Arquitetura L4S: Detecção de Ataque ECN não-responsivo através de técnicas de Machine Learning

Grupo: Lucas Jaiel, José Jantony, Jaaziel Batista

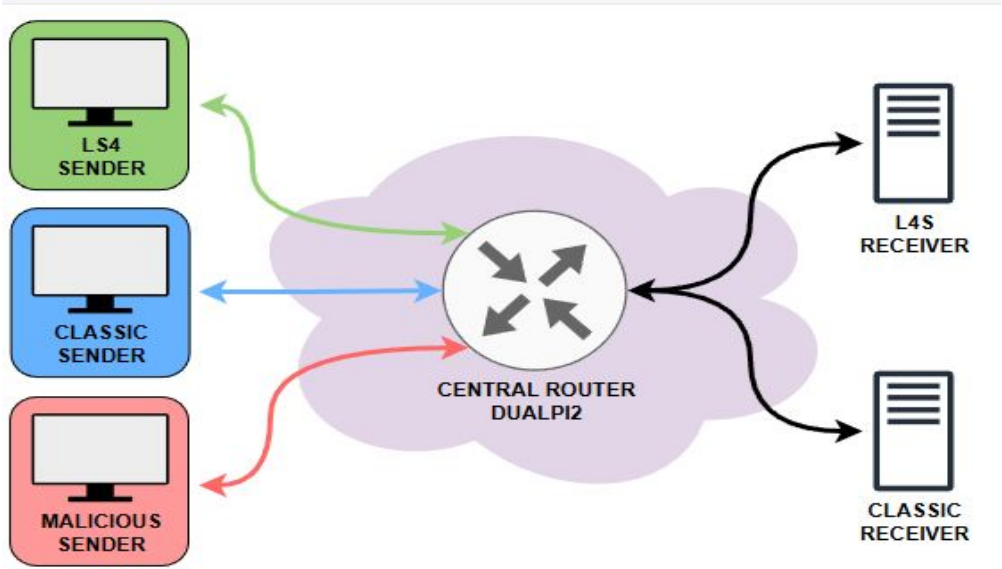
Introdução

O L4S (Low Lattency, Low Loss, Scalable throughput) é uma arquitetura de rede que trás um novo paradigma em relação a controle de congestionamento de rede. Em um mundo digital onde cada segundo conta, as tecnologias que permitem a transmissão de dados fluida e eficiente são fundamentais para garantir a qualidade da experiência do usuário na internet.

Importância

O L4S é ideal para aplicações otimizadas por altas taxas de dados, latência ultrabaixa consistente e perda de pacotes próxima de zero — incluindo jogos na nuvem, realidade virtual/realidade aumentada (RV/RA) e videoconferências de alta qualidade. O L4S também é benéfico para outras aplicações com restrições de latência, como o tráfego HTTP em geral.

Ambiente de Teste para Coleta de dados, Construção de Dataset e Treinamento Supervisionado



INSTITUTO FEDERAL
Paraíba

Avaliação e Desempenho de Rede

Features e Validação

Para manter a latência ultrabaixa consistente do L4S, o projeto desenvolve um IDS leve baseado em Árvore de Decisão (Decision Tree) no roteador central. Este sistema é treinado com um dataset próprio (BENIGNO/MALICIOSO) gerado em nosso *testbed*, utilizando *features* críticas de desempenho. O sucesso do modelo será determinado pela análise do Queue-Delay da Fila L (principal indicador de ataque) e das variações de RTT/Jitter. Nossa validação final se concentrará em garantir alta Precisão (minimizando Falsos Positivos) e Recall (maximizando a detecção) para que a rede seja efetivamente protegida em tempo real.