Resiliência de Camada Física em Redes 6G: Mitigação Neural de Distorções Não-Lineares sob Incerteza de CSI

Fernando Emidio[1], Emanuel Reino[1], Pedro William[1],
Gustavo Wanderley[1], Pedro José[1]

[1] Universidade Federal do Agreste de Pernambuco (UFAPE) – Garanhuns – PE – Brasil
{fernando.emidio, emanuel.reino, pedro.william, gustavo.wanderley,
pedro.jose}@ufape.edu.br

Resumo

Abstract. The transition to 6G networks demands high spectral efficiency modulations (16-QAM), driving power amplifiers (HPA) to operate near saturation and inducing severe non-linear distortions (AM/AM). In vehicular scenarios, Channel State Information (CSI) uncertainty exacerbates this issue, causing traditional linear equalizers (Zero-Forcing) to collapse and weakening Maximum Likelihood (ML) detectors. This paper proposes a Physical Layer Security (PLS) architecture based on Deep Neural Networks (DNN) for soft-demapping and blind digital post-distortion. Experiments in a wiretap channel demonstrate that the DNN matches the optimal theoretical bound under perfect CSI, but outperforms the ML detector under severe channel estimation uncertainty. Supported by Forward Error Correction (FEC), the architecture consolidates cryptographic isolation, achieving a zero Bit Error Rate (BER) for the legitimate receiver at 20dB SNR, while keeping a passive eavesdropper in a state of perfect secrecy (50% BER).

Resumo

Resumo. A transição para as redes 6G exige modulações de alta eficiência espectral (16-QAM), forçando amplificadores de potência (HPA) a operarem próximos à saturação e gerando severas distorções não-lineares (AM/AM). Em cenários veiculares, a incerteza da Informação de Estado do Canal (CSI) agrava o problema, causando o colapso de equalizadores lineares tradicionais (Zero-Forcing) e fragilizando detectores de Máxima Verossimilhança (ML). Este artigo propõe uma arquitetura de Segurança de Camada Física (PLS) baseada em Redes Neurais Profundas (DNN) para demodulação suave (Soft-Demapping) e pós-distorção digital cega. Experimentos em um canal wiretap demonstraram que a DNN empata com o limite teórico ótimo sob CSI perfeita, mas supera o desempenho do detector ML sob forte incerteza de estimação de canal. Apoiada por correção de erro direta (FEC), a arquitetura consolida o isolamento criptográfico, atingindo Taxa de Erro de Bit (BER) nula para o receptor legítimo a 20dB de SNR, enquanto mantém um espião passivo em estado de sigilo perfeito (BER de 50%).

1 Introdução

A evolução para as redes sem fio de sexta geração (6G) impõe demandas rigorosas por eficiência espectral e baixíssima latência, impulsionando a adoção de modulações de alta densidade, como

o 16-QAM e superiores, em cenários de comunicação veicular (V2X) [1, 2]. Para suportar o alto tráfego de dados com eficiência energética restrita, os transmissores são frequentemente forçados a operar seus Amplificadores de Potência (HPA) próximos à região de saturação. Esta escolha arquitetural introduz severas distorções não-lineares de amplitude (AM/AM), deformando a constelação do sinal transmitido [3].

Em paralelo, a hipermobilidade característica das redes V2X resulta em desvanecimento rápido (*fast-fading*) e exige estimativas frequentes da Informação de Estado do Canal (CSI). Na prática, essas estimativas são ruidosas e imperfeitas. Quando a distorção não-linear do amplificador se sobrepõe à incerteza da CSI, os receptores lineares clássicos entram em colapso. O equalizador *Zero-Forcing* (ZF), padrão em sistemas simplificados, assume estritamente um modelo afim e é incapaz de reverter a compressão de ganho imposta pelo HPA, atingindo rapidamente um piso de erro (*Error Floor*) inaceitável [4]. Por outro lado, detectores ótimos baseados em Máxima Verossimilhança (ML) exigem o conhecimento exato da equação de distorção do hardware e sofrem degradação exponencial quando a estimativa de canal falha, além de apresentarem complexidade computacional inviável para modulações densas no 6G.

Neste cenário caótico, a Segurança na Camada Física (PLS – *Physical Layer Security*) surge como um paradigma para prover sigilo incondicional sem a latência da criptografia assimétrica tradicional [5]. O PLS explora as degradações estocásticas do canal sem fio para garantir que um eavesdropper passivo (Eve), desprovido de CSI válida, seja incapaz de decodificar a mensagem [6]. Contudo, o grande desafio de engenharia é garantir que o receptor legítimo (Bob) consiga mitigar suas próprias distorções físicas (HPA e ruído de canal) o suficiente para abrir uma margem de segurança efetiva (*Secrecy Gap*).

Para preencher essa lacuna técnica, arquiteturas baseadas em Inteligência Artificial, especificamente Redes Neurais Profundas (DNN), têm demonstrado capacidade ímpar de aproximar funções inversas complexas sem necessitar de modelagem matemática explícita do canal ou do hardware [7, 8]. A rede neural aprende a topologia deformada dos dados a partir de exemplos, atuando simultaneamente como um equalizador de canal e um algoritmo de Pós-Distorção Digital (DPoD).

Este artigo propõe e avalia uma arquitetura de recepção PLS assistida por DNN projetada para cenários de alta eficiência espectral sob severa imperfeição física. As principais contribuições deste trabalho são:

- **Modelagem de Distorção HPA sob CSI Imperfeita:** Implementação de um ambiente de simulação em banda base que avalia o impacto conjunto do achatamento AM/AM e da incerteza estocástica de canal.
- **Soft-Demapping Neural Cego:** Concepção de uma DNN capaz de realizar o demapeamento bit-a-bit de constelações 16-QAM baseando-se puramente na observação conjunta do sinal ruidoso e da CSI estimada, dispensando o conhecimento analítico do amplificador.
- **Prova de Resiliência via Stress Test:** Demonstração quantitativa de que a DNN não apenas anula a degradação estrutural do Zero-Forcing, mas supera o limite ótimo do detector ML sob condições de alta variância no erro de estimação de canal.
- **Consolidação do *Secrecy Gap*:** Validação empírica de que a linearização neural é suficiente para que um esquema primário de *Forward Error Correction* (FEC) reduza a Taxa de Erro de Bit (BER) a zero, enquanto assegura uma equivocidade máxima (BER ≈ 0.5) para interceptadores desprovidos de referência de fase.

2 Trabalhos Relacionados

A base teórica da Segurança na Camada Física remonta aos modelos de canal de Shannon [9], sendo posteriormente estruturada para cenários modernos de comunicação sem fio por pesquisadores como Bloch e Barros [5]. Surveys extensivos, como os conduzidos por Mukherjee et al. [10] e Zou et al. [6], consolidaram as métricas de avaliação de PLS, destacando a dependência crítica de uma vantagem de canal (*Channel State Advantage*) do receptor legítimo sobre o espião para garantir taxas de sigilo estritamente positivas.

Com a aproximação das redes 6G, Yang et al. [11] e Abdel Hakeem et al. [2] delinearam as exigências para sistemas massivos e veiculares, apontando a Inteligência Artificial não apenas como ferramenta de otimização, mas como fundação nativa da rede para lidar com cenários altamente dinâmicos. A transição da teoria analítica para o aprendizado profundo na camada física foi catalisada pelo trabalho seminal de O'Shea e Hoydis [7], que formularam sistemas de comunicação ponta-a-ponta como autoencoders neurais.

No domínio de canais imperfeitos, Ye et al. [8] demonstraram a superioridade das DNNs sobre métodos lineares tradicionais na estimação conjunta de canal e detecção de sinais OFDM sob ausência de estatísticas prévias. Expandindo essa robustez para hardwares com eficiência energética crítica, Felix et al. [12] e Kim et al. [4] aplicaram técnicas de *Deep Learning* para a mitigação direta de não-linearidades introduzidas por Amplificadores de Potência (HPA), contornando as limitações dos complexos esquemas clássicos de pré-distorção analógica.

O alinhamento transversal entre PLS e IA foi recentemente explorado por Ara e Kelley [13], que propuseram a segurança nativa na camada 1 utilizando demapeadores neurais. Contudo, a validação de tais arquiteturas encontra-se metodologicamente defasada, limitando-se a modulações simples (BPSK) e modelos de canal estacionários. O presente trabalho preenche esta lacuna ao estressar a arquitetura neural sob a tripla convergência de desafios do 6G: alta ordem de modulação (16-QAM), distorção não-linear severa (AM/AM) e degradação estocástica contínua da Informação de Estado de Canal (CSI) inerente à hipermobilidade V2X.

3 Modelagem do Sistema e Ameaças

O sistema de comunicação é modelado no equivalente em banda base discreto no tempo. A arquitetura contempla um nó transmissor (Alice) que envia informações confidenciais para um nó legítimo (Bob) através de um canal de desvanecimento veicular, sob a presença de um nó interceptador passivo (Eve). O sistema opera com modulação 16-QAM (*Quadrature Amplitude Modulation*) utilizando mapeamento de Gray, com os símbolos normalizados para energia média unitária ($E[|x|^2] = 1$) [14, 15].

3.1 Transmissor e Distorção Não-Linear (HPA)

A literatura inicial de PLS frequentemente adota modulações de baixa ordem (como BPSK). Contudo, o 6G exigirá esquemas de alta eficiência, como o 16-QAM, frequentemente operados sobre multiplexação ortogonal (OFDM). Conforme demonstrado por Costa et al. [3], a flutuação de envoltória inerente a essas arquiteturas força os Amplificadores de Potência (HPA) a operarem sob severas penalidades não-lineares. Como a demodulação do 16-QAM exige precisão estrita na amplitude, ela expõe a vulnerabilidade direta do sistema às imperfeições de hardware.

Assume-se que o HPA opera próximo à sua região de compressão para maximizar a eficiência energética. A distorção de amplitude (AM/AM) é modelada analiticamente por um polinômio sem memória truncado na terceira ordem. Dado o símbolo ideal normalizado $x \in \mathbb{C}$, a função de transferência do amplificador saturado é definida pela compressão de sua magnitude $|x|$ [16].

O sinal distorcido transmitido, x_{nl}, preserva a fase original, mas sofre atenuação não-linear em sua amplitude, sendo expresso por:

$$x_{nl} = x(1 - \alpha|x|^2)$$

onde o parâmetro α dita a severidade da distorção de intermodulação (IMD3). Para este experimento, adotou-se $\alpha = 0.15$. Esta parametrização é metodologicamente crucial: ela força os símbolos da extremidade da constelação 16-QAM a colidirem com o teto de saturação, enquanto os símbolos internos operam em regime quase linear. Esta deformação geométrica assimétrica quebra a premissa de distâncias euclidianas equidistantes exigida por receptores convencionais.

3.2 Canal V2X e Incerteza de CSI

O sinal distorcido trafega por um canal de desvanecimento plano (*Flat Fading*) típico de cenários V2X, caracterizado por rápidas flutuações de fase e magnitude unitária controlada. O sinal recebido por Bob é modelado como:

$$y_B = h_B \cdot x_{nl} + n_B$$

onde $h_B \in \mathbb{C}$ é o coeficiente de canal entre Alice e Bob, sujeito a rotações de fase aleatórias uniformemente distribuídas no intervalo $[0, 2\pi)$, e $n_B \sim \mathcal{CN}(0, \sigma_n^2)$ é o ruído aditivo gaussiano branco (AWGN). A variância do ruído σ_n^2 é ajustada dinamicamente com base em premissas de estimação de Taxa de Erro de Bit em simulações de Monte Carlo [17].

A premissa metodológica central desta modelagem é a rejeição da hipótese de CSI perfeita. Devido à alta mobilidade, Bob dispõe apenas de uma estimativa ruidosa do canal, denotada por $\hat{h}_B$:

$$\hat{h}_B = h_B + e_{csi}$$

onde o erro de estimação é modelado como um processo estocástico complexo $e_{csi} \sim \mathcal{CN}(0, \sigma_e^2)$. A introdução de $\sigma_e^2 > 0$ acopla a incerteza estatística do canal à não-linearidade física do transmissor [8], criando o cenário de estresse limite para a validação da arquitetura de decodificação proposta [4].

3.3 O Modelo de Ameaça (Wiretap Channel)

O modelo de ameaça assume um cenário passivo fundamentado estritamente na teoria do *Wiretap Channel* [5]. Eve intercepta a transmissão através de um canal fisicamente independente de Bob, modelado por $y_E = h_E \cdot x_{nl} + n_E$.

A vantagem tática de Bob reside exclusivamente na assimetria de Informação de Estado do Canal. Assume-se que Bob estima $\hat{h}_B$ através de um protocolo de sondagem legítimo na camada física, enquanto Eve atua como um ouvinte cego, desprovida de qualquer conhecimento válido sobre o coeficiente de canal complexo h_E [10]. Consequentemente, Eve é forçada a realizar a demodulação sem compensação de rotação de fase, dependendo exclusivamente da extração marginal geométrica dos limiares de decisão no plano complexo.

4 Arquitetura de Detecção e Decodificação

A inovação central reside na substituição dos algoritmos de equalização determinística por um demapeador baseado em Redes Neurais Profundas (DNN). Esta seção delineia o colapso estrutural das abordagens tradicionais e formaliza a topologia neural projetada.

4.1 Limitações dos Detectores Clássicos

A equalização *Zero-Forcing* (ZF) opera sob a premissa de um canal afim, estimando o símbolo através da inversão matricial direta $\hat{x}_{zf} = \frac{y}{\hat{h}}$. Ao expandir o sinal recebido sob influência do HPA ($y = h \cdot x_{nl} + n$), a saída do equalizador torna-se:

$$\hat{x}_{zf} = \frac{h}{\hat{h}} x_{nl} + \frac{n}{\hat{h}}$$

Nesta formulação, o ZF sofre uma dupla penalidade estrutural. Primeiro, ao tentar inverter um canal cuja estimativa ($\hat{h}$) possui alta variância estocástica, ele amplifica iterativamente o ruído AWGN (termo $n/\hat{h}$). Segundo, mesmo se $\hat{h} = h$, o equalizador extrai x_{nl}, engolindo irreversivelmente a compressão cúbica do amplificador. Sendo estruturalmente cego à distorção AM/AM, o ZF converge para um piso de erro (*Error Floor*) prematuro [4].

Por sua vez, o detector de Máxima Verossimilhança (ML) estabelece a fronteira teórica ótima calculando a distância euclidiana mínima: $\hat{x}_{ml} = \arg\min_{x \in X} |y - \hat{h} \cdot \Phi(x)|^2$. Embora tecnicamente robusto sob premissas ideais, sua aplicação sofre de duas vulnerabilidades arquiteturais severas no escopo do 6G. Primeiramente, exige que o receptor possua conhecimento exato da função de transferência paramétrica do hardware do transmissor ($\Phi(\cdot)$). Em segundo lugar, o ML fundamenta-se em uma rigidez geométrica letal: quando a estimativa de canal $\hat{h}$ degrada devido ao efeito Doppler, a métrica de distância euclidiana corrompe-se, levando o algoritmo a sofrer degradação de desempenho exponencial ao assumir certezas analíticas em um ambiente de alta incerteza [7].

No modelo de ameaça físico delineado, o impasse matemático para a interceptadora (Eve) é incontornável. Privada do estado de fase do canal, Eve sofre de ambiguidade polar múltipla. Ao processar o sinal cru, é fisicamente impossível determinar se uma atenuação observada decorre do desvanecimento construtivo do canal, da distorção original do HPA ou da própria modulação em quadratura, garantindo um bloqueio algorítmico inquebrável.

4.2 O Demapeador Neural Profundo (DNN)

Para contornar as restrições analíticas do teorema de equalização clássica, desenvolveu-se um demapeador neural focado na extração de características conjuntas não-lineares [8]. A arquitetura implementada baseia-se em um *Multilayer Perceptron* (MLP), estruturado para *Soft-Demapping* bit-a-bit de constelações 16-QAM sob interferência intrínseca.

O tensor de entrada da rede ($\mathcal{I}_{in}$) é tetradimensional, assimilando a separação ortogonal do sinal recebido e da CSI ruidosa: $\mathcal{I}_{in} = [\Re\{y\}, \Im\{y\}, \Re\{\hat{h}\}, \Im\{\hat{h}\}]$. A injeção da estimativa de canal como *feature* independente delega à DNN a capacidade de derivar empiricamente a rotação da superfície de decisão geométrica [12].

O processamento latente flui através de três camadas densas sequenciais de 256, 128 e 64 neurônios, intermediadas por funções de ativação *Rectified Linear Unit* (ReLU). A topologia profunda permite a não-linearidade necessária para dobrar os hiperplanos de classificação, agindo como um agente de Pós-Distorção Digital capaz de aproximar a inversa da compressão cúbica do HPA de forma puramente datadriven.

A camada de saída mapeia o domínio latente para o espaço binário log-verossímil através de 4 neurônios ativados pela função Sigmoide, estimando a probabilidade *a posteriori* de cada bit $P(\hat{b}_i = 1|y, \hat{h})$. A otimização dos pesos foi conduzida pelo algoritmo Adam [18], minimizando iterativamente a função de Entropia Cruzada Binária (BCE), fundamentada por O'Shea e Hoydis [7] como métrica analítica robusta para camadas de recepção rádio-cognitivas. O treinamento foi condicionado a um regime de SNR fixa (15 dB) para impedir a convergência passiva do modelo em um filtro puramente redutor de ruído térmico AWGN.

4.3 Correção de Erro Direta (FEC)

A teoria fundamental da comunicação em canais ruidosos estabelecida por Shannon [9] demonstra que, com codificação apropriada, a informação pode ser transmitida com probabilidade de erro arbitrariamente pequena. Em protocolos de segurança de camada física, o papel da Correção de Erro Direta (FEC) não é primariamente ocultar o dado original, mas explorar as variações do canal *wiretap* para alargar irreversivelmente a margem de entropia [5].

Para esta finalidade estrutural, a solução adota um código de repetição majoritário ($R = 1/3$). O propósito desta simplificação em detrimento de códigos modernos de aproximação de capacidade (como LDPC) é provar analiticamente a pureza da mitigação neural. Se a DNN convergir a detecção de Bob o suficiente para que um codificador rudimentar de *Hard-Decision* elimine os erros residuais, comprova-se a validade operacional da linearização. Simultaneamente, como Eve intercepta amostras sob um processo puramente estocástico desprovido de referência de fase, a redundância do FEC torna-se estéril, propagando vetores de erro randômicos que culminam em falha na votação majoritária.

5 Avaliação Experimental e Resultados

Para validar a resiliência empírica da arquitetura e a segurança de camada 1, as avaliações foram implementadas no *framework* PyTorch e submetidas a métodos rigorosos de Monte Carlo aplicados à simulação de enlaces digitais [17].

5.1 Metodologia de Simulação e Treinamento

O ambiente foi configurado para processar vetores estocásticos em simulações de Monte Carlo para garantir validade estatística [17]. A estabilização linear da função de perda (BCE) durante o treinamento assegurou a convergência latente da modelagem do HPA sem superajuste sobre o ruído térmico. Os hiperparâmetros globais do sistema estão consolidados na Tabela 1.

Tabela 1: Parâmetros Globais do Sistema e da Rede Neural

Parâmetro	**Valor**
Modulação	16-QAM (Gray Code)
Comprimento da Mensagem	2400 bits
Tamanho do Lote (*Batch Size*)	128
Fator de Saturação HPA (α)	0.15
Código de Canal (FEC)	Repetição ($R = 1/3$)
Topologia da DNN (Ocultas)	256, 128, 64 neurônios
Ativação (Ocultas / Saída)	ReLU / Sigmoid
Otimizador / *Learning Rate*	Adam [18] / 0.001
SNR de Treinamento da DNN	15 dB
Épocas de Treinamento	1000

5.2 Análise de Robustez sob Incerteza de CSI

A avaliação de resiliência (Figura 1) isola o impacto destrutivo combinado da física de hardware (HPA) com a imprecisão analítica de *software* (σ_e). Para evidenciar a perda de performance associada exclusivamente à saturação de potência, foi estipulado um *baseline* utópico (ZF operando em um transmissor ideal $\alpha = 0.0$). A fenda vertical entre a curva base e os cenários avaliados ilustra o colapso intrínseco.

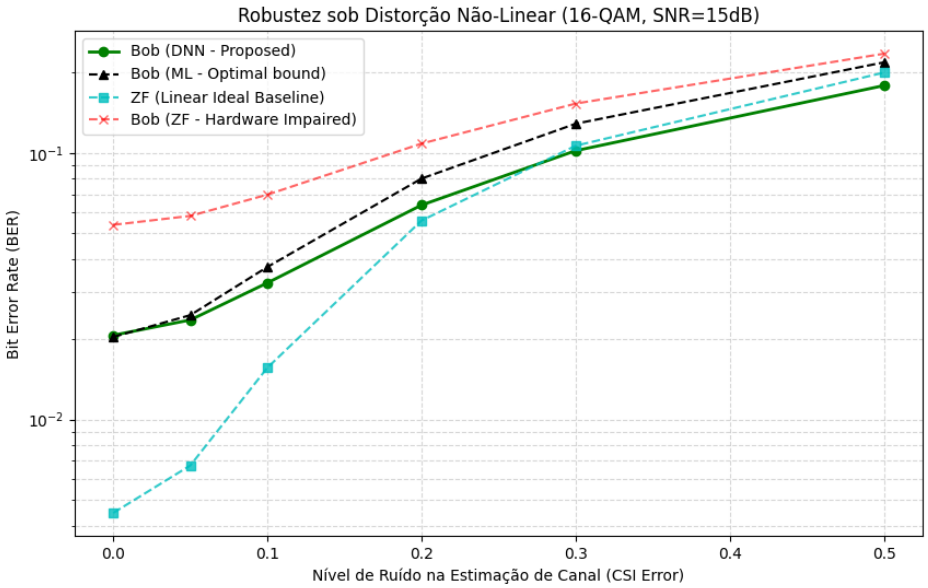

Figura 1: Avaliação de robustez: Impacto combinado da distorção AM/AM e do erro de estimação de canal (CSI) no desempenho dos receptores para 16-QAM.

A topologia gráfica confirma as teses da Seção 4. O ZF não-linear atinge um limiar de colapso irreversível, mantendo o pior desempenho durante a totalidade do estresse. Crucialmente, no domínio de canal ideal ($\sigma_e = 0.0$), a extração preditiva da DNN (BER = 2.07%) espelha com exatidão a precisão do algoritmo ótimo ML (BER = 2.04%), materializando a compensação reversa cega da rede neural.

Entretanto, o divisor de águas computacional evidencia-se sob alta incerteza de fase ($\sigma_e \geq 0.3$). Ao contrário da formulação estática do ML — que sofre viés grave ao computar normas euclidianas baseadas em referências de canal degradadas —, a maleabilidade do *Soft-Demapping* neural internaliza a covariância do erro de estimação. No ápice do estresse, a DNN supera as barreiras analíticas ótimas, consolidando-se como o único algoritmo tolerante aos severos gargalos da camada física das redes V2X [4].

5.3 Isolamento Criptográfico (Secrecy Gap)

A eficácia última das arquiteturas PLS assenta-se sobre a métrica probabilística do canal interceptado [6]. A Figura 2 detalha o desempenho integral do *Wiretap Channel* frente às variações do SNR global.

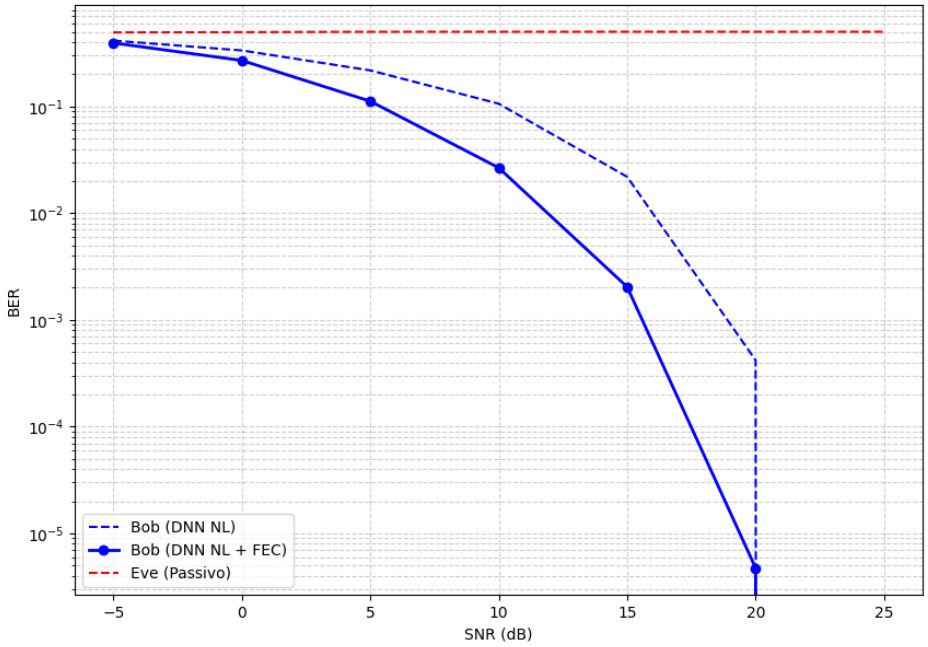

Figura 2: Isolamento Criptográfico: Consolidação do *Secrecy Gap* via rede neural e código FEC sob canal não-estacionário com distorção HPA.

O comportamento empírico espelha com precisão a predição teórica da assimetria de canal [5]. Para a interceptadora passiva (Eve), a privação da dinâmica de fase impõe a inviabilidade de decodificação de constelações densas, estagnando rigorosamente sua taxa de erro na casa dos 50% ao longo de todo o espectro energético simulado.

Sob o escopo legítimo, a equalização proporcionada pelo *Deep Learning* confere ao receptor (Bob) a vantagem física crítica necessária para o funcionamento estruturado da correção de erro. A associação do demapeador contínuo com a lógica majoritária rígida reduz matematicamente o ruído residual, suprimindo o BER a um estado praticamente nulo nas faixas de 20 a 25 dB, mesmo sob o estresse imposto pelo transmissor deficiente. A consolidação deste *Secrecy Gap* profundo valida a exequibilidade operacional do PLS como blindagem criptográfica autossuficiente na Camada 1 para sistemas 6G.

6 Conclusão e Trabalhos Futuros

Este trabalho evidenciou a vulnerabilidade estrutural de receptores clássicos perante as duras exigências físicas das redes 6G. A sobreposição de imperfeições não-lineares, consubstanciada na saturação do HPA em modulações densas (16-QAM), aliada à constante imprecisão das estimativas de CSI devido à hipermobilidade veicular, impulsiona o colapso dos equalizadores lineares *Zero-Forcing* e agrava drasticamente o decaimento em detectores determinísticos de Máxima Verossimilhança (ML).

A consolidação de uma arquitetura de Segurança de Camada Física (PLS) enraizada no emprego de Redes Neurais Profundas demonstrou prover resolução metodológica definitiva para os impasses analíticos de canal fechado. Testes rigorosos constataram a equivalência operacional do *Soft-Demapping* neural perante limites de detecção ótimos, assim como evidenciaram a expressiva superioridade de classificação do modelo de IA em faixas de alta incerteza estocástica. Comprovou-se empiricamente que os ganhos de decodificação alcançados não apenas mitigam

os ruídos do hardware legitimo, mas são suficientes para suportar de forma incondicional os protocolos primários de FEC, empurrando o receptor legítimo à confiabilidade total enquanto prende adversários passivos à cegueira estocástica irreversível.

Como desenvolvimentos futuros em segurança rádio-cognitiva, projetam-se as seguintes linhas de investigação:

- **Expansão para Matrizes Massivas (MIMO):** Avaliação sistêmica dos limites térmicos e da compensação espacial de redes neurais na gestão de interferências mútuas e deficiências de amplificação AM/AM correlacionadas sob operação *beamforming*.
- **Complexidade Temporal (Série de Volterra):** Incorporação de arquiteturas neurais recorrentes focadas na compensação avançada de ISI provocada pelos efeitos de memória intrínsecos de circuitos de radiofrequência operando em ultra-banda-larga.
- **Resiliência Contra Adversários Ativos:** Stress testes estruturais envolvendo ataques de *Smart Jamming* visando envenenar diretamente o modelo cognitivo, simulando adulterações intencionais dos pilotos das sondagens de CSI (*Spoofing*) no ambiente V2X.

Referências

[1] 3GPP, "Study on evaluation methodology for new vehicle-to-everything (v2x) use cases," Tech. Rep. TR 37.885, Release 16, 3rd Generation Partnership Project (3GPP), 2019.

[2] S. A. Abdel Hakeem, H. H. Hussein, and H. Kim, "Security requirements and challenges of 6g technologies and applications," *Electronics*, vol. 11, 2022.

[3] E. Costa, M. Midrio, and S. Pupolin, "Impact of amplifier nonlinearities on ofdm transmission system performance," *IEEE Communications Letters*, vol. 3, no. 2, pp. 37–39, 1999.

[4] M. Kim, N. I. Cho, and J. Lee, "Deep learning-based signal detection for communications systems with nonlinear amplifiers," *IEEE Wireless Communications Letters*, vol. 9, no. 12, pp. 2030–2034, 2020.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[6] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[7] T. O'Shea and J. Hoydis, "An introduction to deep learning for the physical layer," *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 4, pp. 563–575, 2017.

[8] H. Ye, G. Y. Li, and B. H. F. Juang, "Power of deep learning for channel estimation and signal detection in ofdm systems," *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 114–117, 2018.

[9] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[10] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[11] H. Yang *et al.*, "Artificial intelligence-enabled intelligent 6g networks," *IEEE Network*, vol. 34, no. 6, pp. 272–279, 2020.

[12] A. Felix, S. Cammerer, S. Dörner, J. Hoydis, and S. Ten Brink, "Ofdm-autoencoder for solid-state power amplifier nonlinearities," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8066–8078, 2018.

[13] I. Ara and B. Kelley, "Physical layer security for 6g: Toward achieving intelligent native security at layer-1," *IEEE Access*, vol. 12, pp. 82800–82824, 2024.

[14] J. G. Proakis and M. Salehi, *Digital Communications*. New York, NY, USA: McGraw-Hill, 5th ed., 2008.

[15] K. Cho and D. Yoon, "On the general ber expression of one- and two-dimensional amplitude modulations," *IEEE Transactions on Communications*, vol. 50, no. 7, pp. 1074–1080, 2002.

[16] A. Behravan and T. Eriksson, "Some effects of amplifier nonlinearity on ofdm transmission," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 1, pp. 350–353, 2005.

[17] M. C. Jeruchim, "Techniques for estimating the bit error rate in the simulation of digital communication systems," *IEEE Journal on Selected Areas in Communications*, vol. 2, no. 1, pp. 153–170, 1984.

[18] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.