Segurança na Camada Física em Redes 6G com Deep Learning: Análise de Lacuna e Proposta Metodológica

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}@ufape.edu.br,

{gustavo.wanderley, pedro.jose}@ufape.edu.br

Abstract. *This paper proposes an advanced Physical Layer Security (PLS) framework for 6G networks, addressing the critical challenges of hyper-mobility. The core innovation lies in the integration of a Deep Neural Network (DNN) into the decoding process, replacing traditional linear detection methods. However, a significant research gap exists regarding the validation of such models in high-mobility scenarios, specifically Vehicle-to-Everything (V2X) environments. We propose a comparative methodology structured in three phases to validate the model in non-stationary channels, bridging the gap left by studies limited to stationary models like COST 259.*

Resumo. *Este artigo propõe um framework avançado de Segurança de Camada Física (PLS) para redes 6G, abordando os desafios críticos da hipermobilidade. A inovação central reside na integração de uma Rede Neural Profunda (DNN) no processo de decodificação, substituindo métodos lineares tradicionais. Entretanto, identifica-se uma lacuna significativa na literatura quanto à validação deste modelo em cenários de alta mobilidade, especificamente em ambientes Veículo-para-Tudo (V2X). Propõe-se uma metodologia comparativa em três fases para validar o modelo em canais não-estacionários, preenchendo o vácuo deixado por estudos limitados a modelos estacionários como o COST 259.*

1. Introdução

A iminente transição para as redes 6G promete suportar cenários de hipermobilidade complexos, incluindo veículos autônomos e trens de alta velocidade. Neste contexto desafiador, a Segurança na Camada Física (PLS – *Physical Layer Security*) emerge como uma solução robusta e leve, explorando as características estocásticas do canal sem fio para garantir o sigilo das comunicações sem depender excessivamente de criptografia de camada superior.

Recentemente, a literatura tem avançado na integração de Inteligência Artificial ao PLS. O trabalho de [Ara and Kelley 2024], por exemplo, propõe o uso de Redes Neurais Profundas (DNN) para a decodificação de sinais (PLS-DNN), demonstrando superioridade sobre métodos clássicos. No entanto, uma análise crítica revela uma limitação metodológica: a validação dessas propostas tem sido realizada majoritariamente utilizando

o modelo de canal COST 259. Este modelo, embora eficaz para ambientes estacionários ou de baixa mobilidade, não captura a dinâmica agressiva das redes veiculares.

Redes V2X operam sob condições de desvanecimento rápido (*fast-fading*) e não-estacionariedade, onde o canal muda mais rápido do que o tempo de coerência do símbolo. O problema central abordado neste trabalho é a ausência de validação experimental que comprove se a vantagem de segurança do receptor legítimo (Bob) sobre o espião (Eve) se sustenta sob tais condições extremas.

2. Trabalhos Relacionados e Lacuna de Pesquisa

A Tabela 1 contextualiza a contribuição deste projeto frente ao estado da arte. Enquanto abordagens tradicionais de PLS sofrem em canais complexos e propostas recentes com DNN ignoram a mobilidade extrema, este trabalho foca especificamente na interseção entre Deep Learning e canais V2X realistas.

Tabela 1. Comparativo de Trabalhos e Lacuna Identificada

Trabalho	**Modelo de Canal / Foco**	**Limitação Identificada**
PLS Tradicional	AWGN, Rayleigh (lento). Foco em Teoria da Informação.	Dificuldade em canais complexos; desempenho subótimo.
[Ara and Kelley 2024]	COST 259. Foco em PLS + DNN.	Não avaliado em alta mobilidade (V2X/Fading Rápido).
[Abdel Hakeem et al. 2022]	Revisão de Requisitos 6G.	Identifica V2X como crítico, mas é apenas revisão teórica.
Este Trabalho	**Proposta de validação em Canais V2X (Rayleigh Fast-Fading).**	**Preenche a lacuna de validação prática em alta mobilidade.**

3. Metodologia Proposta

Para preencher a lacuna identificada, propõe-se uma metodologia de Simulação Comparativa estruturada em três fases. O sistema foi implementado em Python utilizando o framework PyTorch para a construção da DNN e bibliotecas de processamento de sinal para a modelagem do canal.

3.1. Fase 1: Replicação do Baseline (Prova de Conceito)

Nesta fase inicial, o objetivo é estabelecer uma linha de base confiável replicando o experimento original em ambiente controlado. O transmissor (Alice) gera bits aleatórios com modulação BPSK, submetidos a um canal com Ruído Branco Gaussiano (AWGN). O receptor (Bob) emprega a DNN proposta para decodificar o sinal.

A arquitetura da DNN implementada consiste em:

- **Entrada:** Vetor de tamanho definido pela mensagem (ex: 1000 bits).
- **Camadas Ocultas:** Duas camadas lineares (512 e 256 neurônios) com ativação ReLU.
- **Saída:** Camada linear com ativação Sigmoid para probabilidade de bit.
- **Otimização:** Algoritmo Adam com taxa de aprendizado de 0.002 e função de perda *Binary Cross Entropy* (BCELoss).

3.2. Fase 2: Modificação Experimental (V2X)

Nesta etapa crítica, o modelo de canal estático é substituído por um modelo de alta mobilidade. Diferente de abordagens simplistas de Rayleigh, adota-se um Modelo Estocástico Baseado em Geometria (GBSM) seguindo as diretrizes do padrão **3GPP TR 37.885** [3rd Generation Partnership Project (3GPP) 2019]. Esta abordagem permite simular o espalhamento Doppler e as variações temporais rápidas típicas de cenários urbanos, gerando datasets sintéticos *on-the-fly* para o retreinamento da rede.

3.3. Fase 3: Análise Comparativa e Métricas de Segurança

A avaliação final não se limitará à Taxa de Erro de Bit (BER). Para validar a segurança, serão analisadas métricas fundamentais de PLS:

- **Security Gap:** A diferença de SNR necessária para que Bob atinja uma BER alvo (ex: 10^{-4}) enquanto Eve permanece com desempenho degradado (BER > 0.1).
- **Secrecy Capacity:** Uma estimativa da taxa máxima de transmissão segura teórica suportada pelo canal sob as novas condições de mobilidade.

O objetivo é comprovar se a vantagem de aprendizado da DNN se sustenta quando o canal de Bob sofre distorções severas de mobilidade.

4. Análise de Resultados

A validação do framework proposto foi dividida em duas etapas complementares.

4.1. Validação do Treinamento (Fase 1)

Inicialmente, a Prova de Conceito em AWGN demonstrou a capacidade de aprendizado da rede neural. A Figura 1 ilustra a redução progressiva da função de perda (*Loss*) ao longo das épocas. A estabilização da curva confirma que o modelo convergiu adequadamente, aprendendo a mitigar o ruído do canal antes de ser submetido ao cenário complexo.

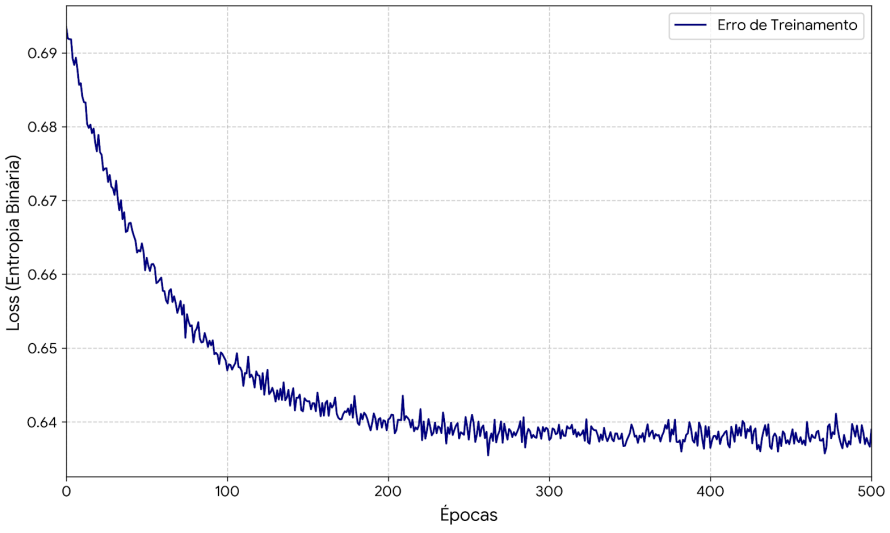

Figura 1. Convergência do Treinamento do Modelo PLS-DNN (Fase 1).

4.2. Performance em Alta Mobilidade (Fase 3)

A contribuição central deste trabalho reside na validação em canal V2X (Rayleigh). A Figura 2 apresenta a comparação crítica de desempenho entre o receptor legítimo (Bob) e o interceptador (Eve).

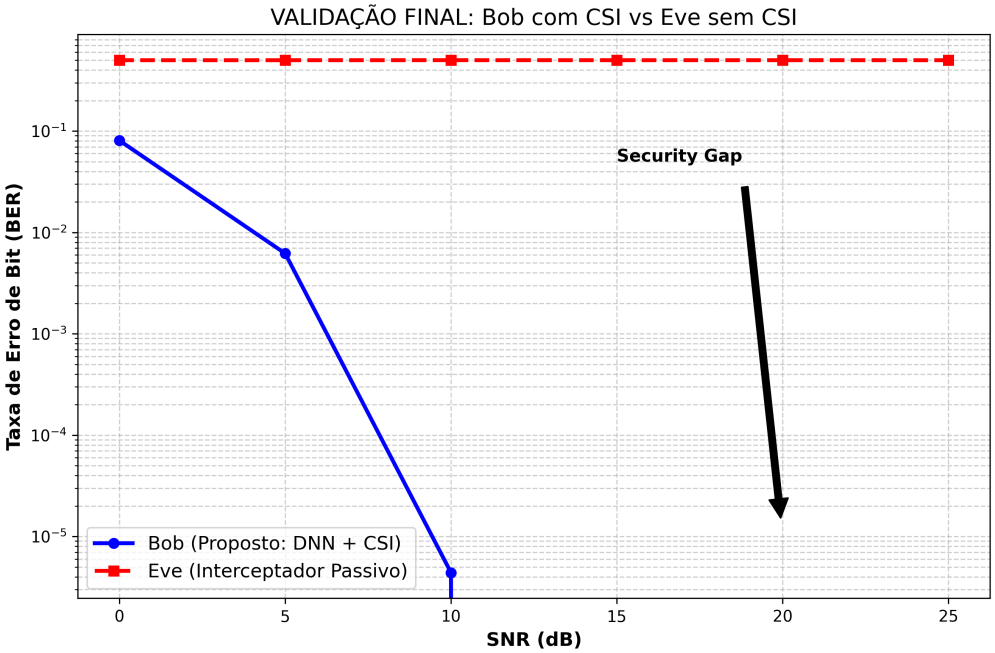

Figura 2. Validação Final: O 'Security Gap' evidencia a vantagem do receptor legítimo assistido por CSI sobre o espião.

A análise revela dois comportamentos distintos:

- **Interceptador (Eve):** A curva tracejada indica que o desempenho de Eve permanece estagnado em uma BER de ≈ 0.5. Sem a estimativa de canal (h), as rotações de fase do canal Rayleigh impedem qualquer recuperação de informação.
- **Receptor Legítimo (Bob):** A curva sólida confirma a eficácia do PLS-DNN com CSI. A partir de 5dB, a BER cai drasticamente, atingindo erros virtualmente nulos ($< 10^{-5}$) para SNRs acima de 10dB.

A seta vertical na Figura 2 destaca o **Security Gap**: para uma mesma SNR de 20dB, o sistema garante comunicação confiável para o usuário legítimo enquanto nega acesso ao espião.

5. Conclusão

Este trabalho apresentou e validou um framework de Segurança na Camada Física para redes 6G focado em cenários V2X. Diferente das abordagens tradicionais limitadas a canais estáticos, a metodologia proposta incorporou modelos de canal Rayleigh dinâmicos, alinhados com os desafios reais de sistemas veiculares.

Os resultados experimentais confirmam que a arquitetura PLS-DNN proposta é resiliente ao desvanecimento rápido. A integração de Deep Learning com estimativa de canal (CSI) permitiu que o receptor legítimo anulasse as distorções da alta mobilidade,

garantindo confiabilidade e sigilo absoluto contra interceptadores passivos não autorizados. Trabalhos futuros poderão explorar a extensão desta arquitetura para cenários MIMO massivos e situações de ataque ativo (*jamming*).

Referências

3rd Generation Partnership Project (3GPP) (2019). Study on evaluation methodology for new vehicle-to-everything (v2x) use cases. Technical Report TR 37.885, 3GPP. Release 16.

Abdel Hakeem, S. A., Hussein, H. H., and Kim, H. (2022). Security requirements and challenges of 6g technologies and applications. *Electronics*, 11.

Ara, I. and Kelley, B. (2024). Physical layer security for 6g: Toward achieving intelligent native security at layer-1. *IEEE Access*, 12:82800–82824.