UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE ENGENHARIA
ENGENHARIA ELÉTRICA - TELECOMUNICAÇÕES

Gustavo Moraes Campos

Ruído artificial para redes PLC residenciais sob a presença de intrusos PLC e sem fio

Juiz de Fora
2023

Gustavo Moraes Campos

Ruído artificial para redes PLC residenciais sob a presença de intrusos PLC e sem fio

Monografia apresentada à Coordenação do Curso de Engenharia Elétrica - Telecomunicações da Universidade Federal de Juiz de Fora, como requisito para aprovação na disciplina ENE064 - Trabalho Final de Curso.

Orientador: Prof. Dr. Moisés Vidal Ribeiro

Coorientador: Dr. Mateus de Lima Filomeno

Juiz de Fora

2023

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF com os dados fornecidos pelo(a) autor(a)

Campos, Gustavo Moraes.
Ruído artificial para redes PLC residenciais sob a presença de intrusos PLC e sem fio / Gustavo Moraes Campos. – 2023.
35 f. : il.

Orientador: Prof. Dr. Moisés Vidal Ribeiro
Coorientador: Dr. Mateus de Lima Filomeno
Trabalho de Conclusão de Curso – Universidade Federal de Juiz de Fora, Engenharia Elétrica - Telecomunicações. Faculdade de Engenharia, 2023.

1. Comunicação híbrida. 2. Comunicação via rede de energia elétrica. 3. Ruído artificial. 4. Segurança da camada física. I. Ribeiro, Moisés Vidal, orient. II. Filomeno, Mateus de Lima, coorient. III. Título.

Gustavo Moraes Campos

Ruído artificial para redes PLC residenciais sob a presença de intrusos PLC e sem fio

Monografia apresentada à Coordenação do Curso de Engenharia Elétrica - Telecomunicações da Universidade Federal de Juiz de Fora, como requisito para aprovação na disciplina ENE064 - Trabalho Final de Curso.

Aprovada em 14 de Dezembro de 2023

BANCA EXAMINADORA

Prof. Dr. Moisés Vidal Ribeiro - Orientador
Universidade Federal de Juiz de Fora

Dr. Mateus de Lima Filomeno - Coorientador
Universidade Federal Juiz de fora

Ma. Cláudia de Magalhães Santos Fonseca
Universidade Federal Juiz de fora

Ms. Túlio Fernandes Moreira
Universidade Federal Juiz de fora

À minha família, amigos, orientadores, e aos meus colegas do LCOM.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer a minha família, especialmente a minha mãe, Márcia Irene Moraes Campos, ao meu pai, Homero de Lima Campos, e a minha irmã Maria Gabriela Moraes Campos, por todo o apoio que me deram ao longo desses anos de vida e graduação.

Gostaria de agradecer também aos meus amigos de graduação, com os quais compartilhei as alegrias e dificuldades da faculdade de engenharia. Agradeço também aos meus colegas do Laboratório de Comunicações pela atenção e disposição em ajudar durante minha iniciação científica. Em particular, agradeço ao Dr. Mateus de Lima Filomeno por toda paciência, ensinamentos e orientações que contribuíram para o meu desenvolvimento.

Agradeço também ao meu orientador, Prof. Dr. Moisés Vidal Ribeiro, pela oportunidade de trabalhar no Laboratório de Comunicações e pela orientação na confecção deste trabalho. Sou grato também à banca examinadora, por aceitar avaliar este trabalho e contribuir com sugestões e comentários.

Também agradeço a todos os professores e funcionários da Universidade Federal de Juiz de Fora, pela contribuição e apoio à minha formação acadêmica e profissional.

Por fim, gostaria de agradecer a Deus.

“... mas eu posso estar errado.”

- Carl Sagan

RESUMO

Neste trabalho investiga-se um ruído artificial projetado com base nos graus de liberdade do prefixo cíclico para aumentar a segurança de redes de comunicação via rede de energia elétrica (do inglês, *power line communication*)(PLC) residenciais. O ruído artificial é gerado para prejudicar a capacidade de decodificação de diversos intrusos, que podem ser dispositivos PLC ou sem fio, sem afetar a decodificação dos dados feita por receptores legítimos. Inicialmente, o modelo do sistema para a transmissão e recepção de informação é apresentado, considerando o esquema de multiplexação por divisão de frequências ortogonais Hermitiano simétrico. Em seguida, descreve-se cuidadosamente o projeto do ruído artificial, baseado nos graus de liberdade introduzidos pelo prefixo cíclico, e as expressões para a relação sinal-ruído do receptor legítimo e dos intrusos. Resultados numéricos obtidos a partir de dados medidos mostram que a técnica de injeção de ruído artificial considerada é mais eficaz nos cenários mais ameaçadores às redes PLC, que se referem àqueles com intrusos PLC próximos ao transmissor legítimo. Ainda, a análise do sinal transmitido indica que o ruído artificial aumenta a razão entre a potência de pico e a potência média de forma expressiva, independentemente do canal considerado no projeto e do esquema de modulação utilizado para a transmissão de informação.

Palavras-chave: comunicação híbrida, comunicação via rede de energia elétrica, ruído artificial, segurança da camada física.

ABSTRACT

In this study, we investigate an artificial noise designed based on the degrees of freedom of the cyclic prefix to enhance the security of in-home power line communication (PLC) networks. The artificial noise is generated to impair the decoding capability of various eavesdroppers, whether they are PLC or wireless devices, without affecting the decoding of data by legitimate receivers.

Initially, we present the system model for the transmission and reception of information, considering the Hermitian symmetric orthogonal frequency-division multiplexing scheme. Next, we meticulously describe the design of the artificial noise based on the degrees of freedom introduced by the cyclic prefix and the expressions for the signal-to-noise ratio of both the legitimate receiver and eavesdroppers. Numerical results derived from measured data demonstrate that the considered artificial noise technique is more effective in more threatening scenarios to PLC networks, specifically those with PLC eavesdroppers close to the legitimate transmitter. Furthermore, analysis of the transmitted signal indicates that the artificial noise significantly increases the peak-to-average power ratio, regardless of the channel used to design it and the modulation scheme assumed to transmit information.

Keywords: artificial noise, hybrid communication, physical layer security, power line communication.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AN	ruído artificial (do inglês, *artificial noise*)
AWGN	ruído Gaussiano branco aditivo (do inglês, *additive white Gaussian noise*)
BER	taxa de erro de bit (do inglês, *bit error rate*)
CCDF	função de distribuição cumulativa complementar (do inglês, *complementary cumulative distribution function*)
CIR	resposta ao impulso do canal (do inglês, *channel impulse response*)
CP	prefixo cíclico (do inglês, *cyclic prefix*)
DFT	transformada discreta de Fourier (do inglês, *discrete Fourier transform*)
IDFT	transformada discreta de Fourier inversa (do inglês, *inverse discrete Fourier transform*)
ISI	interferência intersimbólica (do inglês, *intersymbol interference*)
LP	caminho longo (do inglês, *long-path*)
LTI	linear e invariante no tempo (do inglês, *linear time-invariant*)
MIMO	múltiplas entradas e múltiplas saídas (do inglês, *multiple-input multiple-output*)
OFDM	multiplexação por divisão de frequências ortogonais (do inglês, *orthogonal frequency-division multiplexing*)
PAM	modulação por amplitude de pulso (do inglês, *pulse-amplitude modulation*)
PAPR	razão entre a potência de pico e a potência média (do inglês, *peak-to-average power ratio*)
PLC	comunicação via rede de energia elétrica (do inglês, *power line communication*)
PLS	segurança da camada física (do inglês, *physical layer security*)
PSD	densidade espectral de potência (do inglês, *power spectral density*)
QAM	modulação de amplitude em quadratura (do inglês, *quadrature amplitude modulation*)
SC-CP	monoportadora com prefixo cíclico (do inglês, *single carrier with cyclic prefix*)
SISO	única entrada e única saída (do inglês, *single-input single-output*)
SNR	relação sinal-ruído (do inglês, *signal-to-noise ratio*)
SP	caminho curto (do inglês, *short-path*)
SVD	decomposição em valores singulares (do inglês, *singular value decomposition*)

LISTA DE SÍMBOLOS

$\mathbf{0}_{a\times b}$ Matriz de tamanho $(a \times b)$ completa de zeros

$\text{diag}\{\cdot\}$ Matriz diagonal preservando a diagonal principal da matriz de entrada

$\mathbf{I}_a$ Matriz identidade de tamanho a

$(\cdot)^*$ Operador conjugado complexo

$(\cdot)^\dagger$ Operador de transposição conjugada

$(\cdot)^{\mathrm{T}}$ Operador transposição

$\text{Tr}(\cdot)$ Operador traço

$\forall$ Para todo

$\mathfrak{I}\{\cdot\}$ Parte imaginária do número complexo

$\mathfrak{R}\{\cdot\}$ Parte real do número complexo

$\in$ Pertence

$\mathbb{E}\{\cdot\}$ Valor esperado de uma variável aleatória

$\mathbf{F} \in \mathbb{C}^{N\times N}$ Versão normalizada da matriz da transformada discreta de Fourier (do inglês, *discrete Fourier transform*) (DFT) de comprimento N

SUMÁRIO

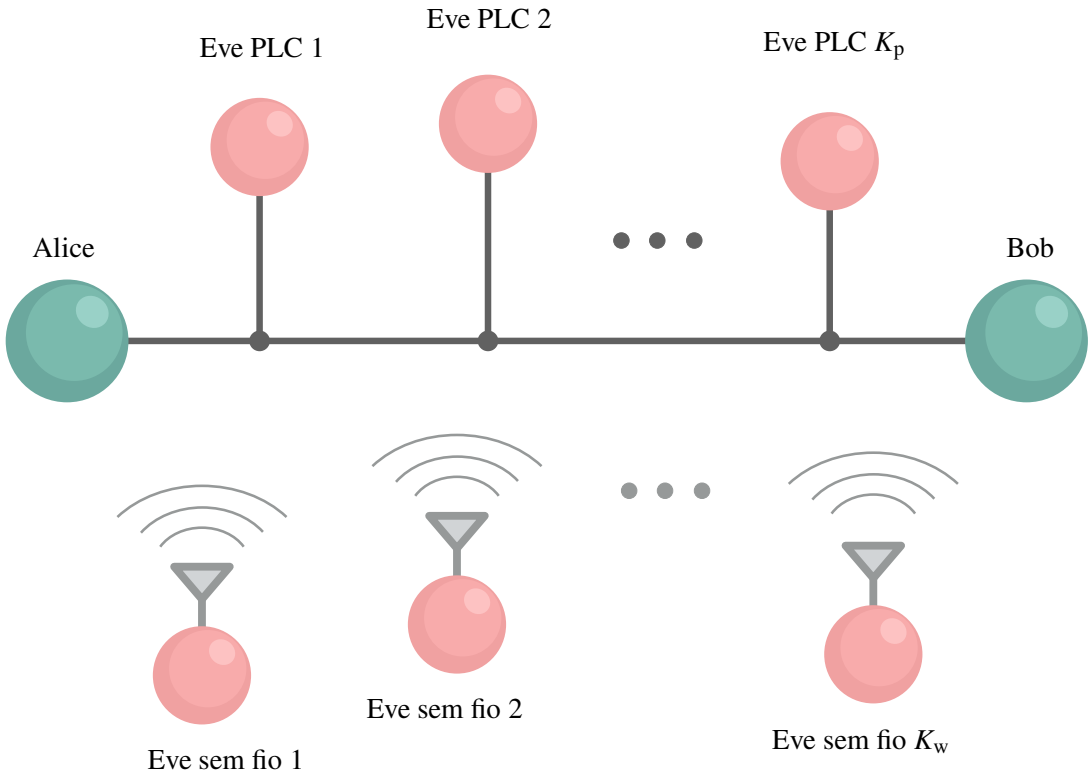
1 INTRODUÇÃO

A crescente demanda por conectividade entre dispositivos e pessoas está impulsionando a ampla adoção da Internet das Coisas (IoT), redes elétricas inteligentes, Indústria 4.0 e conceitos de cidades inteligentes. Isso está gerando esforços em âmbito global para desenvolver uma nova geração de infraestruturas de telecomunicações que sejam eficazes, confiáveis, energeticamente eficientes e de baixo consumo de energia [1]. Nesse contexto, o potencial das redes elétricas como meio de comunicação de dados foi reavivado nas últimas décadas, ao mesmo tempo em que a exploração de recursos subutilizados nessas redes para fins de comunicação de dados foi intensificado. De fato, a utilização da infraestrutura elétrica existente reduz significativamente os custos associados à implementação desse tipo de redes de dados. Além disso, a introdução do esquema de multiplexação por divisão de frequências ortogonais (do inglês, *orthogonal frequency-division multiplexing*) (OFDM) solidificou o status da comunicação via rede de energia elétrica (do inglês, *power line communication*) (PLC) como uma tecnologia viável para comunicação de dados em ambientes internos e externos.

Apesar das vantagens já bem conhecidas, como a ubiquidade, implementação de baixo custo e instalação fácil para níveis de baixa tensão, a rede de energia elétrica foi originalmente projetada para geração, transmissão e distribuição de energia ao invés de comunicação de dados. Assim, os sinais portadores de dados que trafegam pelas redes de energia elétrica enfrentam atenuações significativas devido ao aumento da distância e/ou frequência, ao efeito de multipercurso, às perdas de acoplamento e à interferência com outros sistemas de telecomunicações que operam na mesma faixa de frequência [2–6]. Ainda, a natureza *broadcast* da rede de energia elétrica levanta a possibilidade de vazamento de informação para um intruso PLC, enquanto o fato de que a maioria dos cabos de energia elétrica não são blindados eletricamente permite que um intruso sem fio próximo a eles capture os sinais PLC [6]. Portanto, existe a possibilidade de interceptação de informações privadas por intrusos PLC que recebem sinais do transmissor legítimo através da rede de energia elétrica e intrusos sem fio que recebem sinais do transmissor legítimo pelo ar, como ilustrado na Figura 1. Por convenção, o transmissor legítimo é chamado Alice e o receptor legítimo é nomeado Bob, enquanto que os K_{p} intrusos PLC e K_{w} intrusos sem fio são nomeados Eve PLC e Eve sem fio, respectivamente.

De forma a evitar o vazamento de informações privadas, criptografia é geralmente a primeira opção; no entanto, ela exige a troca de chaves criptográficas e, consequentemente, processamento e recursos de hardware adicionais. Nesse contexto, a segurança da camada física (do inglês, *physical layer security*) (PLS) surgiu como uma estratégia alternativa, aproveitando as propriedades do meio de comunicação e, portanto, não exigindo a troca de chaves criptográficas para aumentar a segurança da informação. Em outras palavras, a PLS visa aproveitar a diversidade nos domínios do tempo, frequência ou espaço para aumentar a segurança da informação [7].

Figura 1 – Cenário de uma rede PLC em que o transmissor legítimo (Alice) e receptor legítimo (Bob) se comunicam por meio da rede de energia elétrica, com a presença de intrusos PLC (Eve PLC) e intrusos sem fio (Eve sem fio).



Fonte: Acervo do autor.

O conceito de segurança no nível da camada física não é novo. Na década de 70, os primeiros estudos acerca de PLS emergiram, em que Wyner [8] abordou o modelo de canal *wiretap* degradado. Logo em seguida, Leung-Yan-Cheong & Hellman [9] analisaram a capacidade segura para o canal *wiretap* Gaussiano. De forma geral, a proposta da PLS é atingir uma capacidade no receptor legítimo que seja superior à do intruso. A partir dessa condição, pode-se empregar um tipo específico de código de canal, denominado código *wiretap*, que introduz simultaneamente aleatoriedade e redundância nos dados transmitidos. A aleatoriedade tem o propósito de impedir que o intruso decifre as informações de maneira correta, resultando em um aumento da taxa de equívoco, enquanto a redundância possibilita que o receptor legítimo remova erros causados pelo canal de comunicação.

No que diz respeito a sistemas PLC, esforços recentes tem explorado a PLS com uma distinção entre cenários de comunicação de única entrada e única saída (do inglês, *single-input single-output*) (SISO) [7, 10–17] e de múltiplas entradas e múltiplas saídas (do inglês, *multiple-input multiple-output*) (MIMO) [18, 19]. Para cenários MIMO, os autores em [18, 19] investigaram a PLS para sistemas PLC de banda larga utilizando canais teóricos. Inicialmente, Zhuang & Lampe [18], impulsionados pelas melhorias nas taxas de dados alcançadas nos sistemas PLC devido ao cenário MIMO, aprimoram a segurança no nível da camada física desses sistemas. Posteriormente, em [19], os autores dedicaram atenção à detecção de sinais

de interferência com o objetivo de reduzir a relação sinal-ruído (do inglês, *signal-to-noise ratio*) (SNR) de um receptor não legítimo em um sistema PLC.

Levando em consideração que a maioria das residências possui circuitos monofásicos, implementar tecnologias MIMO nessas condições pode ser complexo, ou até mesmo não realizável. Nesse contexto, o foco deste trabalho recai sobre o cenário SISO, em que a PLS tem sido objeto de investigação em diferentes configurações de redes. Dentre essas configurações, há as redes exclusivamente PLC [7, 10–12], cujo transmissor legítimo, o receptor legítimo e o intruso estão conectados por meio de cabos de energia elétrica. Além delas, há também redes híbridas PLC-sem fio [13–15], em que os nós legítimos se comunicam através de cabos de energia elétrica e o intruso é um dispositivo sem fio e, ainda, redes híbridas paralelas PLC/sem fio [16, 17], cujos nos legítimos podem estar conectados tanto por meio de cabos de energia elétrica quanto pelo meio sem fio e o intruso pode ser PLC, sem fio ou os dois.

De forma a avaliar o impacto de um intruso PLC, os autores de [7] e [10] consideraram dados de medição, enquanto modelos estatísticos foram adotados em [11]. Esses trabalhos demonstraram usando diferentes critérios e cenários que, devido à correlação existente entre os canais envolvidos, um intruso PLC pode ameaçar a segurança da troca de informações, indicando que soluções de PLS devem ser investigadas. No que diz respeito aos casos em que o intruso é um dispositivo sem fio, Camponogara *et al.* [13–15] estudaram métricas e cenários distintos, incluindo um com intrusos colaboradores [15]. Nesses casos, os canais do intruso e do receptor legítimo podem ser assumidos como menos correlacionados ou até mesmo não correlacionados entre si [15]. Para o caso das redes híbridas paralelas PLC/sem fio, em [16], os autores demonstraram que a diversidade PLC/sem fio apresenta vantagens consideráveis em relação à PLS para aplicações de baixa taxa de dados, especialmente quando o intruso utiliza apenas uma interface de comunicação de dados, seja PLC ou sem fio.

Ao analisar a literatura, fica clara a necessidade do estudo de técnicas de PLS para a rede PLC. Desse modo, tendo em vista que a ideia da PLS é ter a capacidade do receptor legítimo maior que a do intruso, uma abordagem prática para que o receptor legítimo alcance uma capacidade superior é a injeção de ruído artificial (do inglês, *artificial noise*) (AN). Este ruído deve ser gerado de forma inteligente para não degradar a SNR do receptor legítimo, mas reduzir efetivamente a SNR de qualquer intruso passivo. Shafie *et al.* [17], propôs um esquema auxiliado por AN para aprimorar a segurança do sistema de comunicação na presença de um intruso, explorando a natureza desacoplada dos meios de comunicação PLC e sem fio. Contudo, é importante notar que a natureza híbrida do sistema que os autores abordaram em [17] demanda mais recursos de hardware e uma maior complexidade computacional. Já Salem *et al.* [12] consideraram a injeção de AN em uma rede PLC e demonstraram que essa estratégia pode ajudar a reduzir de forma significativa os impactos negativos introduzidos por um intruso PLC. No entanto, os autores, consideraram um cenário cooperativo complexo com eficiência espectral reduzida, onde os nós de retransmissão devem estar sempre disponíveis.

Portanto, uma abordagem alternativa e mais simples deve ser avaliada. Em [20], os autores propuseram uma técnica que atende essa demanda. Considerando um sistema SISO OFDM, eles investigaram o uso dos graus de liberdade introduzidos pelo prefixo cíclico (do inglês, *cyclic prefix*) (CP) para projetar o AN. No entanto, a eficácia dessa técnica pode variar dependendo das condições do meio de comunicação, como propagação de sinal, interferência e níveis de ruído. Consequentemente, para fornecer garantias de segurança consistentes em diferentes cenários, essa técnica específica deve ser cuidadosamente analisada. Ademais, o AN gerado com base nos graus de liberdade do CP ainda não foi avaliado no contexto das redes PLC. Assim, é necessário avaliar se essa técnica pode aumentar a segurança das redes PLC residenciais na presença de intrusos passivos que podem ser dispositivos PLC ou sem fio.

1.1 OBJETIVOS

Com base no contexto apresentado, o presente trabalho possui os seguintes objetivos:

- Investigar a técnica de inserção de AN com base nos graus de liberdade introduzidos pelo CP para redes PLC residenciais. A técnica previamente proposta é estudada tanto em termos de taxa de erro de bit (do inglês, *bit error rate*) (BER) como em termos de razão entre a potência de pico e a potência média (do inglês, *peak-to-average power ratio*) (PAPR).
- Analisar a aplicabilidade da técnica de inserção de AN, baseada nos graus de liberdade do CP, para aumentar a segurança em redes PLC residenciais, considerando diferentes cenários. São considerados os seguintes cenários: intrusos PLC e sem fio; diferentes distâncias relativas entre transmissor legítimo e intruso; e, finalmente, diferentes proporções de potência entre sinal de informação e AN.

1.2 ORGANIZAÇÃO DO TRABALHO

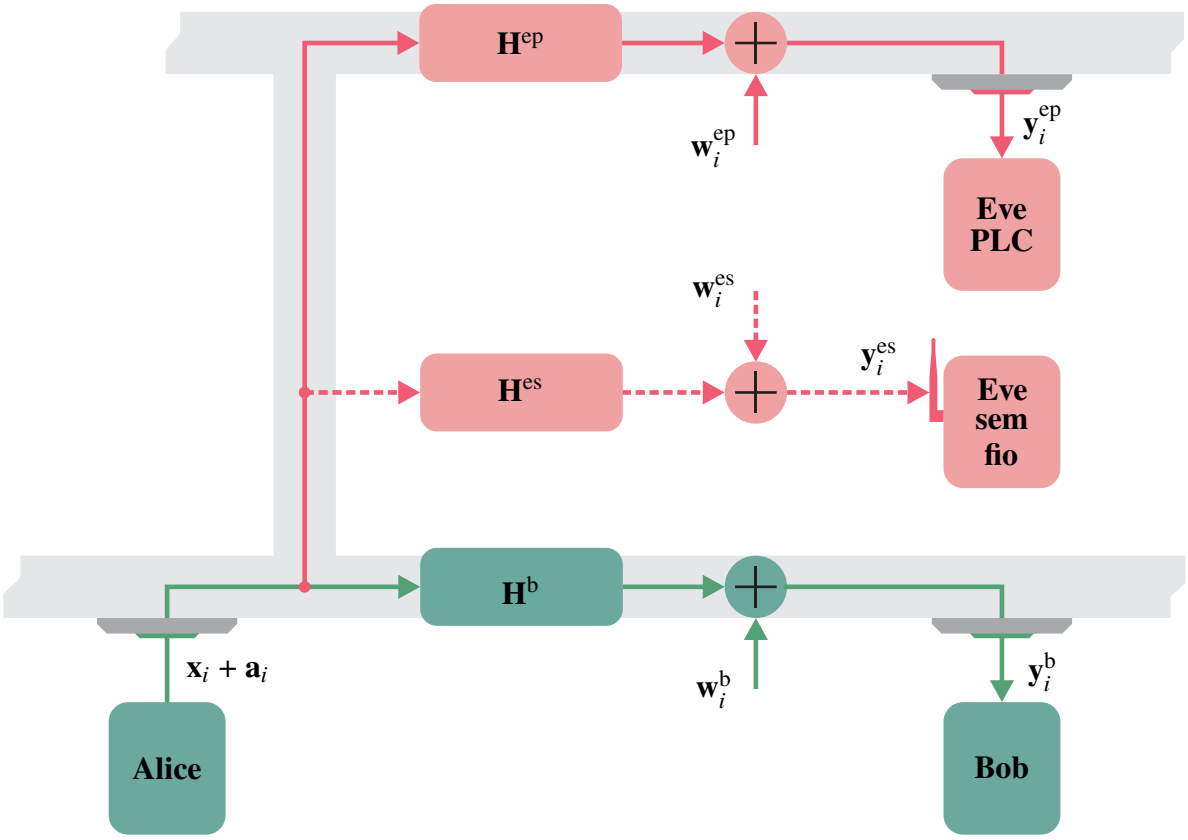
Este trabalho está organizado da seguinte forma:

- Capítulo 2: apresenta-se o modelo do sistema e formula-se os processos de transmissão e recepção nos domínios do tempo discreto e da frequência discreta;
- Capítulo 3: apresenta-se as formulações e deduções do AN. Além disso, as SNRs resultantes no receptor legítimo e no intruso são detalhadas, de forma a entender como o AN aumenta a segurança do sistema.
- Capítulo 4: discute-se os resultados numéricos em termos de BER e PAPR, considerando o método de inserção de AN em redes PLC residenciais;
- Capítulo 5: as conclusões sobre o presente trabalho são contempladas.

2 MODELO DO SISTEMA

Neste capítulo, considera-se o modelo do sistema ilustrado na Figura 2. Esse modelo representa um cenário em que um transmissor PLC legítimo, Alice, envia informações privadas para um receptor PLC legítimo, Bob, enquanto dois intrusos maliciosos, Eve PLC e Eve sem fio, visam escutar as mensagens privadas trocadas entre Alice e Bob. Note que Eve PLC possui a capacidade de interceptar mensagens privadas por meio de uma conexão física com a rede de energia elétrica, enquanto Eve sem fio pode sensoriar o campo eletromagnético emitido pelo sinal PLC quando este trafega pela rede de energia elétrica não blindada. Além disso, a comunicação de dados nesse sistema é feita usando o esquema OFDM Hermitiano simétrico, também conhecido como modulação discreta em múltiplos tons, que será detalhado a seguir.

Figura 2 – Modelo do sistema de comunicação de dados entre Alice (PLC) e Bob (PLC), sob a presença de Eve PLC e Eve sem fio. As linhas tracejadas representam os canais sem fio, enquanto as linhas contínuas representam os canais PLC.



Fonte: Acervo do autor (inspirado em [21]).

Seja $\overline{\mathbf{X}}_i \in \mathbb{C}^{(N/2)\times 1}$ o i-ésimo bloco de sinais modulados, que é representado por $\overline{\mathbf{X}}_i = [\overline{X}_{i,0} \quad \overline{X}_{i,1} \quad \cdots \quad \overline{X}_{i,(N/2)-1}]^{\mathrm{T}}$. No esquema em questão, o mapeamento, denominado Hermitiano simétrico, é aplicado ao bloco $\overline{\mathbf{X}}_i$, transformando-o no i-ésimo bloco mapeado. Este bloco é expresso no domínio da frequência discreta como $\mathbf{X}_i = [X_{i,0} \quad X_{i,1} \quad \cdots \quad X_{i,N-1}]^{\mathrm{T}}$, em que $\mathbf{X}_i \in \mathbb{C}^{N\times 1}$. O mapeamento é executado de modo que o k-ésimo elemento de $\mathbf{X}_i$ seja

determinado por

$$X_{i,k} = \begin{cases} \Re\{\overline{X}_{i,(N/2)-1}\}, & k = 0 \\ \overline{X}_{i,k-1}, & k = 1, \cdots, (N/2)-1 \\ \Im\{\overline{X}_{i,(N/2)-1}\}, & k = N/2 \\ \overline{X}^{*}_{i,N-1-k}, & k = (N/2)+1, \cdots, N-1 \end{cases}. \tag{2.1}$$

Considera-se que $\mathbb{E}\{\mathbf{X}_i\} = \mathbf{0}_{N\times 1}$, $\forall i$, e $\mathbb{E}\{\mathbf{X}_i\mathbf{X}_i^{\dagger}\} = \mathbf{\Lambda}_{\sigma_{\mathbf{x}}^2}$, $\forall i$, é uma matriz diagonal que representa a matriz de autocorrelação dos blocos transmitidos, de forma que $\mathrm{Tr}(\mathbf{\Lambda}_{\sigma_{\mathbf{x}}^2}) = P_{\mathbf{x}}N$, em que $P_{\mathbf{x}}$ é a potência total média atribuída ao bloco de informação transmitido. No domínio do tempo discreto, o bloco de informação transmitido na banda base, e portanto contendo apenas elementos reais, pode ser representado como

$$\mathbf{x}_i = \mathbf{\Psi}_{\mathrm{T}}\mathbf{F}^{\dagger}\mathbf{X}_i, \tag{2.2}$$

em que a matriz $\mathbf{\Psi}_{\mathrm{T}} = [\mathbf{E}^{\mathrm{T}}_{N_{\mathrm{cp}}\times N}\mathbf{I}_N]^{\mathrm{T}}$ é responsável pela inserção do CP, com N_{cp} indicando o comprimento do CP e $\mathbf{E}_{N_{\mathrm{cp}}\times N} = [\mathbf{0}_{N_{\mathrm{cp}}\times(N-N_{\mathrm{cp}})}\mathbf{I}_{N_{\mathrm{cp}}}]$. Alice envia o bloco de informação $\mathbf{x}_i$ junto com um bloco de AN, $\mathbf{a}_i \in \mathbb{R}^{(N+N_{\mathrm{cp}})\times 1}$, tal que $\mathbb{E}\{\mathbf{a}_i\} = \mathbf{0}_{(N+N_{\mathrm{cp}})\times 1}$, $\forall i$, e $\mathbb{E}\{\mathbf{a}_i\mathbf{a}_i^{\dagger}\} = \mathbf{R}_{\mathbf{aa}}$, $\forall i$, é a matrix de autocorrelação do AN, sendo que $\mathrm{Tr}(\mathbf{R}_{\mathbf{aa}}) = P_{\mathbf{a}}(N + N_{\mathrm{cp}})$, em que $P_{\mathbf{a}}$ é a potência total média atribuída ao AN. A potência de transmissão total é, portanto, $P_{\mathrm{T}} = P_{\mathbf{x}} + P_{\mathbf{a}}$.

O bloco completo construído, ou seja, informação mais AN, é transmitido por meio de um canal de comunicação, que possui um tempo de coerência maior que o intervalo de tempo do bloco construído, de modo que ele possa ser modelado como um sistema linear e invariante no tempo (do inglês, *linear time-invariant*) (LTI). Através desse canal de comunicação, o bloco transmitido chega a Bob, Eve PLC e Eve sem fio, indexados respectivamente por "b", "ep" e "es". Assumindo-se que $\{h^l[n]\}_{n=0}^{L_l-1}$ representa os coeficientes da resposta ao impulso do canal (do inglês, *channel impulse response*) (CIR) entre Alice e o usuário l, com $l \in \{\mathrm{b}, \mathrm{ep}, \mathrm{es}\}$, sendo que L_l denota o comprimento da CIR, a matriz de canal Toeplitz [20] associada ao usuário l pode ser definida como

$$\mathbf{H}^l = \begin{bmatrix} h^l[0] & 0 & 0 & \cdots & \cdots & 0 & 0 \\ h^l[1] & h^l[0] & 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ h^l[L_l-1] & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & h^l[0] & 0 \\ 0 & \cdots & 0 & h^l[L_l-1] & \cdots & h^l[1] & h^l[0] \end{bmatrix}. \tag{2.3}$$

Para transmissão na banda base, $\mathbf{H}^l \in \mathbb{R}^{(N+N_{\mathrm{cp}})\times(N+N_{\mathrm{cp}})}$. Note que $\mathbf{C}^l_{\mathbf{H}} = \mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^l\mathbf{\Psi}_{\mathrm{T}} \in \mathbb{R}^{N\times N}$ é a matriz circulante cuja primeira coluna contém os coeficientes da CIR do usuário l seguidos de

zeros, e $\mathbf{\Lambda}_{\mathbf{H}}^{l} = \mathbf{F}\mathbf{C}_{\mathbf{H}}^{l}\mathbf{F}^{\dagger} \in \mathbb{C}^{N\times N}$ é uma matriz diagonal com a resposta em frequência do canal do usuário l na diagonal principal.

No usuário l, o i-ésimo bloco recebido no domínio do tempo discreto pode ser escrito como

$$\mathbf{y}_i^l = \mathbf{H}^l(\mathbf{x}_i + \mathbf{a}_i) + \mathbf{w}_i^l, \qquad \forall l \in \{\mathrm{b}, \mathrm{ep}, \mathrm{es}\}, \tag{2.4}$$

em que $\mathbf{w}_i^l \in \mathbb{R}^{(N+N_{\mathrm{cp}})\times 1}$ indica o vetor de ruído aditivo que afeta o i-ésimo bloco e l-ésimo usuário. O usuário l, então, realiza nos blocos recebidos $\mathbf{y}_i^l$ a operação inversa àquelas realizadas em Alice. Como resultado, o i-ésimo bloco recebido pelo usuário l pode ser representado no domínio da frequência discreta como

$$\begin{aligned}
\mathbf{Y}_i^l &= \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{y}_i^l \\
&= \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^l\mathbf{x}_i + \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^l\mathbf{a}_i + \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{w}_i^l \\
&= \mathbf{\Lambda}_{\mathbf{H}}^l\mathbf{X}_i + \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^l\mathbf{a}_i + \mathbf{W}_i^l,
\end{aligned} \tag{2.5}$$

com a matriz $\mathbf{\Psi}_{\mathrm{R}} = [\mathbf{0}_{N\times N_{\mathrm{cp}}}\mathbf{I}_N]$ sendo responsável pela remoção do CP e $\mathbf{W}_i^l = \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{w}_i^l$ indicando o bloco de ruído aditivo no domínio da frequência discreta, com $\mathbb{E}\{\mathbf{W}_i^l\} = \mathbf{0}_{(N)\times 1}$, $\forall i$, e $\mathbb{E}\{\mathbf{W}_i^l(\mathbf{W}_i^l)^{\dagger}\} = \mathbf{\Lambda}_{\sigma_{\mathbf{W}}^2}^{l}$, $\forall i$, tal que $\mathrm{Tr}(\mathbf{\Lambda}_{\sigma_{\mathbf{W}}^2}^{l}) = P_{\mathbf{W}^l}$, em que $P_{\mathbf{W}^l}$ denota a potência média do ruído no usuário l.

3 RUÍDO ARTIFICIAL BASEADO NOS GRAUS DE LIBERDADE DO PREFIXO CÍCLICO

O AN deve ser desenvolvido para deteriorar a SNR de Eve PLC e Eve sem fio mas não a de Bob. Neste capítulo é descrito um projeto de AN para esse fim, baseando-se nos graus de liberdade introduzidos pelo CP [20]. O objetivo é criar um AN que afete de forma significativa as SNRs dos intrusos, ao passo que seja minimamente prejudicial para o receptor legítimo.

Desta forma, o capítulo está dividido da seguinte maneira: a Seção 3.1 detalha o projeto do AN e a Seção 3.2 apresentada as SNRs resultantes nos usuários legítimos e intrusos, permitindo uma análise detalhada do impacto da injeção do AN.

3.1 PROJETO DO RUÍDO ARTIFICIAL

Primeiramente, Alice precisa projetar $\mathbf{a}_i$ de tal modo que ao ser convoluído com o canal de Bob resulte em um sinal nulo, o que não deve acontecer no caso de Eve PLC ou Eve sem fio. Matematicamente, poderia-se procurar por $\mathbf{a}_i$ tal que $\mathbf{H}^{\mathrm{b}}\mathbf{a}_i = \mathbf{0}_{(N+N_{\mathrm{cp}})\times 1}$. Contudo, $\mathbf{H}^{\mathrm{b}}$ é uma matriz quadrada de posto[1] completo, cujo espaço nulo é composto inteiramente por zeros, ou seja, a única solução seria $\mathbf{a}_i = \mathbf{0}_{(N+N_{\mathrm{cp}})\times 1}$. Essa solução não é desejável visto que não deteriora as SNRs de Eve PLC e Eve sem fio. Uma possível alternativa seria projetar o AN em uma etapa diferente, por exemplo, usando as matrizes $\mathbf{C}^{\mathrm{b}}_{\mathbf{H}}$ ou $\mathbf{\Lambda}^{\mathrm{b}}_{\mathbf{H}}$. No entanto, essas matrizes possuem, igualmente, posto completo, o que impossibilita suas aplicações no projeto do AN.

De forma a evitar os problemas descritos acima, os autores de [20] exploraram os graus de liberdade introduzidos pelo CP, utilizando a matriz $\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{b}} \in \mathbb{R}^{N\times(N+N_{\mathrm{cp}})}$ para projetar o AN. De acordo com o trabalho [20], $\mathbf{a}_i = \mathbf{V}^{\mathrm{b}}_{\mathrm{null}}\mathbf{d}_i$, tal que $\mathbf{d}_i \in \mathbb{R}^{N_{\mathrm{cp}}\times 1}$ é um vetor de variáveis aleatórias Gaussianas independentes e de mesma variância, enquanto $\mathbf{V}^{\mathrm{b}}_{\mathrm{null}} \in \mathbb{R}^{(N+N_{\mathrm{cp}})\times N_{\mathrm{cp}}}$ define o espaço nulo à direita de $\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{b}}$, ou seja,

$$\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{\mathrm{b}}\mathbf{V}^{\mathrm{b}}_{\mathrm{null}} = \mathbf{0}_{N\times N_{\mathrm{cp}}}. \tag{3.1}$$

Note que apenas $\mathbf{d}_i$ e $\mathbf{V}^{\mathrm{b}}_{\mathrm{null}}$ precisam ser encontrados para projetar $\mathbf{a}_i$ de acordo com essa estratégia. O primeiro pode ser obtido a partir de um gerador de variáveis aleatórias Gaussianas [22], enquanto o segundo é obtido por meio da decomposição em valores singulares (do inglês, *singular value decomposition*) (SVD)—vide Apêndice A.

3.2 RELAÇÃO SINAL-RUÍDO

Uma vez que o AN é projetado conforme descrito na subseção anterior, de acordo com (2.5), a representação no domínio da frequência discreta do i-ésimo bloco recebido por

[1] O posto de uma matriz indica o menor valor entre o número máximo de linhas ou colunas linearmente independentes presentes na matriz.

Bob e Eve PLC ou Eve sem fio será dada, respectivamente, por

$$\mathbf{Y}_i^{\mathrm{b}} = \mathbf{\Lambda}_{\mathbf{H}}^{\mathrm{b}}\mathbf{X}_i + \mathbf{W}_i^{\mathrm{b}} \tag{3.2}$$

e

$$\mathbf{Y}_i^{e} = \mathbf{\Lambda}_{\mathbf{H}}^{e}\mathbf{X}_i + \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i + \mathbf{W}_i^{e}, \quad \forall e \in \{\mathrm{ep}, \mathrm{es}\}. \tag{3.3}$$

Assim, o bloco resultante recebido por Eve PLC ou Eve sem fio possui um termo adicional de ruído, ou seja, $\mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i, \forall e \in \{\mathrm{ep}, \mathrm{es}\}$, que irá prejudicar suas SNRs.

Para calcular a SNR por subportadora, pode-se computar a porção da energia recebida relacionada ao bloco de informação, dividida pela porção da energia recebida relacionada ao ruído. Além disso, pode-se extrair esses termos de energia da diagonal principal da matriz de autocorrelação associado à cada um dos processos aleatórios, do bloco de informação e do bloco do ruído. Com base em (3.2), a SNR de Bob, no domínio da frequência discreta, pode ser escrita como a matriz diagonal que segue:

$$\begin{aligned}
\mathbf{\Lambda}_{\gamma}^{\mathrm{b}} &= \frac{\mathrm{diag}\{\mathbb{E}\{(\mathbf{\Lambda}_{\mathbf{H}}^{\mathrm{b}}\mathbf{X}_i)(\mathbf{\Lambda}_{\mathbf{H}}^{\mathrm{b}}\mathbf{X}_i)^{\dagger}\}\}}{\mathrm{diag}\{\mathbb{E}\{\mathbf{W}_i^{\mathrm{b}}(\mathbf{W}_i^{\mathrm{b}})^{\dagger}\}\}} \\
&= \frac{\mathrm{diag}\{\mathbf{\Lambda}_{\mathbf{H}}^{\mathrm{b}}\mathbb{E}\{\mathbf{X}_i\mathbf{X}_i^{\dagger}\}\mathbf{\Lambda}_{\mathbf{H}}^{\mathrm{b}\dagger}\}}{\mathrm{diag}\{\mathbb{E}\{\mathbf{W}_i^{\mathrm{b}}(\mathbf{W}_i^{\mathrm{b}})^{\dagger}\}\}} \\
&= \frac{\mathbf{\Lambda}_{\sigma_{\mathbf{x}}^2}\mathbf{\Lambda}_{|\mathbf{H}|^2}^{\mathrm{b}}}{\mathbf{\Lambda}_{\sigma_{\mathbf{W}}^2}^{\mathrm{b}}},
\end{aligned} \tag{3.4}$$

em que $\mathbf{\Lambda}_{|\mathbf{H}|^2}^{l}$ é uma matriz diagonal com os ganhos dos subcanais que compõe a resposta em frequência do canal entre Alice e o usuário l. Nos usuários Eve PLC e Eve sem fio, a SNR no domínio da frequência discreta pode ser calculada de maneira semelhante, exceto pelo fato de haver dois termos de ruído adicionais. Portanto, ela é dada por:

$$\mathbf{\Lambda}_{\gamma}^{e} = \frac{\mathrm{diag}\{\mathbb{E}\{(\mathbf{\Lambda}_{\mathbf{H}}^{e}\mathbf{X}_i)(\mathbf{\Lambda}_{\mathbf{H}}^{e}\mathbf{X}_i)^{\dagger}\}\}}{\mathrm{diag}\{\mathbb{E}\{(\mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i + \mathbf{W}_i^{e})(\mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i + \mathbf{W}_i^{e})^{\dagger}\}\}}, \quad \forall e \in \{\mathrm{ep}, \mathrm{es}\}. \tag{3.5}$$

Nesse ponto, é importante ressaltar que o termo relacionado ao AN, ou seja, $\mathbf{F}\mathbf{\Psi}\mathrm{R}\mathbf{H}^{e}\mathbf{a}_i, \forall e \in \{\mathrm{ep}, \mathrm{es}\}$, é independente do termo de ruído natural presente em Eve PLC, $\mathbf{W}_i^{\mathrm{ep}}$, e Eve sem fio, $\mathbf{W}_i^{\mathrm{es}}$. Consequentemente, a matriz de autocorrelação do ruído total resultante em Eve PLC ou Eve sem fio, que compõe o denominador de (3.5), pode ser descrita como

$$\begin{aligned}
\mathbf{R}_{\mathrm{noise}}^{e} &= \mathbb{E}\{(\mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i + \mathbf{W}_i^{e})(\mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i + \mathbf{W}_i^{e})^{\dagger}\} \\
&= \mathbb{E}\{(\mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i)(\mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{a}_i)^{\dagger} + (\mathbf{W}_i^{e})(\mathbf{W}_i^{e})^{\dagger}\} \\
&= \mathbf{F}\mathbf{\Psi}_{\mathrm{R}}\mathbf{H}^{e}\mathbf{R}_{\mathbf{aa}}\mathbf{H}^{e\dagger}\mathbf{\Psi}_{\mathrm{R}}^{\dagger}\mathbf{F}^{\dagger} + \mathbf{\Lambda}_{\sigma_{\mathbf{W}}^2}^{e} \\
&= \mathbf{R}_{\mathrm{an}}^{e} + \mathbf{\Lambda}_{\sigma_{\mathbf{W}}^2}^{e}, \quad \forall e \in \{\mathrm{ep}, \mathrm{es}\},
\end{aligned} \tag{3.6}$$

em que $\mathbf{R}_{\text{an}}^{e} = \mathbf{F}\boldsymbol{\Psi}_{\text{R}}\mathbf{H}^{e}\mathbf{R}_{\mathbf{aa}}\mathbf{H}^{e\dagger}\boldsymbol{\Psi}_{\text{R}}^{\dagger}\mathbf{F}^{\dagger}, \forall e \in \{\text{ep}, \text{es}\}$, é a matriz de autocorrelação da porção de ruído associada ao AN em Eve PLC ou Eve sem fio. Finalmente, a SNR de Eve PLC ou Eve sem fio no domínio da frequência discreta pode ser obtida a partir da seguinte matriz diagonal:

$$\boldsymbol{\Lambda}_{\gamma}^{e} = \frac{\boldsymbol{\Lambda}_{\sigma_{\mathbf{x}}^{2}}\boldsymbol{\Lambda}_{|\mathbf{H}|^{2}}^{e}}{\boldsymbol{\Lambda}_{\sigma_{\text{an}}^{2}}^{e} + \boldsymbol{\Lambda}_{\sigma_{\mathbf{W}}^{2}}^{e}}, \quad \forall e \in \{\text{ep}, \text{es}\}, \tag{3.7}$$

no qual $\boldsymbol{\Lambda}_{\sigma_{\text{an}}^{2}}^{e} = \text{diag}\{\mathbf{R}_{\text{an}}^{e}\}, \forall e \in \{\text{ep}, \text{es}\}$.

Ao comparar (3.4) com (3.7), é observado que o termo adicional de AN resulta na introdução de um termo adicional no denominador da SNR de Eve PLC e Eve sem fio. Na próxima seção, será realizada um avaliação numérica do impacto desse termo adicional de ruído no desempenho de Bob, Eve PLC e Eve sem fio em duas diferentes configurações: intruso próximo ao transmissor legítimo e intruso próximo ao receptor legítimo.

4 RESULTADOS NUMÉRICOS

Neste capítulo, avalia-se o desempenho do AN projetado com base nos graus de liberdade introduzidos pelo CP em redes PLC residenciais que enfrentam potencial ameaça de intrusos PLC ou sem fio. As CIRs dos canais Alice-Bob e Alive-Eve PLC foram obtidas a partir da campanha de medição reportada em [23], enquanto as CIRs do canal Alice-Eve sem fio derivam da campanha de medição dos canais híbridos PLC-sem fio relatada em [6]. Dois cenários são considerados para cada tipo de intruso: um para o intruso próximo ao transmissor legítimo, denominado caminho curto (do inglês, *short-path*) (SP), e outro para o intruso próximo ao receptor legítimo, denominado caminho longo (do inglês, *long-path*) (LP). Portanto, quatro cenários diferentes são analisados, como ilustrado na Figura 3.

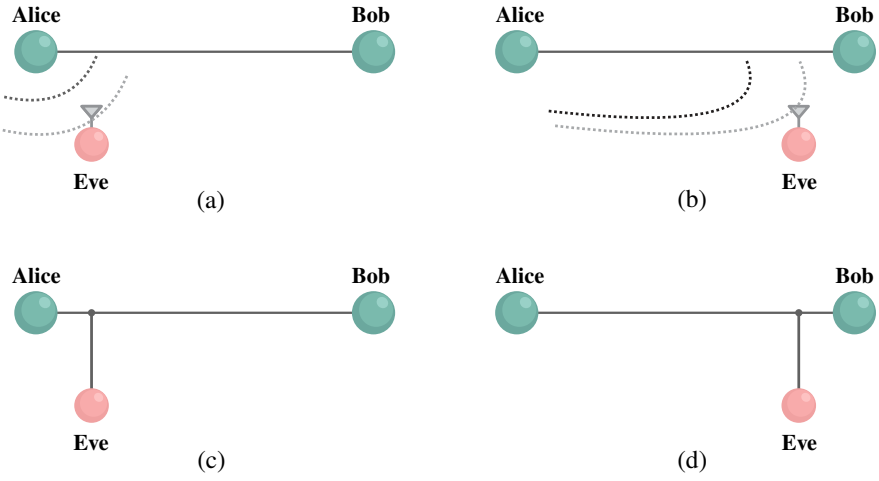
As análises numéricas são realizas em termos de BER e PAPR. Para isso, foi utilizado um esquema OFDM Hermitiano simétrico com $N = 4096$ e $N_{\text{cp}} = 512$ amostras, o que garante a ausência de interferência intersimbólica (do inglês, *intersymbol interference*) (ISI) para todos os canais simulados. A abordagem numérica para potência média de transmissão P_{T} é tal que $P_{\mathbf{x}} = (1-\alpha)P_{\text{T}}$ e $P_{\mathbf{a}} = \alpha P_{\text{T}}$, com $\alpha \in [0, 1]$. Assume-se alocação uniforme de potência, logo $\mathbf{\Lambda}_{\sigma^2_{\mathbf{x}}} = \mathbf{I}_N P_{\mathbf{x}}$.

Este capítulo está estruturado da seguinte maneira: na Seção 4.1, detalha-se os resultados obtidos de BER; na Seção 4.2, discute-se os resultados obtidos de PAPR.

4.1 ANÁLISE DA TAXA DE ERRO DE BIT

Nesta seção, avalia-se o impacto do AN para a segurança de uma rede PLC residencial em termos de BER. As análises consideram os valores de BER de Bob, Eve PLC e Eve sem fio em função da potência média de transmissão total (P_{T}). Para isso, foram consideradas simulações de

Figura 3 – Cenários analisados com diferentes posições relativas do intruso. (a) Eve sem fio SP. (b) Eve sem fio LP. (c) Eve PLC SP. (d) Eve PLC LP.

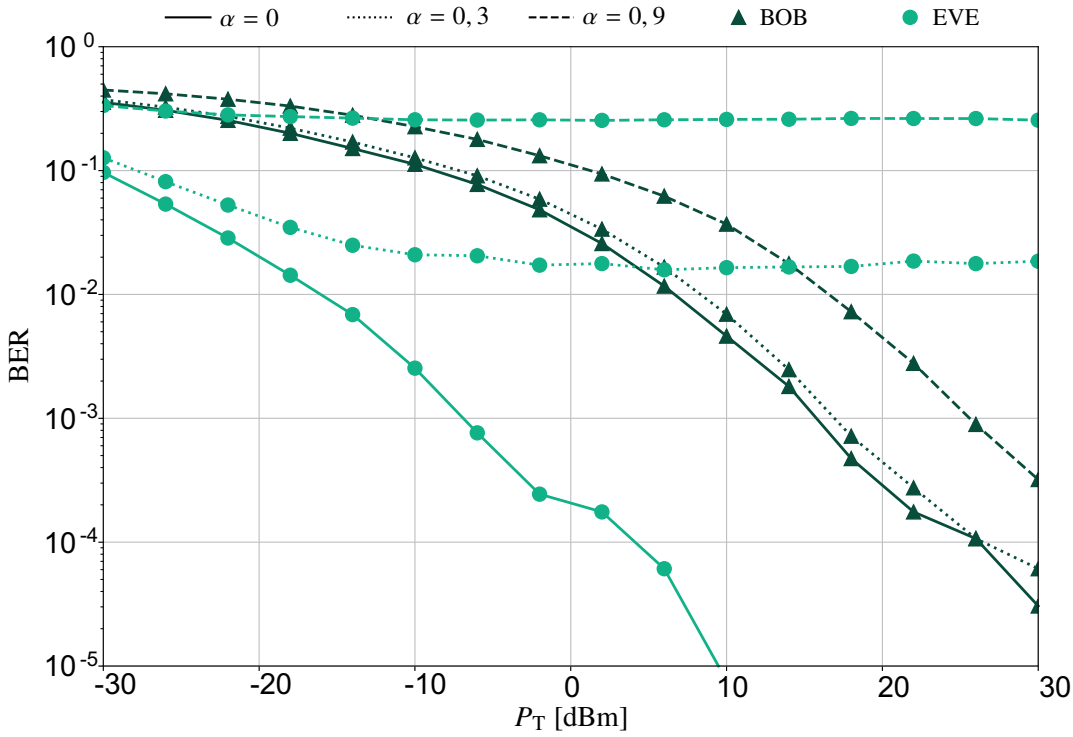


Fonte: Acervo do autor (inspirado em [21]).

Monte Carlo com a transmissão de 2^{17} bits, os quais foram mapeados em símbolos da modulação de amplitude em quadratura (do inglês, *quadrature amplitude modulation*) (QAM) de ordem 4. Adicionalmente, os usuários PLC estão sujeitos ao ruído Gaussiano colorido aditivo com densidade espectral de potência (do inglês, *power spectral density*) (PSD) de $1/f$, enquanto Eve sem fio está sujeita ao ruído Gaussiano branco aditivo (do inglês, *additive white Gaussian noise*) (AWGN). Ainda, assume-se $P_{\mathbf{W}}^{l} = 10^{-8}, \forall l$ [24].

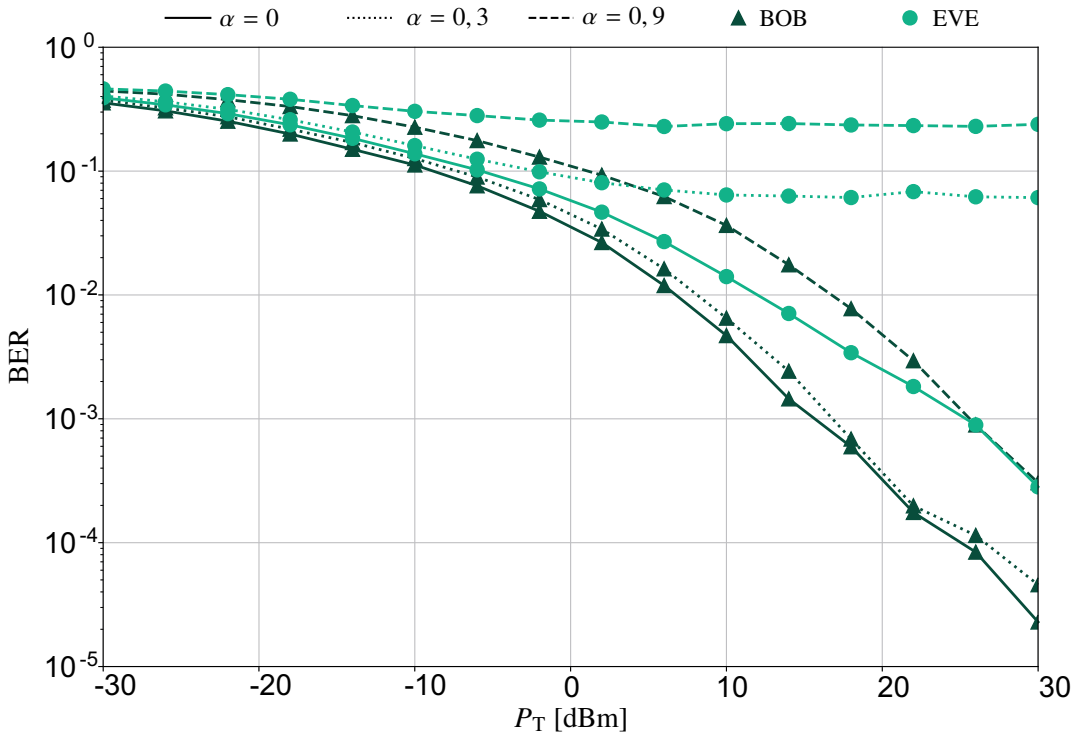
Nas Figuras 4 e 5, apresenta-se os resultados de BER para Bob e Eve PLC, considerando valores de $\alpha \in \{0, 0{,}3, 0{,}9\}$ e valores de $P_{\mathrm{T}} \in [-30, 30]$ dBm. Inicialmente, na Figura 4, essa análise considera Eve PLC próxima a Alice, ou seja, SP. Para $\alpha = 0$ (sem inserção de AN), a BER de Eve PLC é naturalmente menor do que a de Bob. No entanto, a medida que a potência do AN aumenta, a BER de Bob aumenta ligeiramente, uma vez que P_{T} está dividida entre o sinal e o AN. Por outro lado, o AN impacta severamente a BER de Eve PLC, de modo que ela se torna maior do que a de Bob para $P_{\mathrm{T}} > 6$ dBm se $\alpha = 0,3$ e para $P_{\mathrm{T}} \geq -10$ dBm se $\alpha = 0,9$. Enquanto isso, são apresentados na Figura 5 os resultados para Eve PLC próxima a Bob, ou seja, LP. Nesse cenário, a BER de Bob é menor do que a de Eve PLC se $\alpha = 0$, ou seja, o canal de Bob é inerentemente melhor do que o de Eve PLC. Conforme α aumenta, os valores de BER de Bob e Eve PLC também aumentam, com uma degradação mais perceptível para Eve PLC. Contudo, não é necessário alocar excessiva potência para o AN quando Eve PLC está próxima a Bob, considerando o menor impacto do AN nesse cenário específico.

Figura 4 – BER vs P_{T} para Bob e Eve PLC sob valores distintos de α para o cenário SP.



Fonte: Acervo do autor.

Figura 5 – BER vs P_T para Bob e Eve PLC sob valores distintos de α para o cenário LP.



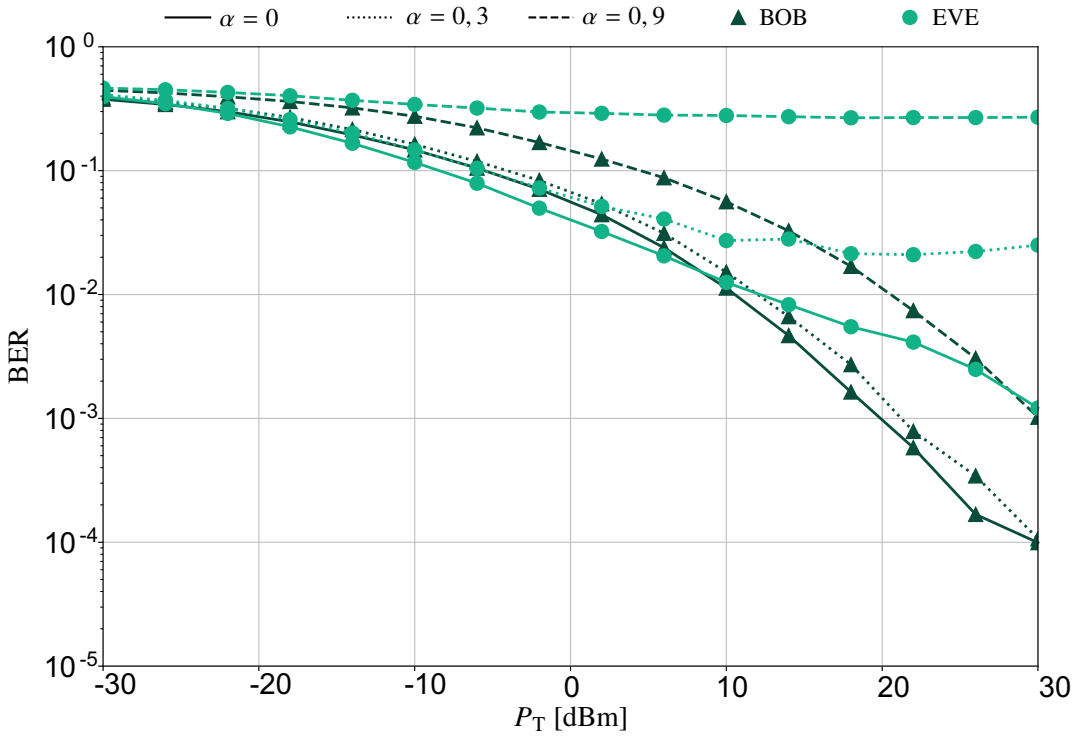
Fonte: Acervo do autor.

Nas Figuras 6 e 7, examina-se o efeito da injeção do AN na rede PLC sob a presença de um intruso sem fio. Portanto, o canal do receptor legítimo da análise anterior é mantido enquanto o canal do intruso muda para o canal híbrido PLC-sem fio. Na Figura 6, mostra-se os resultados para o cenário SP. Note que na ausência de AN ($\alpha = 0$), a BER de Eve sem fio é ligeiramente menor do que a de Bob para $P_T < 10$ dBm. Contudo, conforme mais potência é alocada para o AN a BER de Bob se torna menor do que a de Eve sem fio para $P_T > 2$ dBm se $\alpha = 0,3$ e para qualquer valor de P_T se $\alpha = 0,9$. Mudando as análises para os resultados do cenário LP, exibidos na Figura 7, observa-se que a BER de Eve sem fio é maior do que a de Bob para todos os valores simulados de α, ou seja, a BER de Eve sem fio é pior do que a de Bob independentemente da quantidade de potência alocada para AN. Portanto, quando Eve sem fio está próxima de Alice, ou quando Eve PLC está próxima do transmissor legítimo, ocorre uma queda na segurança do sistema de comunicação. Contudo, a segurança do sistema aumenta à medida que o intruso se afasta do transmissor legítimo.

Em geral, os resultados obtidos mostram que os intrusos PLC são mais perigosos para a segurança de uma rede PLC residencial do que intrusos sem fio, o que se deve tanto à correlação dos canais PLC para nós próximos quanto à menor atenuação do canal associado ao intruso PLC. Quando a rede PLC está na presença de um intruso sem fio, não é necessário alocar muita potência para o AN, visto que a atenuação do canal relacionada aos intrusos sem fio é maior. Ademais, o AN é mais vantajoso em cenários com intrusos PLC próximos ao transmissor.

Portanto, a técnica analisada pode vir a ser útil no cenário mais ameaçador à rede PLC.

Figura 6 – BER vs P_T para Eve sem fio e Bob sob valores distintos de α para o cenário SP.



Fonte: Acervo do autor.

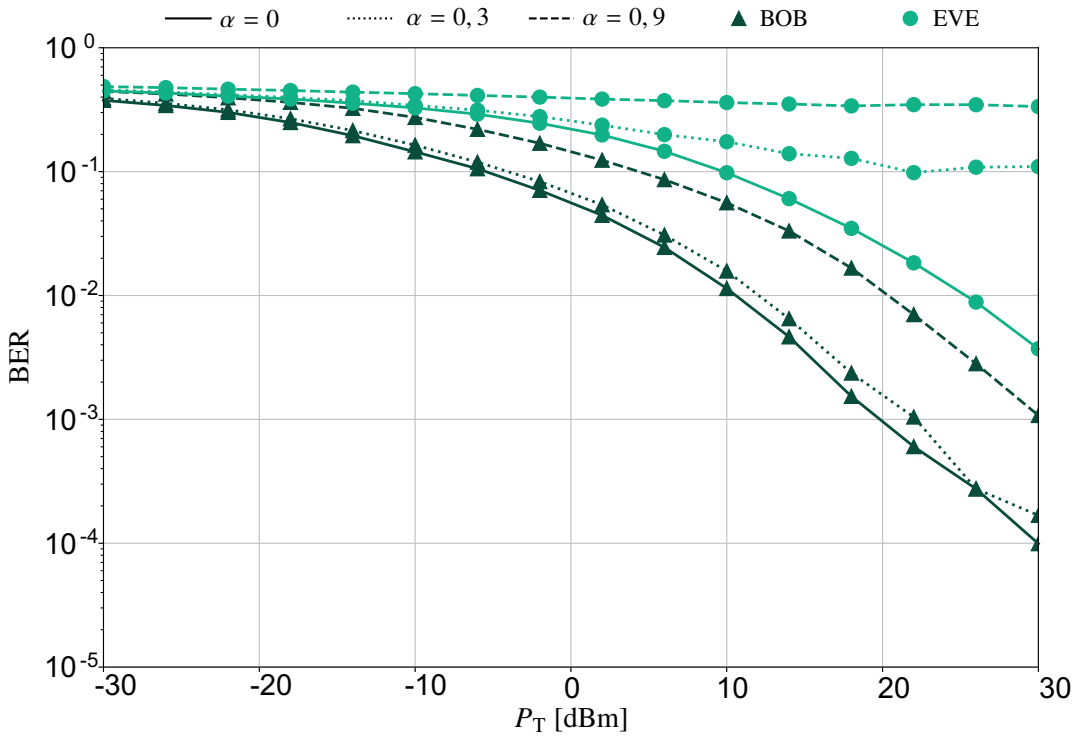
4.2 ANÁLISE DA RELAÇÃO PICO PARA MÉDIA DE POTÊNCIA

Nesta seção, faz-se uma análise do sinal transmitido em termos de PAPR variando a quantidade de potência que é alocada para o AN. Esta análise considera a função de distribuição cumulativa complementar (do inglês, *complementary cumulative distribution function*) (CCDF) empírica da PAPR, obtida a partir da transmissão de 2^{25} bits. Ainda, de forma a obter resultados de PAPR representativos de um sinal no tempo contínuo, foi considerado um fator de *upsampling* igual a 4 [25]. Finalmente, para fins de comparação, utiliza-se a curva teórica da CCDF da PAPR do sinal transmitido para um esquema OFDM Hermitiano simétrico desenvolvida por Hua *et al.* [26]:

$$\mathbb{P}[\text{PAPR} > \text{PAPR}_0] = 1 - \exp\left(-\frac{2N}{\sqrt{3}}\exp\left(\frac{-\text{PAPR}_0}{2}\right)\right). \tag{4.1}$$

Na Figura 8, apresenta-se as curvas da PAPR considerando o AN projetado a partir do canal de Bob para diferentes valores de α. Inicialmente, pode-se observar que a curva simulada sem a adição de AN ($\alpha = 0$) mantém proximidade com a curva teórica. Contudo, à medida que mais potência é alocada para o AN, a PAPR atinge valores mais elevados. Para $\alpha = 0,1$, a PAPR excede 16 dB com uma probabilidade de 10^{-4}, o que caracteriza um aumento de cerca

Figura 7 – BER vs P_T para Eve sem fio e Bob sob valores distintos de α para o cenário LP.



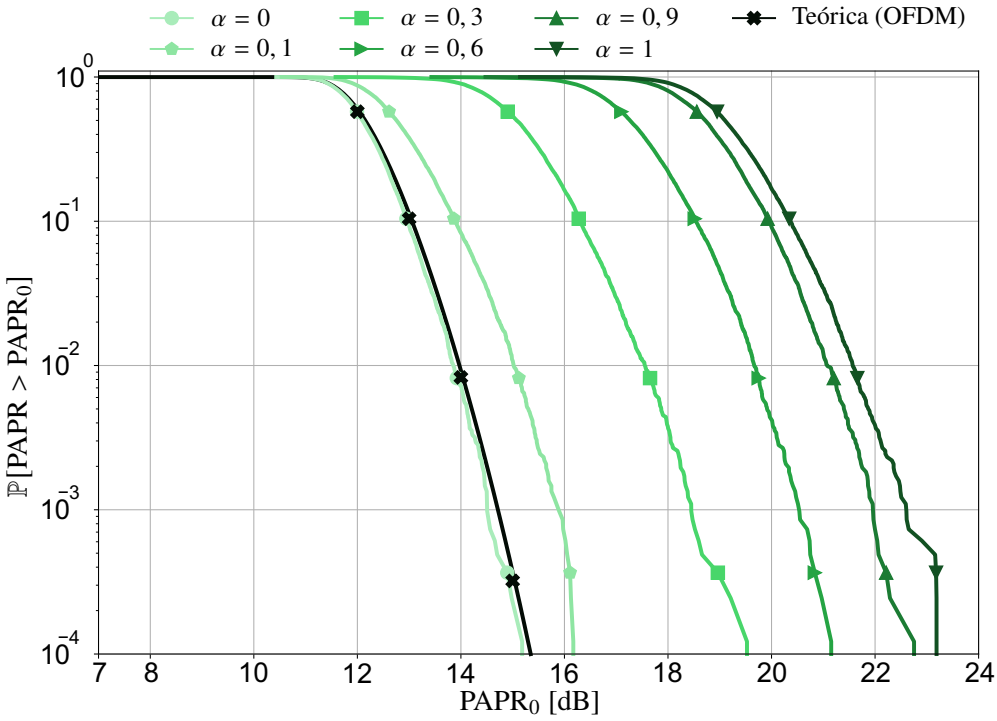
Fonte: Acervo do autor.

de 1 dB em relação a curva sem adição de AN. Essa diferença amplia-se ainda mais a partir de $\alpha = 0,3$, passando para aproximadamente 4 dB e podendo chegar a quase 8 dB para $\alpha = 0,9$. Portanto, o AN gerado a partir dos graus de liberdade introduzidos pelo CP pode impactar significativamente a PAPR do sinal transmitido.

Com o propósito de analisar se esse impacto gerado pelo AN na PAPR existe unicamente devido ao canal de Bob, foram geradas curvas de CCDF empírica da PAPR considerando a geração do AN a partir de outros canais. Nas Figuras 9 e 10, apresenta-se os resultados de PAPR dos símbolos transmitidos quando o AN foi gerado utilizando os canais de Eve PLC nos cenários SP e LP, respectivamente. Para $\alpha = 0,1$, a PAPR ultrapassa 16 dB com uma probabilidade de 10^{-4}, cerca de 1 dB maior que a curva sem adição de AN. Além disso, observa-se que a alocação de mais potência para o AN resulta em níveis mais elevados de PAPR. Note que esses resultados são similares aos observados na Figura 8, em que a relação entre a adição de AN e o aumento da PAPR foi evidenciada. Consequentemente, pode-se dizer que a PAPR do sinal transmitido (informação mais AN) não difere de forma significativa de acordo com o canal PLC utilizado no projeto do AN.

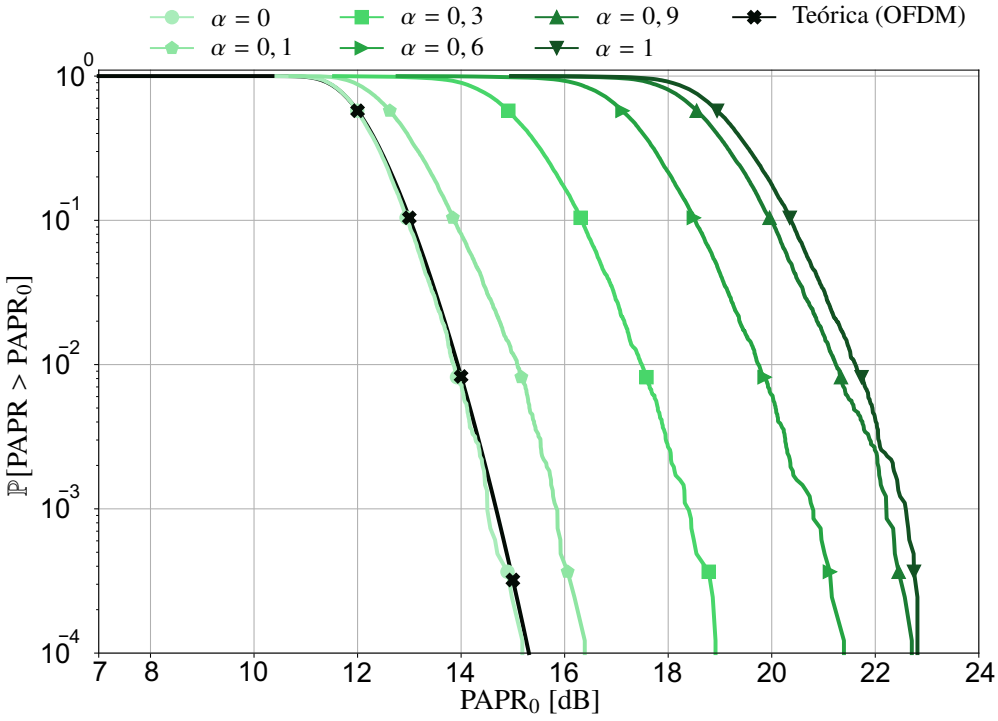
Agora, busca-se avaliar se os altos valores de PAPR são influenciados pela interação entre sinal de informação e AN ou apenas pelo AN. Em contraste com os resultados prévios baseados no esquema OFDM Hermitiano simétrico, utiliza-se então o esquema de monoportadora com prefixo cíclico (do inglês, *single carrier with cyclic prefix*) (SC-CP), que gera símbolos

Figura 8 – CCDF empírica da PAPR quando se utiliza o canal de Bob para projetar o AN sob valores distintos de α, considerando o esquema OFDM Hermitiano simétrico.



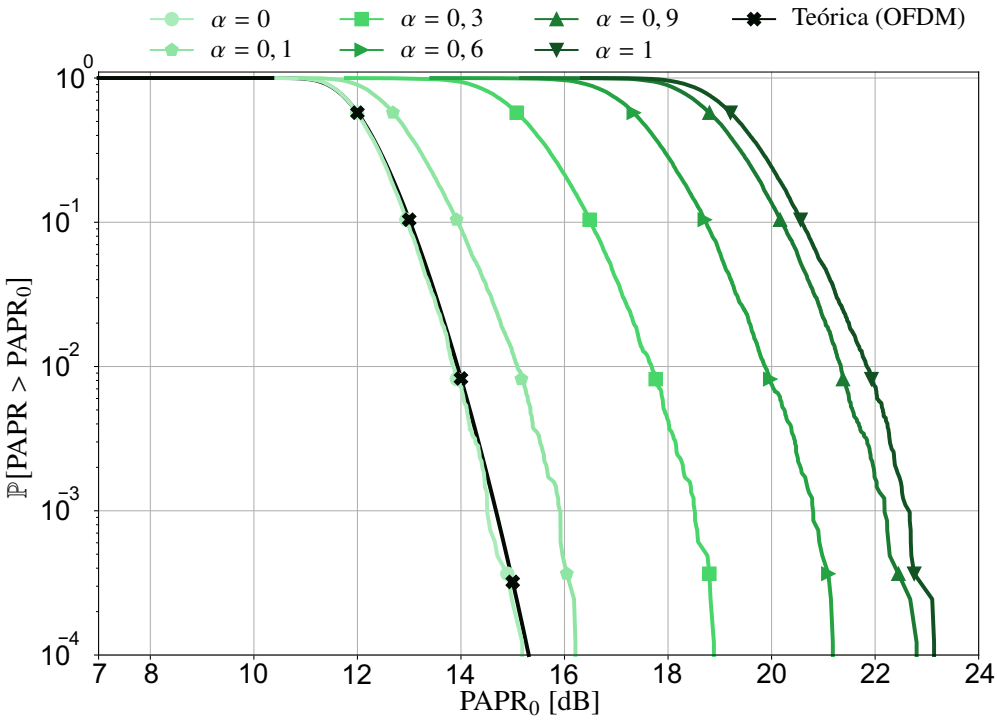
Fonte: Acervo do autor.

Figura 9 – CCDF empírica da PAPR quando se utiliza o canal de Eve, no cenário SP, para projetar o AN sob valores distintos de α, considerando o esquema OFDM Hermitiano simétrico.



Fonte: Acervo do autor.

Figura 10 – CCDF empírica da PAPR quando se utiliza o canal de Eve, no cenário LP, para projetar o AN sob valores distintos de α, considerando o esquema OFDM Hermitiano simétrico.

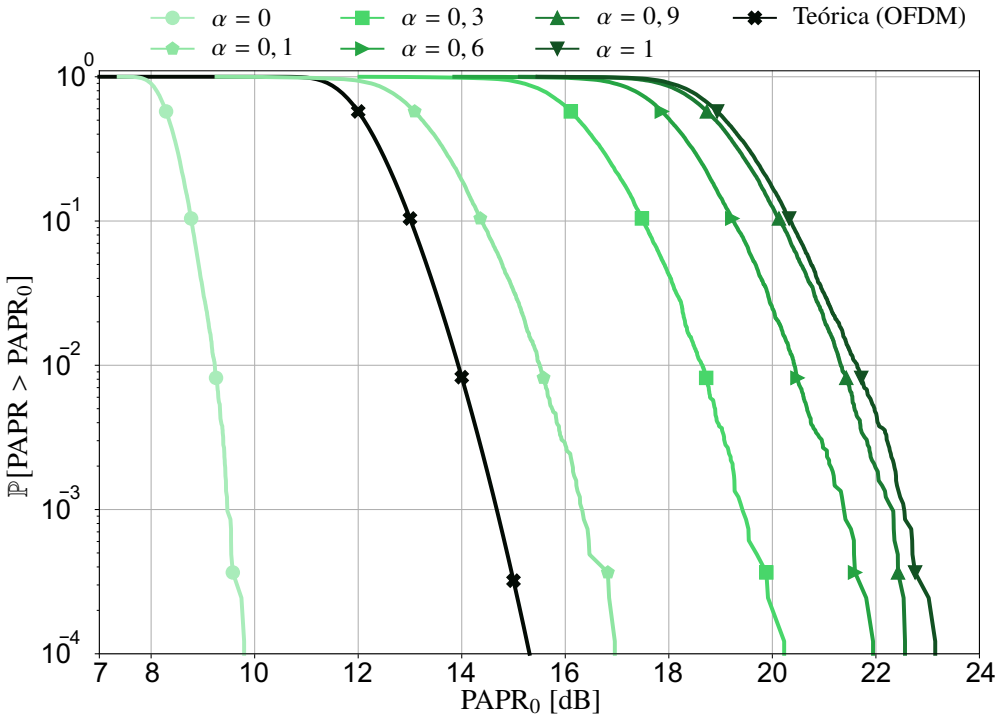


Fonte: Acervo do autor.

transmitidos com baixos valores de PAPR. Observe que a geração do AN necessita apenas do CP, também utilizado no esquema SC-CP, e não da transformada discreta de Fourier inversa (do inglês, *inverse discrete Fourier transform*) (IDFT) no transmissor. Além disso, para esse esquema de modulação, os bits são mapeados em símbolos da modulação por amplitude de pulso (do inglês, *pulse-amplitude modulation*) (PAM) de ordem 2.

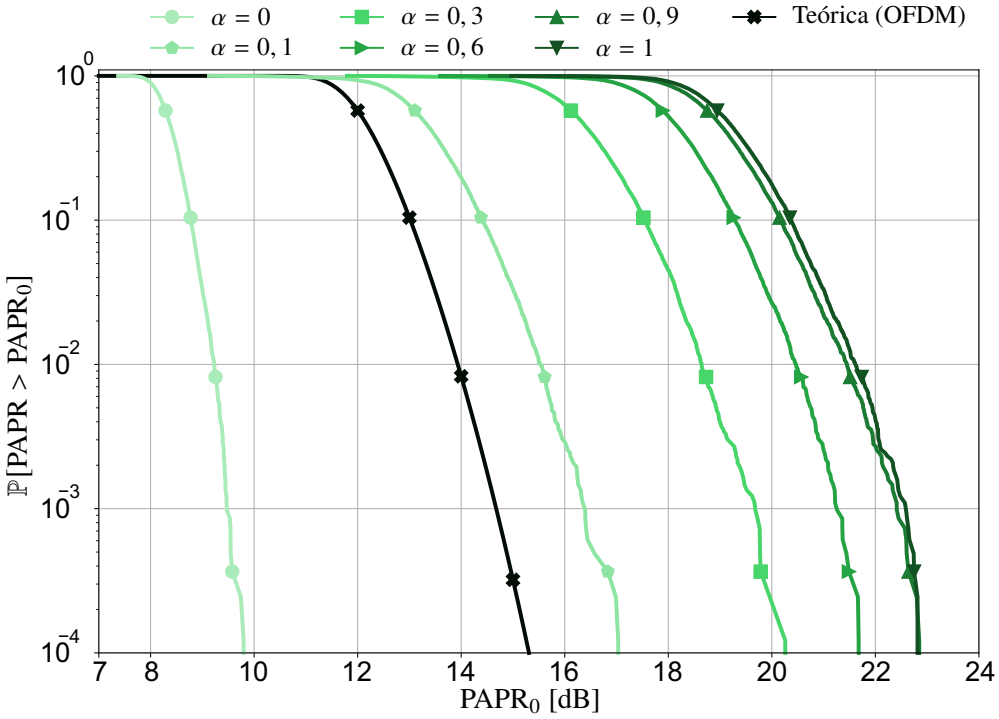
Nas Figuras 11, 12 e 13, ilustra-se os resultados de PAPR quando se utiliza o esquema SC-CP e o AN é projetado considerando, respectivamente, os canais de Bob, Eve PLC no cenário SP e Eve PLC no cenário LP. De forma geral, observa-se que o sinal sem a adição de AN possui uma PAPR que ultrapassa $9,8$ dB com uma probabilidade de 10^{-4}, uma redução de cerca de 5 dB em relação ao mesmo cenário com o esquema OFDM Hermitiano simétrico. Por outro lado, quando $\alpha = 0,1$, observa-se um valor de PAPR que ultrapassa 17 dB com uma probabilidade de 10^{-4}, o que caracteriza um aumento de cerca de 7 dB em relação a curva sem adição de AN. Note que mesmo para um valor baixo de potência de AN ($\alpha = 0,1$), a PAPR do sinal transmitido assemelha-se consideravelmente à PAPR considerando o esquema OFDM. Portanto, a influência do esquema de modulação nos resultados de PAPR é baixa quando se utiliza a técnica de injeção de AN com base nos graus de liberdade introduzidos pelo CP. Adicionalmente, os resultados obtidos revelam que a PAPR atinge valores elevados à medida que α aumenta, ou seja, mais potência é alocada ao AN.

Figura 11 – CCDF empírica da PAPR quando se utiliza o canal de Bob para projetar o AN sob valores distintos de α, considerando o esquema SC-CP.



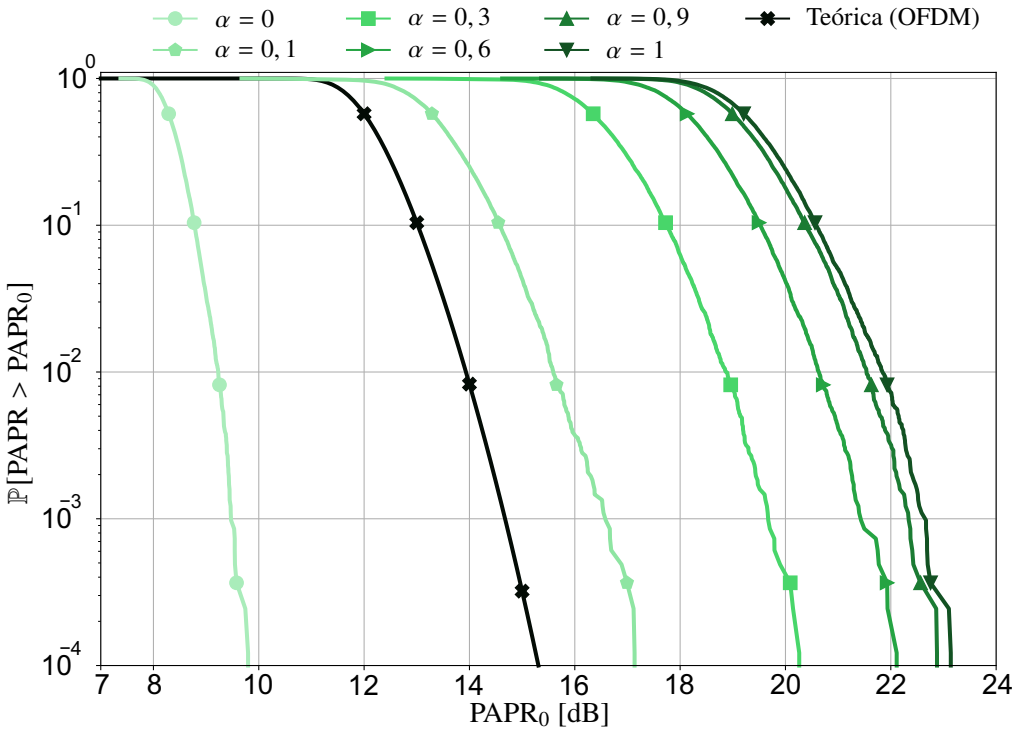
Fonte: Acervo do autor.

Figura 12 – CCDF empírica da PAPR quando se utiliza o canal de Eve, no cenário SP, para projetar o AN sob valores distintos de α, considerando o esquema SC-CP.



Fonte: Acervo do autor.

Figura 13 – CCDF empírica da PAPR quando se utiliza o canal de Eve, no cenário LP, para projetar o AN sob valores distintos de α, considerando o esquema SC-CP.



Fonte: Acervo do autor.

5 CONSIDERAÇÕES FINAIS

Neste trabalho, investigou-se os efeitos da introdução de um ruído artificial, projetado com base nos graus de liberdade introduzidos pelo CP, em redes PLC residenciais na presença de intrusos PLC ou sem fio. O esquema OFDM Hermitiano simétrico e as fases de transmissão e recepção do bloco de informação, juntamente com o ruído artificial, foram minuciosamente detalhados. A partir da apresentação do modelo do sistema, o projeto do ruído artificial foi descrito em detalhes, assim como as expressões para a relação sinal-ruído do receptor legítimo e dos intrusos. O ruído artificial foi desenvolvido de modo a degradar significativamente a relação sinal-ruído de Eve, enquanto tem um impacto mínimo na de Bob. Foram gerados resultados numéricos, expressos em termos de BER para cenários distintos. A variação na alocação de potência para o ruído artificial também foi considerada, e o sinal transmitido foi analisado em termos de PAPR, abrangendo diferentes esquemas de modulação e canais PLC.

A análise numérica em termos de BER indicou que o ruído artificial pode degradar o desempenho de um intruso passivo localizado próximo do transmissor legítimo, resultando em um aumento significativo da BER do intruso. Por outro lado, quando o intruso está próximo ao receptor legítimo, a efetividade do ruído artificial diminui, causando apenas um ligeiro aumento em sua BER. Vale ressaltar que, ao comparar intrusos com diferentes interfaces de comunicação, o intruso PLC foi identificado como uma ameaça mais significativa à rede PLC. Também é importante destacar que o ruído artificial gerado a partir dos graus de liberdade do prefixo cíclico tem um impacto substancial na PAPR do sinal transmitido. Logo, conforme mais potência é alocada para o ruído artificial, a PAPR atinge valores mais elevados. Além disso, a PAPR do sinal transmitido não apresenta diferenças significativas de acordo com o canal PLC utilizado no projeto do ruído artificial. Adicionalmente, para a técnica de injeção de ruído artificial assumida, o esquema de modulação considerado parece ter uma influência pequena na PAPR do sinal transmitido. Finalmente, como trabalhos futuros, pode-se mencionar uma análise estatística da técnica de injeção de ruído artificial, bem como uma investigação de técnicas de redução de PAPR voltadas para o ruído artificial.

REFERÊNCIAS

[1] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[2] J. Cortes, F. Canete, L. Diez, and J. Entrambasaguas, "Characterization of the cyclic short-time variation of indoor power-line channels response," in *Proc. International Symposium on Power Line Communications and Its Applications.*, 2005, pp. 326–330.

[3] J. A. Cortés, F. J. Cañete, L. Díez, and J. L. G. Moreno, "On the statistical properties of indoor power line channels: Measurements and models," in *Proc. IEEE International Symposium on Power Line Communications and Its Applications*, 2011, pp. 271–276.

[4] A. Cataliotti, V. Cosentino, D. Di Cara, and G. Tinè, "Measurement issues for the characterization of medium voltage grids communications," *IEEE Transactions on Instrumentation and Measurement*, vol. 62, no. 8, pp. 2185–2196, Aug. 2013.

[5] 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, Nov. 2014.

[6] T. R. Oliveira, F. J. A. Andrade, A. M. Picorone, H. A. Latchman, S. L. Netto, and M. V. Ribeiro, "Characterization of hybrid communication channel in indoor scenario," *Journal of Communication and Information Systems*, vol. 31, no. 1, pp. 224–235, Sept. 2016.

[7] A. Pittolo and A. Tonello, "Physical layer security in power line communication networks: An emerging scenario, other than wireless," *IET Communications*, vol. 8, pp. 1239–1247, May 2014.

[8] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Nov. 1975.

[9] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, July 1978.

[10] Â. 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, Mar. 2021.

[11] V. Mohan, A. Mathur, V. Aishwarya, and S. Bhargav, "Secrecy analysis of PLC system with channel gain and impulsive noise," in *Proc. IEEE Vehicular Technology Conference*, 2019, pp. 1–6.

[12] 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.

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

[14] Â. 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.

[15] Â. Camponogara, R. D. Souza, and M. V. Ribeiro, "The effective secrecy throughput of a broadband power line communication system under the presence of colluding wireless eavesdroppers," *IEEE Access*, vol. 10, pp. 85 019–85 029, 2022.

[16] Â. 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 of Things Journal*, vol. 6, no. 2, pp. 2760–2769, April 2019.

[17] 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 International Conference on Communications*, 2018, pp. 1–6.

[18] Y. Zhuang and L. Lampe, "Physical layer security in MIMO power line communication networks," in *Proc. 18th IEEE International Symposium on Power Line Communications and Its Applications*, 2014, pp. 272–277.

[19] G. Prasad, O. Taghizadeh, L. Lampe, and R. Mathar, "Securing MIMO power line communications with full-duplex jamming receivers," in *Proc. IEEE International Symposium on Power Line Communications and its Applications*, 2019, pp. 1–6.

[20] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Transactions on Wireless Communications*, vol. 12, no. 6, pp. 2717–2729, June 2013.

[21] Â. Camponogara and M. V. Ribeiro, "The effective secrecy throughput for the hybrid wiretap channel: Analysis based on a measurement campaign," *Journal of Communication and Information Systems*, vol. 36, no. 1, p. 44–51, Feb. 2021.

[22] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Transactions on Modeling and Computer Simulation*, vol. 8, no. 1, p. 3–30, Jan. 1998.

[23] 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 Transactions on Communications*, vol. 64, no. 2, pp. 778–789, Feb. 2016.

[24] G. Prasad, L. Lampe, and S. Shekhar, "In-band full duplex broadband power line communications," *IEEE Transactions on Communications*, vol. 64, no. 9, pp. 3915–3931, Sept. 2016.

[25] S. H. Han and J. H. Lee, "An overview of peak-to-average power ratio reduction techniques for multicarrier transmission," *IEEE Wireless Communications*, vol. 12, no. 2, pp. 56–65, April 2005.

[26] H. Yu, M. Chen, and G. Wei, "Distribution of PAR in DMT systems," *Electronics Letters*, vol. 39, pp. 799 – 801, June 2003.

[27] G. Strang, "Positive definite matrices," in *Linear algebra and its applications*, 4th ed. Thomson, Brooks/Cole, 2006, pp. 345–389.

[28] R. van de Geijn and M. Myers, "The singular value decomposition," in *Advanced Linear Algebra: Foundations to Frontiers*, 1st ed. University of Texas, Jan. 2022, pp. 58–101.

Apêndice A – Decomposição em Valores Singulares

Neste apêndice, apresenta-se a decomposição em valores singulares, que decompõe uma matriz num produto de outras três matrizes (fatores) [27, 28]. Nesse contexto, dada uma matriz $\mathbf{A} \in \mathbb{C}^{m\times n}$ qualquer de posto r, existe uma matriz unitária $\mathbf{U} \in \mathbb{C}^{m\times m}$, uma matriz unitária $\mathbf{V} \in \mathbb{C}^{n\times n}$ e uma matriz diagonal $\mathbf{\Sigma} \in \mathbb{R}^{m\times n}$, tal que

$$\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\dagger}. \tag{A.1}$$

Na equação anterior,

$$\begin{aligned} \mathbf{V}^{\dagger} &= \left[\begin{array}{cccc|ccc} \mathbf{v}_1^{\dagger} & \mathbf{v}_2^{\dagger} & \cdots & \mathbf{v}_r^{\dagger} & \mathbf{v}_{r+1}^{\dagger} & \cdots & \mathbf{v}_n^{\dagger} \end{array}\right]^{\mathrm{T}} \\ &= \left[\begin{array}{c|c} \mathbf{V}_{\mathcal{R}}^{\dagger} & \mathbf{V}_{\mathcal{N}}^{\dagger} \end{array}\right]^{\mathrm{T}}, \end{aligned} \tag{A.2}$$

em que $\mathbf{V}_{\mathcal{R}}^{\dagger} = \left[\begin{array}{cccc} \mathbf{v}_1^{\dagger} & \mathbf{v}_2^{\dagger} & \cdots & \mathbf{v}_r^{\dagger} \end{array}\right]^{\mathrm{T}} \in \mathbb{C}^{r\times n}$ e $\mathbf{V}_{\mathcal{N}}^{\dagger} = \left[\begin{array}{ccc} \mathbf{v}_{r+1}^{\dagger} & \cdots & \mathbf{v}_n^{\dagger} \end{array}\right]^{\mathrm{T}} \in \mathbb{C}^{(n-r)\times n}$, tal que $\mathbf{v}_j \in \mathbb{C}^{n\times 1}$, $\forall\, j \in \{1, 2, \ldots, n\}$, representa, o j-ésimo autovetor de $\mathbf{A}^{\dagger}\mathbf{A}$;

$$\begin{aligned} \mathbf{U} &= \left[\begin{array}{cccc|ccc} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_r & \mathbf{u}_{r+1} & \cdots & \mathbf{u}_m \end{array}\right] \\ &= \left[\begin{array}{c|c} \mathbf{U}_{\mathcal{R}} & \mathbf{U}_{\mathcal{N}} \end{array}\right], \end{aligned} \tag{A.3}$$

em que $\mathbf{U}_{\mathcal{R}} = \left[\begin{array}{cccc} \mathbf{u}_1 & \mathbf{u}_2 & \cdots & \mathbf{u}_r \end{array}\right] \in \mathbb{C}^{m\times r}$ e $\mathbf{U}_{\mathcal{N}} = \left[\begin{array}{ccc} \mathbf{u}_{r+1} & \cdots & \mathbf{u}_m \end{array}\right] \in \mathbb{C}^{m\times(m-r)}$, tal que $\mathbf{u}_z \in \mathbb{C}^{m\times 1}$, $\forall\, z \in \{1, 2, \ldots, m\}$, representa, o z-ésimo autovetor de $\mathbf{A}\mathbf{A}^{\dagger}$; e

$$\mathbf{\Sigma} = \left[\begin{array}{cccc:c} \sigma_1 & 0 & \cdots & 0 & \\ 0 & \sigma_2 & \cdots & 0 & \\ \vdots & \vdots & \ddots & \vdots & \mathbf{0}_{r\times(n-r)} \\ 0 & 0 & \cdots & \sigma_r & \\ \hdashline \multicolumn{4}{c:}{\mathbf{0}_{(m-r)\times r}} & \mathbf{0}_{(m-r)\times(n-r)} \end{array}\right], \tag{A.4}$$

cujos r elementos da diagonal principal, representados por $\sigma_w, \forall w \in \{1, 2, \ldots, r\}$, são chamados de valores singulares de $\mathbf{A}$. Os valores singulares são as raízes quadradas dos autovalores não nulos de $\mathbf{A}^{\dagger}\mathbf{A}$ e $\mathbf{A}\mathbf{A}^{\dagger}$, e são usualmente ordenados de forma que

$$\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_r \geq 0. \tag{A.5}$$

Uma vez que $\mathbf{A}$ possui posto r, as colunas da matriz $\mathbf{U}_{\mathcal{R}} \in \mathbb{C}^{m\times r}$ fornecem uma base ortonormal para o espaço-coluna de $\mathbf{A}$. De forma similar, as colunas da matriz $\mathbf{V}_{\mathcal{R}} \in \mathbb{C}^{n\times r}$ fornecem uma base ortonormal para o espaço-linha de $\mathbf{A}$. Finalmente, as colunas de $\mathbf{U}_{\mathcal{N}} \in \mathbb{C}^{m\times(m-r)}$ e $\mathbf{V}_{\mathcal{N}} \in \mathbb{C}^{n\times(n-r)}$ fornecem, respectivamente, uma base ortonormal para o espaço nulo esquerdo de $\mathbf{A}$ e uma base ortonormal para o espaço nulo direito de $\mathbf{A}$. Ademais, por serem matrizes unitárias tem-se que:

$$\mathbf{U}\mathbf{U}^{\dagger} = \mathbf{I}_m \tag{A.6}$$

e

$$\mathbf{V}\mathbf{V}^{\dagger} = \mathbf{I}_n. \tag{A.7}$$

Para o caso em que $\mathbf{A} \in \mathbb{R}^{m \times n}$, tem-se que $\mathbf{\Sigma}$ permanece real, mas $\mathbf{U}$ e $\mathbf{V}$ passam a ser matrizes reais, e ao invés de unitárias, as matrizes $\mathbf{U}$ e $\mathbf{V}$ se tornam ortogonais, ou seja, $\mathbf{U}\mathbf{U}^{\mathrm{T}} = \mathbf{I}_m$ e $\mathbf{V}\mathbf{V}^{\mathrm{T}} = \mathbf{I}_n$. Além disso, toma-se a transposta de $\mathbf{V}$ para decomposição de $\mathbf{A}$, ou seja, $\mathbf{A} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^{\mathrm{T}}$.