi}_1^{\text{PLC}} \) and \( \bar{\Psi}_2^{\text{PLC}} \) for all eavesdroppers. Moreover, 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 for the LP scenario. Furthermore, LP yields higher values of \( \bar{\Psi}_1 \) and \( \bar{\Psi}_2 \) 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 a PLC or a hybrid PLC/WLC eavesdropper located far from Alice and near Bob. For instance, when \( P_T = 30 \text{ dBm} \), \( \bar{\Psi}_1^* = 2.09 \) and 0.19 b/s/Hz and \( \bar{\Psi}_2^* = 1.40 \) and 0.1 b/s/Hz are found for LP and SP scenarios when Eve is a PLC device, respectively. Also \( \bar{\Psi}_1^* = 0.89 \) and 0.06 b/s/Hz and \( \bar{\Psi}_2^* = 0.39 \) 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 \( \bar{\Psi}_1^* = 0.37 \) and 0 b/s/Hz and \( \bar{\Psi}_2^* = 0.15 \) and 0 b/s/Hz for the LP and SP scenarios, respectively.

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 \( \Psi_1^* \) for SP than the ones found for LP. Also, higher

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

In Fig. 4, when 90\textsuperscript{th} and 10\textsuperscript{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\textsuperscript{th} percentile are found in SP and LP scenarios, respectively, and \( \bar{G}_l = -27.8 \) and -16.7 dB are observed for 10\textsuperscript{th} percentile, respectively. Likewise, regarding the hybrid PLC-WLC CFRs, it can be seen that \( \bar{G}_l = -28.3 \) and -36.4 dB for SP and LP scenarios, respectively, for 90\textsuperscript{th} percentile and \( \bar{G}_l = -36.9 \) and -48.8 dB, respectively, for 10\textsuperscript{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.
the adoption of $P_T = 30$ dBm, one sees $R_{E,1}^* = 8.63$ 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
is a PLC device, respectively. Regarding the hybrid PLC/WLC eavesdropper, $R_{E,2}^*$ and $R_{B,2}^*$ versus total transmission power, $P_T$. (a) $R_{E,2}^* \times P_T$. (b) $R_{B,2}^* \times P_T$.

![Diagram showing wiretap code rates versus total transmission power.](image)

**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) $R_{E,2}^* \times P_T$.

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, PLC, and WLC 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**


