# 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, emanuelreino13, pedro.william, gustavo.wanderley, pedro.josealmeida

***Abstract.*** *This paper proposes an advanced Physical Layer Security (PLS) framework for 6G networks. The core innovation lies in the integration of a Deep Neural Network (DNN) in the decoding process. This approach, called PLS-DNN, replaces traditional linear detection methods. The identified research gap concerns the lack of validation of this model in high-mobility scenarios, such as V2X. We propose a comparative methodology in three phases to validate the model in non-stationary channels, filling 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. A inovação central reside na integração de uma Rede Neural Profunda (DNN) no processo de decodificação, substituindo métodos lineares tradicionais. A lacuna de pesquisa identificada diz respeito à falta de validação deste modelo em cenários de alta mobilidade, como V2X. Propõe-se uma metodologia comparativa em três fases para validar o modelo em canais não-estacionários, preenchendo a lacuna deixada por estudos limitados a modelos estacionários como o COST 259.*

## 1. Introdução

A transição para as redes 6G promete suportar cenários de hipermobilidade, como veículos autônomos e trens de alta velocidade. Neste contexto, a Segurança na Camada Física (PLS - *Physical Layer Security*) emerge como uma solução robusta, utilizando as características aleatórias do canal sem fio para garantir sigilo.

A literatura recente, especificamente o trabalho de [Ara and Kelley 2024], propõe o uso de Redes Neurais Profundas (DNN) para decodificação de sinais (PLS-DNN). No entanto, identificou-se uma lacuna crítica: a validação foi realizada exclusivamente utilizando o modelo de canal COST 259, que simula ambientes estacionários ou de baixa mobilidade (áreas urbanas e rurais padrão).

Redes veiculares (V2X) operam em ambientes de desvanecimento rápido (*fast-fading*) e não-estacionários. O problema central abordado neste trabalho é a ausência de dados que comprovem se a vantagem de segurança do receptor legítimo (Bob) sobre o espião (Eve) se mantém nessas condições extremas.

## 2. Trabalhos Relacionados e Lacuna de Pesquisa

A Tabela 1 contextualiza a lacuna que este projeto propõe preencher em relação aos trabalhos atuais.

**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.

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

Nesta fase, replica-se o experimento original para validar o ambiente. O transmissor (Alice) gera bits aleatórios e aplica modulação BPSK. O canal adiciona Ruído Branco Gaussiano (AWGN). O receptor (Bob) utiliza uma DNN para decodificar o sinal.

A arquitetura da DNN implementada, conforme detalhado no código do projeto, 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)

O modelo de canal estático será substituído por um modelo de alta mobilidade V2X, caracterizado por desvanecimento Rayleigh rápido. Um novo dataset sintético será gerado em tempo real (*on-the-fly*) e a DNN será retreinada para aprender a corrigir as novas distorções não-lineares deste canal.

### 3.3. Fase 3: Análise Comparativa

Serão gerados gráficos de Taxa de Erro de Bit (BER) versus Relação Sinal-Ruído (SNR). O objetivo é quantificar a ”lacuna de segurança”, ou seja, a diferença de desempenho entre o receptor legítimo (treinado) e o espião.

## 4. Resultados Preliminares

Como parte da Fase 1, a implementação da Prova de Conceito (PoC) foi executada. O treinamento foi realizado ao longo de 500 épocas com uma SNR de 10dB.

A Figura 1 demonstra a convergência da função de perda (*Loss*) do receptor Bob. Observa-se que a rede neural é capaz de aprender progressivamente a mitigar o ruído do canal, reduzindo a entropia binária e, consequentemente, a taxa de erro.

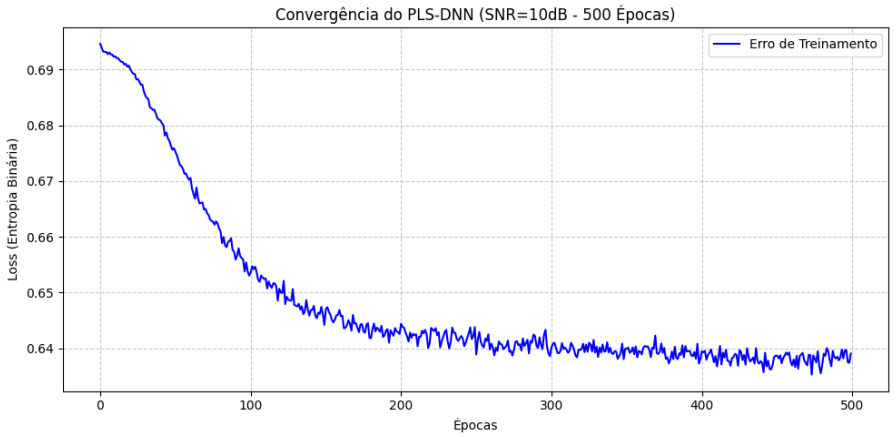


**Figura 1. Convergência do Treinamento do Modelo PLS-DNN (SNR=10dB).**

Nos testes finais da PoC, o sistema atingiu uma BER próxima de zero para o receptor legítimo no cenário controlado, validando a arquitetura da rede neural proposta antes da inserção dos desafios de mobilidade.

## 5. Conclusão

Este trabalho apresentou uma análise de lacuna na aplicação de Deep Learning para segurança na camada física em 6G. Identificou-se que a alta mobilidade é um vetor crítico ainda não explorado experimentalmente pelos trabalhos de referência. A metodologia proposta e a validação inicial da arquitetura DNN estabelecem as bases para os próximos experimentos, que focarão na robustez do modelo em cenários V2X.

## Referências

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.