

On the Statistical Behavior of CP-Based Artificial Noise at the Receiver-Side in PLC Systems

Gustavo M. Campos, Mateus de L. Filomeno, and Moisés V. Ribeiro

Abstract—This paper analyzes the statistical behavior of the cyclic prefix (CP)-based artificial noise (AN) from the eavesdropper’s perspective to evaluate physical-layer security in power line communication (PLC) systems. The received AN is modeled as a random vector, and its analysis is based on the derivation of first- and second-order statistical moments. Numerical results across narrowband and broadband PLC channels show that, despite being theoretically zero-mean, residual structures emerge in practice. Moreover, the analysis reveals that the transmitter’s null-space projection introduces non-negligible cyclic correlation patterns. These structural characteristics indicate that the received AN is not strictly random, representing a critical vulnerability that an eavesdropper could potentially exploit to perform a security breach.

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

I. INTRODUCTION

The inherent broadcast nature of power line communication (PLC) systems raises critical security and privacy concerns. Since the medium is shared between the users in the network, any device connected to the same electric power grid can potentially intercept sensitive messages. To prevent information leakage, cryptography is generally the first option. However, the requirement for key management may render it unsuitable for resource-constrained scenarios, such as those involving Internet of Things (IoT) devices. Against this backdrop, physical layer security (PLS) has emerged as an alternative strategy that capitalizes on the medium’s time, frequency, or spatial diversity to enhance the secrecy [1].

Fundamentally, PLS aims to ensure that the legitimate receiver achieves a higher channel capacity than the eavesdropper. A practical approach to guarantee this advantage is the injection of artificial noise (AN), designed to degrade the eavesdropper’s signal-to-noise-ratio (SNR) without impairing legitimate communication. Within PLC networks, existing AN schemes tend to incur high computational complexity or reduce overall spectral efficiency [2], [3]. To circumvent these limitations, a simpler alternative originating from single-input single-output (SISO)-orthogonal

frequency-division multiplexing (OFDM) exploits the temporal degrees of freedom introduced by the cyclic prefix (CP) [4].

Building on this concept, the authors in [5] analyzed this CP-based AN in PLC systems, showing its effectiveness against near eavesdroppers. This technique operates by projecting the AN into the null space of the legitimate multipath channel. However, this null-space projection inherently forces the resulting AN samples to exhibit structural correlation. While essential for preserving the legitimate signal, this correlation introduces a critical security vulnerability. As highlighted by the authors in [6], an eavesdropper could potentially exploit these statistical patterns to estimate and mitigate the disruptive impact of the AN. Also, in [6], the authors investigated the statistical behavior of the CP-based AN for the PLC system, focusing on the transmitter side, which, unfortunately, does not reveal how it behaves from the eavesdropper’s perspective. In other words, the statistical properties of this AN, particularly once it propagates through the channel and reaches a malicious node, remain unexplored and need to be pursued.

To address this gap, this paper conducts a statistical analysis of the CP-based AN from the eavesdropper’s perspective. By modeling the AN received by a malicious node as a random vector and deriving its first- and second-order statistical moments, we investigate whether this structural correlation creates exploitable vulnerabilities. Ultimately, by evaluating these properties across narrowband (9 – 500 kHz) and broadband (1.7 – 86 MHz) PLC channels, this work assesses the extent to which these statistical patterns compromise the intended security.

Notation: $\mathbb{E}\{\cdot\}$ denotes the expectation operator, while $(\cdot)^T$ and $(\cdot)^\dagger$ denote the transpose and Hermitian operators, respectively. Furthermore, $\mathbf{0}_{c \times d}$ stands for an $(c \times d)$ -size matrix of zeros, whereas $\mathbf{I}_c$ is a c -size identity matrix.

II. PROBLEM FORMULATION

This section presents the formulation for a baseband communication system adopting the discrete-time wiretap channel model [5], where a legitimate transmitter, Alice, sends confidential information to a receiver, Bob, while an eavesdropper, Eve, seeks to intercept it. The transmission employs a CP-based structure, in which a CP is appended to each block to avoid interblock interference and facilitate intersymbol interference (ISI) mitigation. This system model is designed to encompass different digital modulation techniques, such as OFDM, orthogonal chirp-division multiplexing (OCDM), and single carrier with cyclic prefix (SC-CP).

This work was supported in part by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) under grants 312908/2025-3 and 445958/2024-3, Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG) under grants APQ-04623-22 and APQ-05901-25.

Gustavo M. Campos, Mateus de L. Filomeno, and Moisés V. Ribeiro are with the Electrical Engineering Department, Federal University of Juiz de Fora (UFJF), Juiz de Fora, MG 36036-900, Brazil, (e-mail: gustavo.moraes@estudante.ufjf.br, mateus.filomeno@ufjf.br, moises.ribeiro@ufjf.br).

Alice and Bob communicate over a PLC channel, which is modeled as an linear time-invariant (LTI) system impaired by additive noise. Since PLC requires baseband transmission, the transmitted block symbols must have a real-valued representation in the discrete-time domain. In this context, let $\mathbf{x}_i' \in \mathbb{R}^{N \times 1}$ denote the vector representation of the i^{th} transmitted information block in the discrete-time domain. After CP insertion, the vector representation of the real-valued transmitted information block is given by $\mathbf{x}_i = \Psi_T \mathbf{x}_i'$, where the matrix $\Psi_T = [\mathbf{E}_{L_{cp} \times N}^T \mathbf{I}_N]^T$ is responsible for the CP insertion, with L_{cp} indicating the CP-length and $\mathbf{E}_{L_{cp} \times N} = [\mathbf{0}_{L_{cp} \times (N-L_{cp})} \mathbf{I}_{L_{cp}}]$.

Alice sends the information block $\mathbf{x}_i$ along with a AN random vector $\mathbf{a}_i \in \mathbb{R}^{(N+L_{cp}) \times 1}$. This composite block is transmitted through distinct communication channels to Bob and Eve, indexed as “b” and “e”, respectively. Furthermore, the channel convolution matrix associated with user l can be described by a Toeplitz matrix $\mathbf{H}^l \in \mathbb{R}^{(N+L_{cp}) \times (N+L_{cp})}$, where $l \in \{b, e\}$. Assuming perfect synchronization, the i^{th} received block for user l in the discrete-time domain can be expressed as $\mathbf{y}_i^l = \mathbf{H}^l(\mathbf{x}_i + \mathbf{a}_i) + \mathbf{w}_i^l$, $\forall l \in \{b, e\}$, in which $\mathbf{w}_i^l \in \mathbb{R}^{(N+L_{cp}) \times 1}$ denotes the additive noise vector affecting the i^{th} symbol block of user l .

Next, the user l removes the CP from $\mathbf{y}_i^l$. Consequently, the vector representation of the i^{th} block received by the user l is given by

$$\begin{aligned} \mathbf{y}_i^l &= \Psi_R \mathbf{y}_i^l \\ &= \Psi_R \mathbf{H}^l \mathbf{x}_i + \Psi_R \mathbf{H}^l \mathbf{a}_i + \Psi_R \mathbf{w}_i^l, \end{aligned} \quad (1)$$

with the matrix $\Psi_R = [\mathbf{0}_{N \times L_{cp}} \mathbf{I}_N]$ being responsible for the CP removal.

As shown in (1), both users receives an additional interference term associated with the AN, given by $\Psi_R \mathbf{H}^l \mathbf{a}_i$. Ideally, Alice must design the AN vector $\mathbf{a}_i$ so that its convolution with Bob’s channel (*i.e.*, $\mathbf{H}^b$) results in a null vector, which should not be the case for Eve’s channel. Developing this further, the approach investigated in [4] exploits the degrees of freedom introduced by the CP, employing the matrix $\Psi_R \mathbf{H}^b \in \mathbb{R}^{N \times (N+L_{cp})}$ to project the AN vector. This technique allows the AN vector to be given by

$$\mathbf{a}_i = \mathbf{V}_{\text{null}}^b \mathbf{d}_i, \quad (2)$$

such that $\mathbf{d}_i \in \mathbb{R}^{L_{cp} \times 1}$ is a vector of independent Gaussian random variables and $\mathbf{V}_{\text{null}}^b \in \mathbb{R}^{(N+L_{cp}) \times L_{cp}}$ defines the right null space of $\Psi_R \mathbf{H}^b$, *i.e.*, $\Psi_R \mathbf{H}^b \mathbf{V}_{\text{null}}^b = \mathbf{0}_{N \times L_{cp}}$. Note that to design the AN vector $\mathbf{a}_i$, Alice needs to obtain the channel impulse response (CIR) of Bob, which can be accomplished, for instance, via a feedback channel. Then, $\mathbf{H}^b$ is constructed, and the matrix $\mathbf{V}_{\text{null}}^b$ is computed via singular value decomposition (SVD).

Therefore, if the AN vector $\mathbf{a}_i$ is correctly designed, it is expected that the i^{th} block received by Bob and Eve will be given, respectively, by

$$\mathbf{y}_i^b = \Psi_R \mathbf{H}^b \mathbf{x}_i + \Psi_R \mathbf{w}_i^b \quad (3)$$

and

$$\mathbf{y}_i^e = \Psi_R \mathbf{H}^e \mathbf{x}_i + \Psi_R \mathbf{H}^e \mathbf{a}_i + \Psi_R \mathbf{w}_i^e. \quad (4)$$

Note that the resulting block received by Eve has an additional noise vector, $\Psi_R \mathbf{H}^e \mathbf{a}_i$, which will impair its SNR.

Nevertheless, since the AN vector $\mathbf{a}_i$ is constructed using (2), its statistical properties are inherently determined by the structure of the matrix $\mathbf{V}_{\text{null}}^b$. Although the vector $\mathbf{d}_i$ comprises uncorrelated random variables, the transformation applied by $\mathbf{V}_{\text{null}}^b$ can introduce correlation among the elements of the AN vector $\mathbf{a}_i$. Furthermore, Eve’s channel ($\Psi_R \mathbf{H}^e$) further transforms this AN, altering its interference profile. This composite transformation may potentially allow Eve to exploit its structure to mitigate its disruptive impact. To assess this vulnerability, the following section analyzes the AN as a random vector through its first- and second-order statistics.

III. ANALYSIS OF THE RECEIVED AN AS A RANDOM VECTOR

The AN can be modeled as a random vector projected onto the null space of Bob’s CIR. However, this projection introduces correlation patterns that an eavesdropper might exploit to mitigate the jamming effect. Consequently, this section describes an investigation of the statistical behavior of the received CP-based AN. The investigation models the AN as a vector and derives its first- and second-order statistical moments (specifically, the expectation vector and the autocorrelation matrix).

From Eve’s standpoint, the received AN vector can be written as

$$\begin{aligned} \mathbf{z}_i^e &= \mathbf{H}^e \mathbf{a}_i \\ &= \mathbf{H}^e \mathbf{V}_{\text{null}}^b \mathbf{d}_i. \end{aligned} \quad (5)$$

As this additional noise vector is also a random vector, let $\mathbf{z}_i^e$ denote the i^{th} sample function of this random vector, corresponding to the AN vector observed by Eve during the i^{th} received symbol block.

A. Expectation

The expectation of the AN vector received by Eve is given by

$$\boldsymbol{\mu}_z^e = \mathbb{E}\{\mathbf{z}_i^e\}. \quad (6)$$

Although the PLC channel is inherently random and slowly time-varying, its null-space $\mathbf{V}_{\text{null}}^b$ is treated as deterministic. This holds under the assumption that the AN vector generation occurs within the coherence time of the PLC channel, during which its properties and characteristics remain time-invariant. Assuming that $\mathbf{H}^e$ also remains invariant within the channel’s coherence time, the entire composite matrix $\mathbf{H}^e \mathbf{V}_{\text{null}}^b$ can be treated as deterministic for this analysis. Consequently, the expectation boils down to

$$\begin{aligned} \boldsymbol{\mu}_z^e &= \mathbb{E}\{\mathbf{H}^e \mathbf{V}_{\text{null}}^b \mathbf{d}_i\} \\ &= \mathbf{H}^e \mathbf{V}_{\text{null}}^b \mathbb{E}\{\mathbf{d}_i\}. \end{aligned} \quad (7)$$

Since $\mathbf{d}_i$ is a zero-mean random vector, it follows that

$$\boldsymbol{\mu}_z^e = \mathbf{0}_{(N+L_{cp}) \times 1}. \quad (8)$$

Hence, the received AN vector by Eve is a zero-mean random vector. This result sets the stage for evaluating the autocorrelation matrix.

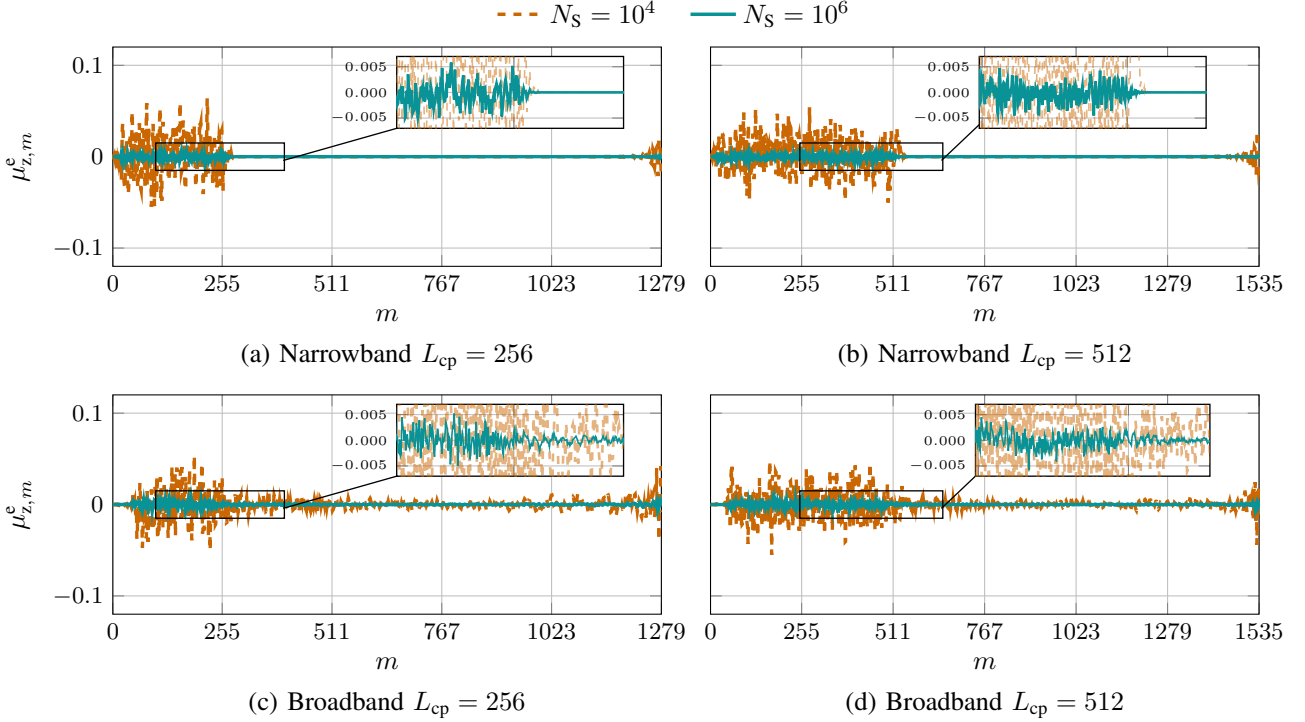


Fig. 1. Expectation of the received AN by Eve for the narrowband and broadband PLC channels, estimated with varying N_S and evaluated for different L_{cp} values. Here $\mu_{z,m}^e$ represents the m^{th} element of μ_z^e .

B. Autocorrelation Matrix

The autocorrelation matrix of a random vector is a deterministic matrix that quantifies the temporal dependence between elements of the vector at different lags. For the AN vector received by Eve, it is expressed as

$$\mathbf{R}_{zz}^e = \mathbb{E}\{\mathbf{z}_i^e(\mathbf{z}_i^e)^\dagger\}, \quad (9)$$

which is a symmetric and positive-definite matrix. By substituting (5) into (9), one obtains

$$\begin{aligned} \mathbf{R}_{zz}^e &= \mathbb{E}\{(\mathbf{H}^e \mathbf{V}_{\text{null}}^b \mathbf{d}_i)(\mathbf{H}^e \mathbf{V}_{\text{null}}^b \mathbf{d}_i)^\dagger\} \\ &= \mathbf{H}^e \mathbf{V}_{\text{null}}^b \mathbf{\Lambda}_{\sigma_d^2} \mathbf{V}_{\text{null}}^{b\dagger} (\mathbf{H}^e)^\dagger. \end{aligned} \quad (10)$$

in which $\mathbf{\Lambda}_{\sigma_d^2} = \mathbb{E}\{\mathbf{d}_i \mathbf{d}_i^\dagger\}$, is a diagonal matrix that stands for the correlation matrix of the AN vector $\mathbf{a}_i$.

The knowledge of (8) states that the autocorrelation and autocovariance matrices are equivalent. To quantify the correlation between the elements of the AN vector at Eve, the correlation coefficient is utilized, which is given by

$$\rho_{zz}^e[m, n] = \frac{R_{zz}^e[m, n]}{\sqrt{R_{zz}^e[m, m] R_{zz}^e[n, n]}}, \quad (11)$$

$\forall m, n \in \{0, 1, \dots, (N + L_{cp}) - 1\}$, in which $R_{zz}^e[m, n]$ is the correlation between m^{th} and n^{th} elements of the vector $\mathbf{z}_i^e$. Note that $-1 \leq \rho_{zz}^e[m, n] \leq 1$.

The main diagonal elements of the autocorrelation matrix $\mathbf{R}_{zz}^e$ represent the variances of the AN vector $\mathbf{z}_i^e$. These variances can be collected into a vector given by $\sigma_{e,z}^2 = [\sigma_{e,z,0}^2, \sigma_{e,z,1}^2, \dots, \sigma_{e,z,N+L_{cp}-1}^2]^\top$, in which $\sigma_{e,z,m}^2 = R_{zz}^e[m, m]$.

IV. NUMERICAL RESULTS AND DISCUSSIONS

This section numerically evaluates and analyzes the expectation vector and autocorrelation matrix of the AN impinging on the eavesdropper. While the transmitted AN vector exhibits specific statistical structures [6], understanding how these statistics transform after propagating through the wiretap channel is crucial. Therefore, this analysis focuses exclusively on the received AN vector observed by the eavesdropper.

In this sense, two distinct PLC bandwidths are considered: narrowband (3 – 500 kHz) and broadband (1.7 – 100 MHz). In the broadband case, the Alice-Eve PLC CIR is obtained from [7]. For the narrowband case, the CIR is based on the multi-path model [8] using IEEE 1901.2 Standard parameters [9]. However, because this synthetic narrowband model yields independent channel realizations, it fails to capture the shared-medium nature of the PLC wiretap channel. To overcome this limitation, spatial correlation between the legitimate and wiretap links is synthesized following [10], which cascades a shared common CIR with the independent CIRs of the respective users' branches.

For the statistical analysis, the received AN random vector is evaluated over independent and identically distributed realizations, assuming $i \in \{1, \dots, N_S\}$, with $N_S \in \{10^4, 10^6\}$, $N = 1024$, and $L_{cp} \in \{256, 512\}$. The expectation vector and autocorrelation matrix for Eve's received noise are estimated based on (6) and (9), respectively. The expectation operator is performed by a conventional unbiased sample mean estimator, and the autocorrelation matrix is obtained from an unbiased covariance estimator over the N_S realizations.

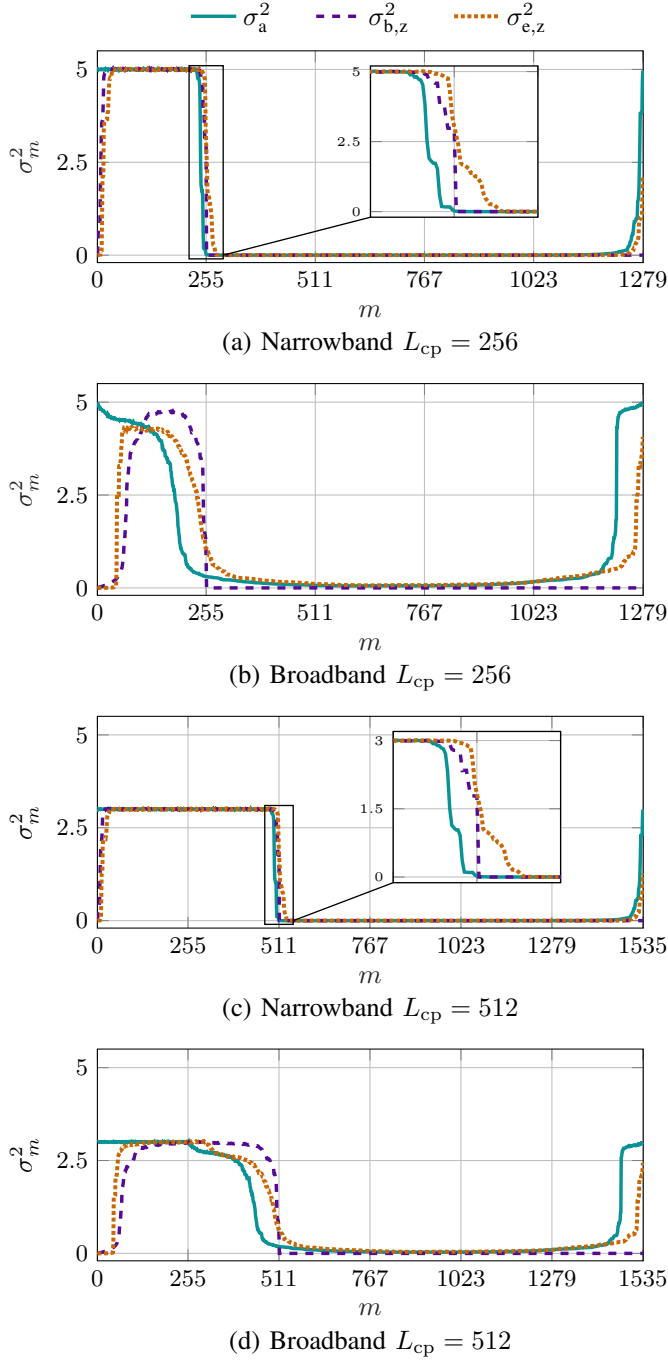


Fig. 2. Variance of the transmitted and received AN vectors for the narrowband and broadband PLC channels, estimated over $N_S = 10^6$ and evaluated under different values of L_{cp} . In this figure, σ_m^2 denotes the m^{th} element of the variance vectors associated with σ_a^2 , $\sigma_{e,z}^2$, and $\sigma_{b,z}^2$.

From the eavesdropper's perspective, if the statistical structures of the transmitted AN [6] are preserved at the PLC channel output, they constitute an exploitable security vulnerability. First, the expectation of the received AN vector at Eve is investigated. Fig. 1 depicts the unbiased estimate of the expectation vector, μ_z^e , as a function of the sample index m for $N_S \in \{10^4, 10^6\}$. Specifically, Figs. 1(a) and (b) correspond to the narrowband PLC channel with $L_{cp} = 256$ and $L_{cp} = 512$, respectively, whereas Figs. 1(c) and (d)

show the corresponding estimates for the broadband PLC channel. The results reveal that convolution with the wiretap channel alters the statistics of the transmitted AN vector but fails to eliminate them. Indeed, for $N_S = 10^4$, the estimated expectation exhibits pronounced non-zero values. In the narrowband scenarios, this effect is highly concentrated within the CP block because the CIR focuses energy into a few highly correlated taps. Conversely, the diffuse multipath nature of the broadband channel smears these non-zero values across a larger portion of the samples. For $N_S = 10^6$, the expectation vector converges much closer to zero across all investigated scenarios, although minor deviations persist within the CP interval. Notably, the non-zero expectations outside the CP block are finite-sample estimation artifacts. Since they rapidly converge to zero as N_S increases, exploiting these fluctuations would be impractical for Eve.

The presence or absence of residual structure in the estimated expectation vector shows how energy is distributed across the transmitted and received AN vectors. In this context, Fig. 2 shows the variance for both the narrowband and broadband PLC channels, computed with $N_S = 10^6$ across different CP block durations ($L_{cp} \in \{256, 512\}$). In these plots, the variance of the transmitted AN (σ_a^2) is contrasted with the noise variances of the received AN vectors observed by Eve ($\sigma_{e,z}^2$) and Bob ($\sigma_{b,z}^2$). Note that, after the AN vector undergoes the PLC channel, the high values of variance are mostly concentrated over the CP block duration at the legitimate receiver. As can be observed, the eavesdropper also experiences a relatively high variance over the CP interval due to the inherent spatial correlation between the Alice-Bob and Alice-Eve channels. However, note that the residual AN leakage into Eve's data block remains sufficient to degrade her reception quality, contrasting with the legitimate receiver. Consequently, Bob can effectively eliminate the interference associated with the received AN vector simply by discarding the CP, without the need for additional processing. On the other hand, at Eve, the energy of the received AN vector spills over into the data symbol block. This leakage corrupts the data symbols, thereby degrading SNR.

Finally, the autocorrelation matrix of the received AN vector observed by Eve is analyzed. In this regard, Fig. 3 shows the heatmaps of the correlation matrix estimated over $N_S = 10^6$ samples, considering different CP lengths ($L_{cp} \in \{256, 512\}$). For the narrowband PLC channel, shown in Figs. 3(a) and (c), the correlation structure remains remarkably similar to that of the transmitter AN vector previously investigated by the authors in [6]. Correlation patterns are preserved extending beyond the CP block duration, indicating that the low dispersion of the narrowband PLC channel introduces minimal distortion to the temporal dependencies of the received AN vector. Conversely, for the broadband PLC channel in subfigures (b) and (d), the dispersive nature of the medium significantly alters the correlation profile. Notably, these matrices exhibit distinct high-magnitude values that recur in a cyclical pattern. This behavior is particularly evident for the shortest CP length ($L_{cp} = 256$), where significant correlation permeates even the CP block duration. Ultimately, these correlation characteristics may pose a

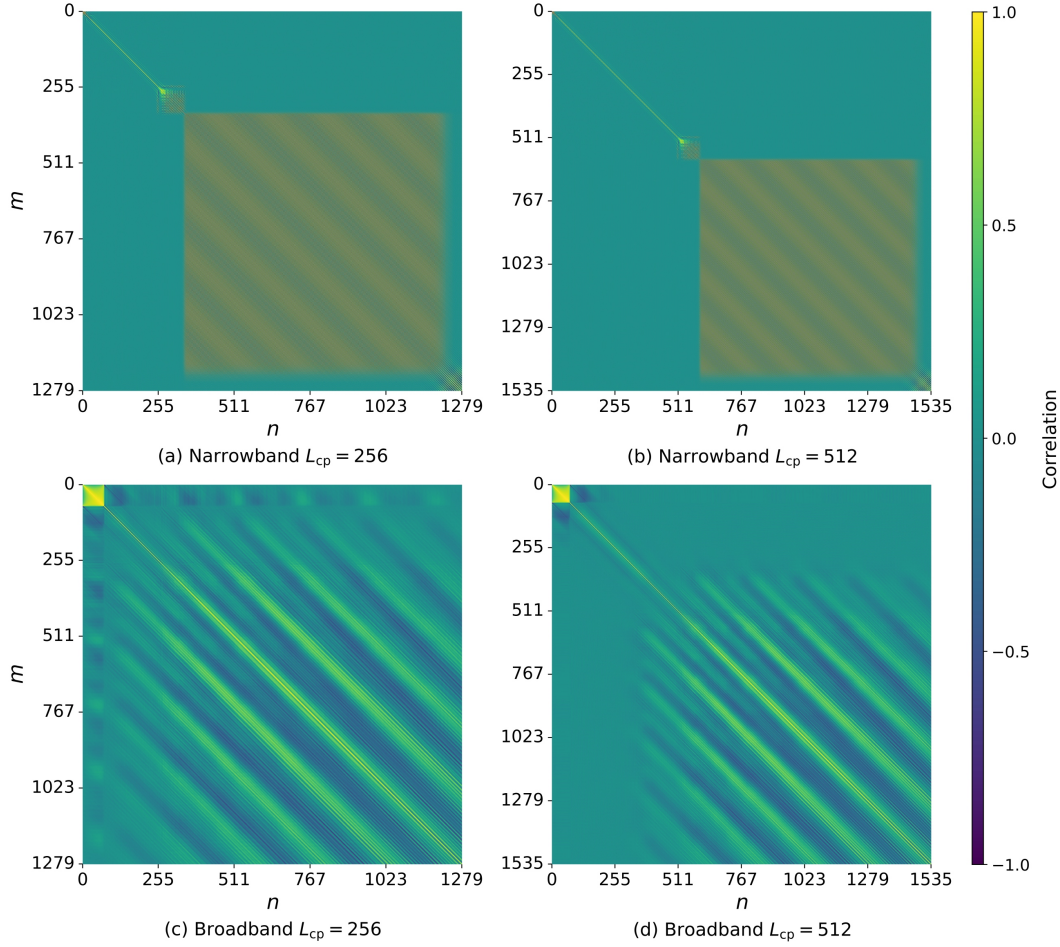


Fig. 3. Heatmap of the correlation matrix of the received AN vector by Eve for the narrowband and broadband PLC channels, for different values of L_{cp} .

security vulnerability, as their structured and persistent nature could enable Eve to develop advanced signal-processing or guesswork countermeasures against AN-based protection.

V. CONCLUSIONS

This paper investigated the statistical behavior of CP-based AN from the eavesdropper's perspective in both narrowband and broadband PLC systems. Modeling the received AN at an eavesdropper as a random vector and deriving its first- and second-order moments reveals that the transmitter's null-space projection introduces non-negligible structural correlations that persist after channel propagation. While this approach successfully confines the AN energy to the CP interval for the legitimate receiver, it leaks into the eavesdropper's data block to degrade SNR. The resulting cyclic correlation patterns indicate that the AN is not strictly random. Consequently, this structural persistence represents a critical vulnerability that malicious nodes could exploit to perform a security breach. Future works will investigate specific eavesdropper countermeasures based on these exploitable statistical patterns.

REFERENCES

- [1] A. Pittolo and A. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Commun.*, vol. 8, pp. 1239–1247, May 2014.
- [2] A. El Shafie, M. F. Marzban, R. Chabaan, and N. Al-Dhahir, "An artificial-noise-aided secure scheme for hybrid parallel PLC/wireless OFDM systems," in *Proc. IEEE Int. Conf. Commun.*, 2018, pp. 1–6.
- [3] A. Salem, K. A. Hamdi, and E. Alsusa, "Physical layer security over correlated log-normal cooperative power line communication channels," *IEEE Access*, vol. 5, pp. 13 909–13 921, 2017.
- [4] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wirel. Commun.*, vol. 12, no. 6, pp. 2717–2729, June 2013.
- [5] M. de L. Filomeno, G. M. Campos, Á. Camponogara, P. H. Sartorello, and M. V. Ribeiro, "Artificial noise for in-home PLC networks under the presence of PLC and wireless eavesdroppers," in *Symp. Internet Things*, Oct. 2023, pp. 1–5.
- [6] G. M. Campos, M. de L. Filomeno, A. M. Tonello, and M. V. Ribeiro, "Statistical analysis of CP-based artificial noise in narrowband and broadband PLC systems," in *XLI Braz. Symp. Telecommun. Signal Process.*, Sep. 2025, pp. 1–6.
- [7] 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.
- [8] M. Zimmermann and K. Dostert, "A multipath model for the powerline channel," *IEEE Trans. on Commun.*, vol. 50, no. 4, pp. 553–559, Apr. 2002.
- [9] "IEEE Standard for low-frequency (less than 500 khz) narrowband power line communications for smart grid applications," *IEEE Std 1901.2-2013*, pp. 1–269, 2013.
- [10] Á. 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, 2019.