Relatório de Análise de Lacuna de Pesquisa 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[1]
Garanhuns – Pernambuco – Brasil

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, demonstrating a substantial performance improvement on the order of 10-15 dB in Signal-to-Noise Ratio (SNR). Additionally, the work introduces, for the first time, the combination of this PLS scheme with Alamouti Space-Time Coding (STC), aiming to increase transmission reliability.*

Resumo. *O artigo em questão 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. Esta abordagem, denominada PLS-DNN, substitui os métodos de detecção linear tradicionais, demonstrando uma melhoria de desempenho substancial, na ordem de 10-15 dB, em termos de Relação Sinal-Ruído (SNR). Adicionalmente, o trabalho introduz, pela primeira vez, a combinação deste esquema PLS com Codificação Espaço-Tempo (STC) de Alamouti, visando aumentar a confiabilidade da transmissão.*

1. Análise do Artigo e Identificação da Lacuna de Pesquisa

A metodologia de validação dos autores consiste em simulações de Monte Carlo que avaliam a Taxa de Erro de Bit (BER) versus SNR para os receptores legítimos (Bob) e para o espião (Eve). Os resultados, apresentados nas Figuras 9 a 13 do artigo de referência (Ara, I. & Kelley, B., 2024)[1], comprovam que, enquanto Bob (o receptor legítimo) atinge uma decodificação quase perfeita em SNRs mais baixas, Eve (o espião) mantém uma taxa de erro de bit elevada, confirmando a eficácia da segurança.

A Tabela 1 contextualiza o artigo principal em relação a trabalhos anteriores e à lacuna que este projeto propõe preencher.

A lacuna de pesquisa identificada emerge da limitação dos ambientes de teste. O artigo afirma explicitamente que todas as análises de desempenho foram conduzidas utilizando o modelo de canal COST 259. Este modelo simula ambientes como área urbana (TUx), área rural (RAx) e terreno montanhoso (HTx). Embora sejam cenários padrão, eles representam canais majoritariamente estacionários ou de variação lenta.

Contudo, as redes 6G são projetadas para suportar casos de uso de hipermobilidade, como transporte automatizado e comunicações Veículo-para-Tudo (V2X). Esses

[1]Artigo de referência: `https://ieeexplore.ieee.org/document/10555268/`

Table 1. Tabela comparativa dos trabalhos analisados e da proposta.

Autor/Trabalho	**Foco Principal**	**Modelo de Canal Utilizado**	**Lacuna de Pesquisa / Limitação**
PLS Tradicional (Genérico)	Segurança baseada em teoria da informação (ex: sigilo).	AWGN, Rayleigh (lento).	Dificuldade em se adaptar a canais complexos; desempenho subótimo.
Ara et al. (2024)	PLS + Decodificação DNN; PLS + STC.	COST 259, AWGN.	Desempenho não avaliado em canais não-estacionários de alta mobilidade (ex: V2X).
Abdel Hakeem et al. (2022)	Revisão dos requisitos de segurança 6G.	N/A (Revisão).	Identifica V2X/CAV como aplicações 6G críticas que exigem segurança em alta mobilidade.
Este Trabalho (Proposto)	**Análise de desempenho do PLS-DNN em canais V2X.**	**COST 259 (Baseline) vs. Modelo V2X (ex: Rayleigh com *fading* rápido).**	**Preenche a lacuna de validação do PLS-DNN em ambientes de alta mobilidade.**

cenários são caracterizados por canais não-estacionários e de variação extremamente rápida, cujas características não são capturadas pelo modelo COST 259. Portanto, a lacuna de pesquisa é a ausência de uma análise de desempenho e validação do framework PLS-DNN em ambientes de canal não-estacionários e de rápida variação (fast-fading), que são cruciais para muitos dos casos de uso prometidos pelo 6G.

2. Definição da Metodologia Proposta

Para preencher a lacuna identificada, propõe-se uma metodologia de Simulação Comparativa, estruturada em três fases principais. O objetivo é quantificar o impacto de canais de alta mobilidade no desempenho de segurança do framework PLS-DNN proposto no artigo.

2.1. Fase 1: Replicação do Baseline e Validação

O primeiro passo consiste em replicar fielmente o experimento do artigo original para validar o ambiente de simulação. Isso envolve a implementação do framework PLS-DNN em Python, utilizando bibliotecas como PyTorch ou TensorFlow para a DNN e NumPy para as operações de sinal. O transmissor (Alice), o receptor (Bob) e o espião (Eve) serão modelados conforme descrito, e o decodificador de Bob e Eve será a arquitetura DNN detalhada na Figura 4 do artigo de referência. O canal de comunicação implementado será o COST 259. A simulação será executada varrendo os níveis de SNR para gerar as curvas de BER. O sucesso desta fase será determinado pela capacidade de reproduzir,

com margem de erro aceitável, os gráficos de desempenho apresentados no artigo original (ex: Figuras 10 e 11), confirmando a validade do setup.

2.2. Fase 2: Modificação Experimental e Retreinamento

Nesta fase, o componente do canal de comunicação será substituído para endereçar a lacuna. O modelo de canal COST 259 será trocado por um modelo que simule um ambiente de alta mobilidade V2X, como um canal Rayleigh com desvanecimento (fading) rápido e não-estacionário. Mantendo todo o restante do framework (Alice, Bob, Eve e a arquitetura da DNN) idêntico, um novo dataset sintético será gerado usando este novo modelo de canal. Um passo crítico será o retreinamento dos modelos DNN de Bob e Eve usando este novo dataset. A IA, que foi originalmente treinada para as características do COST 259, deve agora aprender a decodificar os sinais sob as novas e mais complexas distorções do canal V2X.

2.3. Fase 3: Análise Comparativa e Conclusão

Após o retreinamento, a simulação de BER vs. SNR será executada novamente. O resultado final será um conjunto de gráficos comparativos que sobrepõem o desempenho do baseline (Fase 1) com o do novo experimento (Fase 2). A análise se concentrará na ”lacuna de segurança” (a diferença vertical entre as curvas de BER de Bob e Eve). Esta metodologia permitirá responder quantitativamente à pergunta de pesquisa: A vantagem de segurança proporcionada pelo PLS-DNN se sustenta, diminui ou colapsa quando submetida a ambientes de canal de alta mobilidade, típicos do 6G?

Referências Adicionais

Abaixo estão os links para outros artigos citados ou relevantes para o contexto deste trabalho:

- **Abdel Hakeem et al. (2022):** Security Requirements and Challenges of 6G Technologies and Applications.
  `https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9322055/`
- **Ma et al. (2021):** Intelligent Zero Trust Architecture for 5G/6G Networks.
  `https://arxiv.org/abs/2105.01478`
- **Olimid & Nencioni (2020):** 5G Network Slicing: A Security Overview.
  `https://ieeexplore.ieee.org/document/9098253`
- **Yang et al. (2020):** Artificial-Intelligence-Enabled Intelligent 6G Networks.
  `https://fardapaper.ir/mohavaha/uploads/2023/02/Fardapaper-Artificial-Intelligence-Enabled-Intelligent-6G-Networks.pdf`