O Problema: A Segurança do 6G em Alta Velocidade

O contexto central do nosso trabalho reside na transição para as redes 6G, que prometem suportar cenários de hipermobilidade, como veículos autônomos e trens de alta velocidade. A literatura recente, especificamente o trabalho de Ara e Kelley (2024), propõe uma solução robusta de Segurança de Camada Física (PLS) utilizando Redes Neurais Profundas (DNN) para decodificação de sinais. No entanto, identificamos uma lacuna crítica nessa pesquisa: a validação foi realizada exclusivamente utilizando o modelo de canal COST 259, que simula ambientes estacionários ou de baixa mobilidade, como áreas urbanas e rurais padrão.

Essa limitação cria uma incerteza sobre a viabilidade da segurança em cenários reais de 6G. Redes veiculares (V2X), por exemplo, operam em ambientes de desvanecimento rápido (*fast-fading*) e não-estacionários, onde as características do canal de comunicação mudam drasticamente em milissegundos. O problema que estamos atacando é justamente a ausência de dados que comprovem se a vantagem de segurança do receptor legítimo (Bob) sobre o espião (Eve) se mantém ou colapsa quando submetida a essas condições extremas de velocidade.

A Nossa Solução: Simulação PLS-DNN com Canais Dinâmicos

Para preencher essa lacuna, desenvolvemos uma Prova de Conceito (PoC) baseada em simulação computacional, estruturada em Python com o uso de PyTorch. Nossa abordagem substitui os decodificadores lineares tradicionais por uma Rede Neural Profunda (DNN). Diferente dos métodos clássicos que seguem regras matemáticas fixas, a nossa DNN é treinada para "aprender" a corrigir as distorções causadas pelo ruído do canal, permitindo uma recuperação de sinal muito mais eficiente.

A implementação técnica inova ao utilizar uma estratégia de dados 100% sintéticos gerados em tempo real ("on-the-fly"). Em vez de dependermos de datasets estáticos e limitados, nosso sistema possui um transmissor virtual (Alice) que gera bits e simula a passagem por canais físicos matematicamente modelados. Isso nos dá a flexibilidade de alternar entre o cenário base (COST 259 com ruído AWGN) e, futuramente, o cenário desafiador de alta mobilidade (Rayleigh com fading rápido), sem precisar reescrever a arquitetura do sistema.

Atualmente, na fase funcional apresentada, validamos o "caminho feliz": o sistema consegue gerar transmissões, aplicar ruído e treinar o receptor legítimo para reduzir a Taxa de Erro de Bit (BER) à medida que o treinamento avança. O objetivo final é gerar gráficos comparativos de BER versus SNR, demonstrando quantitativamente a "lacuna de segurança" — ou seja, provar que, mesmo em alta velocidade, nossa IA consegue garantir que o receptor legítimo decodifique a mensagem enquanto o espião permanece com uma taxa de erro elevada.