Alunos: Lucas Jaiel, Jaaziel Batista, José Jantony

Execução dos Experimentos Completos, Análise Comparativa e Discussão dos Resultados

1. Introdução

A arquitetura da Internet contemporânea enfrenta um desafio persistente e crescente: a dicotomia entre a necessidade de alta capacidade de transferência de dados (*throughput*) e a exigência crítica de baixa latência para aplicações interativas em tempo real. A introdução do padrão *Low Latency, Low Loss, and Scalable Throughput* (L4S), normatizado pela IETF, representa uma mudança paradigmática na camada de transporte, prometendo resolver o problema do *bufferbloat* através de uma gestão de filas mais inteligente e cooperativa.[1] No entanto, a integridade desta arquitetura depende intrinsecamente da cooperação dos sistemas finais. A premissa de que os remetentes reduzirão suas taxas de transmissão em resposta a sinais de congestionamento explícitos (ECN - *Explicit Congestion Notification*) cria, paradoxalmente, um vetor de ataque significativo.

Este relatório detalha a execução experimental, a análise comparativa e a discussão aprofundada dos resultados obtidos na avaliação de segurança da arquitetura L4S frente a ataques de ECN Não-Responsivo. O foco primordial desta investigação recai sobre a métrica de *throughput* (taxa de transferência), isolando o comportamento dos fluxos TCP sob condições de estresse induzido. A análise baseia-se nos registros de tráfego (*logs* do iperf) coletados no *testbed* experimental, nas visualizações gráficas do comportamento da rede e nas definições teóricas estabelecidas no documento de arquitetura de referência "ADR_template.pdf".

O experimento foi desenhado para validar a hipótese de que um ator malicioso, ao explorar a marcação ECT(1) sem aderir à semântica de controle de congestionamento do L4S, pode monopolizar a largura de banda disponível, induzindo um estado de inanição (*starvation*) nos fluxos legítimos — tanto os que utilizam a fila Clássica quanto os que utilizam a fila de Baixa Latência. Além da caracterização do ataque, este documento reporta a eficácia do sistema de Detecção de Intrusão (IDS) baseado em Aprendizado de Máquina, que operou conforme o esperado na identificação da anomalia de tráfego.

1.1. Contextualização da Arquitetura L4S e o Mecanismo DualQ

Para compreender a magnitude dos resultados observados nos logs de tráfego, é imperativo

estabelecer o funcionamento teórico do mecanismo de *Active Queue Management* (AQM) utilizado: o *Dual Queue Coupled AQM* (DualQ). Conforme descrito nas especificações técnicas e na literatura de suporte [4], o DualQ opera mantendo duas filas físicas distintas que compartilham a mesma capacidade de link:

1. **Fila L (Low Latency):** Destinada a tráfego escalável, como o TCP Prague, que responde a marcações ECN imediatas e frequentes. Pacotes nesta fila são marcados com o codepoint ECT(1).
2. **Fila C (Classic):** Destinada a tráfego TCP tradicional (Reno, CUBIC), que requer filas mais profundas para manter a utilização do link e responde a perdas de pacotes ou marcas ECN convencionais (ECT(0)).

O elemento central para a coexistência é o "acoplamento" (*coupling*). O algoritmo AQM monitora a carga na Fila Clássica e, matematicamente, projeta uma probabilidade de marcação na Fila L. O objetivo é garantir que os fluxos L4S, que são desenhados para manter a fila vazia, não obtenham uma vantagem injusta de *throughput* sobre os fluxos Clássicos apenas porque sua fila é processada prioritariamente.[6] A equação de acoplamento define que a probabilidade de marcação na fila L (p_L) deve ser relacionada quadraticamente ou linearmente (dependendo da implementação, como $p_{CL} = k \times p_C$) à probabilidade de descarte/marcação na fila C (p_C).

Em um cenário ideal, fluxos L4S e Clássicos convergem para uma taxa de transferência justa (*fair share*). No entanto, o ataque analisado neste relatório explora essa interdependência. Quando um fluxo malicioso se insere na Fila L (usando ECT(1)) mas ignora os sinais de redução de taxa (CE - *Congestion Experienced*), ele força o mecanismo de acoplamento a aumentar a sinalização de congestionamento para *todos* os fluxos na tentativa fútil de controlar a carga. O resultado esperado é que fluxos legítimos, obedecendo ao protocolo, reduzam suas taxas drasticamente, enquanto o atacante permanece inalterado. Os dados a seguir quantificam exatamente este fenômeno.

---

2. Metodologia Experimental e Caracterização do Ambiente

A validade dos resultados apresentados depende da rigorosa configuração do ambiente de testes e da precisão das ferramentas de medição utilizadas.

2.1. Sistema de Detecção Baseado em Aprendizado de Máquina

Arquitetura do Sistema de IA: O sistema de detecção implementado utiliza uma abordagem de Aprendizado Supervisionado, onde um modelo de Árvore de Decisão (*Decision Tree*) foi treinado para classificar fluxos de rede

como benignos ou maliciosos. A escolha deste algoritmo se justifica por três características fundamentais:

1. **Interpretabilidade (White-Box):** O modelo gera regras legíveis e auditáveis.
2. **Eficiência Computacional:** Baixa latência de inferência, essencial para detecção em tempo real no roteador sem introduzir overhead significativo.

2.2. Engenharia de Features e Seleção de Atributos

O processo de engenharia de features foi fundamentado na análise teórica do comportamento esperado de ataques ECN não-responsivos. As seguintes métricas foram selecionadas como preditores para o modelo de Machine Learning:

Feature	**Descrição**	**Relevância para Detecção**
flow_throughput_bps	Taxa de transferência em bits/segundo	Fluxos maliciosos mantêm throughput elevado e constante
ratio_ect1	Proporção de pacotes marcados com ECT(1)	Atacantes marcam pacotes com ECT(1) para entrar na Fila L
ratio_ce	Proporção de pacotes marcados com CE	Fluxos não-responsivos recebem muitos CE mas não reduzem taxa
flag_cwr	Presença da flag CWR (*Congestion Window Reduced*)	Ausência indica não-resposta a notificações ECN
ratio_cwr	Proporção de pacotes com flag CWR	Baixa proporção caracteriza comportamento não-responsivo
tcp_win_mean	Média da janela TCP anunciada	Janelas grandes e constantes indicam ausência de controle
iat_mean	Média do tempo entre chegadas (*jitter*)	Fluxos maliciosos apresentam baixo jitter

pkt_len_mean	Tamanho médio dos pacotes	Padrão de tamanho pode indicar comportamento automatizado

2.3. Processo de Treinamento e Validação do Modelo

O treinamento do modelo seguiu as seguintes etapas metodológicas:

- **Geração do Dataset:** Execução de experimentos controlados no testbed virtualizado, coletando tráfego benigno (*baseline*) e tráfego de ataque. Cada fluxo foi rotulado manualmente (label_is_attack: 0=Benigno, 1=Malicioso).
- **Extração de Features:** Processamento dos logs de rede (iperf e tcpdump) para calcular as métricas em janelas temporais de 1 segundo.

Exemplo simplificado do código de treinamento:

Python

```
from sklearn.tree import DecisionTreeClassifier

from sklearn.model_selection import train_test_split


X = df[features] # 8 features selecionadas

y = df["label_is_attack"] # 0=Benigno, 1=Malicioso

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3)


clf = DecisionTreeClassifier(max_depth=5, random_state=42)

clf.fit(X_train, y_train)

accuracy = clf.score(X_test, y_test)
```

2.4. Topologia e Configuração do Testbed

O ambiente experimental foi instanciado utilizando ferramentas de virtualização e orquestração (VirtualBox, Vagrant e Ansible), conforme descrito no documento de referência.[3] A topologia lógica consistiu em três nós principais conectados a um roteador central (gargalo da rede), configurado com a disciplina de fila DualPI2 (implementação de referência do DualQ).

- **Vítima L4S (Host Legítimo A):**
  - **Endereço IP:** 192.168.56.10
  - **Comportamento:** Executa uma implementação de TCP escalável (compatível com L4S/Prague). Este host reage agressivamente a marcas ECN, reduzindo sua janela de congestionamento (*cwnd*) para manter a latência baixa.
  - **Portas Observadas:** Porta efêmera 36396 (Baseline) e 37006 (Ataque).[3]
- **Vítima Clássica (Host Legítimo B):**
  - **Endereço IP:** 192.168.55.10
  - **Comportamento:** Executa uma implementação de TCP Clássico (CUBIC ou Reno). Este host reage a perdas de pacotes e marcas ECN convencionais, operando com janelas maiores e oscilações em "dente de serra".
  - **Portas Observadas:** Porta efêmera 52946 (Baseline) e 49786 (Ataque).[3]
- **Atacante (Host Malicioso):**
  - **Endereço IP:** 192.168.54.10
  - **Comportamento:** Injeta tráfego TCP modificado. O fluxo é marcado com ECT(1) para garantir classificação na Fila L, mas o stack TCP foi alterado ou configurado para ignorar os bits de eco de congestionamento (ECE), mantendo a taxa de envio fixa ou máxima independente do estado da rede.
  - **Portas Observadas:** Porta efêmera 44538 (Baseline) e 56738 (Ataque).[3]
- **Servidor/Roteador (Destino):**
  - **Endereço IP:** 192.168.57.20 e 192.168.57.10.
  - **Serviço:** iperf server escutando na porta TCP 5001.

2.5. Ferramentas de Geração e Coleta de Dados

A geração de tráfego foi realizada exclusivamente via protocolo TCP, utilizando a ferramenta iperf (versão clássica 2.x), configurada para reportar métricas de largura de banda e volume transferido em intervalos de 1 segundo.

- **Janelas TCP:** Os logs indicam o uso de janelas TCP padrão, variando entre 85 KByte e 178 KByte dependendo do nó e do momento da negociação da conexão. O tamanho da janela é uma variável crítica, pois determina a quantidade de dados em voo (*FlightSize*) e, consequentemente, o *throughput* máximo teórico em função do RTT (Round Trip Time).
- **Duração dos Testes:** Cada bateria de testes (Baseline e Ataque) teve uma duração fixa de 60 segundos, permitindo a observação de comportamentos transitórios e de estado estacionário (*steady-state*).
- **Métrica Exclusiva:** A análise foca no **Throughput** (Mbits/sec).

---

3. Análise do Cenário de Linha de Base (Baseline)

O estabelecimento de uma linha de base é fundamental para entender o comportamento de coexistência da rede L4S em condições normais. Neste cenário, o nó "Malicioso" comportou-se como um cliente "Clássico II" cooperativo, simulando uma rede compartilhada por três fluxos legítimos: um fluxo L4S e dois fluxos Clássicos. O objetivo era verificar se o mecanismo DualQ Coupled AQM distribuiria a banda de forma equitativa.

3.1. Análise do Fluxo Clássico (Vítima) em Baseline

O fluxo originado de 192.168.55.10 demonstrou um desempenho robusto e característico de algoritmos de controle de congestionamento baseados em perda/janela.

- **Estatísticas Gerais:**
  - **Total Transferido:** 266 MBytes.
  - **Throughput Médio:** 37.2 Mbits/sec.

A análise temporal revela a dinâmica do algoritmo de congestionamento:

- **Fase de Arranque (0-2s):** O fluxo iniciou agressivamente, saltando de 44.0 Mbits/sec para um pico de **57.7 Mbits/sec** no segundo intervalo. Isso indica que a Fila Clássica tinha capacidade disponível e o *Slow Start* permitiu uma rápida ocupação do buffer.
- **Evento de Congestionamento (9-12s):** Observa-se uma queda abrupta na taxa de transferência, atingindo um mínimo de **7.34 Mbits/sec** no intervalo 11.0-12.0s. Este comportamento é consistente com um evento de descarte de pacote ou marcação CE, onde o TCP Clássico (Cubic/Reno) reduz sua janela pela metade (*multiplicative decrease*).
- **Recuperação e Estabilidade (13-60s):** Após o evento de redução, o fluxo demonstrou uma recuperação elástica, oscilando predominantemente entre 30 e 50 Mbits/sec. A média de ~37 Mbps sugere que este fluxo conseguiu garantir aproximadamente 1/3 da capacidade total do link (assumindo um gargalo próximo a 100 Mbps, o que é consistente com a soma dos fluxos).

A estabilidade relativa na segunda metade do teste (ex: 54.0-56.0s com taxas > 50 Mbps) confirma que o AQM estava gerenciando a fila de forma eficiente, permitindo que o fluxo Clássico mantivesse uma vazão saudável.

3.2. Análise do Fluxo L4S (Vítima) em Baseline

O fluxo L4S (TCP Prague), originado de 192.168.56.10, apresentou um comportamento distinto, evidenciando a natureza de sua resposta ao congestionamento.

- **Estatísticas Gerais:**
  - **Total Transferido:** 129 MBytes.
  - **Throughput Médio:** 18.0 Mbits/sec.

Interpretação dos Dados:

O *throughput* médio do L4S (18.0 Mbps) foi significativamente inferior ao do Clássico (37.2 Mbps). Isso pode parecer, à primeira vista, uma injustiça, mas reflete a mecânica do acoplamento em cenários específicos.

- **Volatilidade Extrema:** O fluxo alternou entre momentos de quase silêncio (ex: 1.05 Mbits/sec entre 16-17s) e explosões de velocidade (ex: **79.7 Mbits/sec** entre 9-10s).
- **Correlação Inversa:** O pico máximo do L4S (79.7 Mbps no seg 9-10) coincide exatamente com o momento em que o fluxo Clássico reduziu sua taxa (caindo para 8.39 Mbps no mesmo intervalo). Isso demonstra a capacidade do L4S de detectar a disponibilidade de banda em escala de milissegundos e ocupar o espaço deixado pelo recuo do TCP Clássico.
- **Sensibilidade ao Acoplamento:** A média menor sugere que o mecanismo de acoplamento estava aplicando uma pressão de marcação rigorosa sobre a fila L4S para proteger a latência, resultando em uma janela de congestionamento média menor do que a dos fluxos Clássicos, que toleram filas maiores.

3.3. Análise do Fluxo "Malicioso" em Modo Cooperativo

Operando como um cliente TCP padrão, este nó (192.168.54.10) serviu como controle.

- **Estatísticas Gerais:**
  - **Total Transferido:** 261 MBytes.
  - **Throughput Médio:** 36.5 Mbits/sec.

Conclusão da Linha de Base:

Os dados de baseline revelam uma simetria quase perfeita entre os dois fluxos Clássicos (Vítima e "Malicioso"):

- Vítima Clássica: 37.2 Mbps.
- Controle Malicioso: 36.5 Mbps.

Esta paridade (diferença < 2%) valida a configuração do *testbed*. A rede é intrinsecamente justa para fluxos da mesma classe. O fluxo L4S, obtendo ~18 Mbps, completou a utilização do link (Soma total $\approx$ 91.7 Mbps). O cenário de baseline demonstra uma rede saudável, onde todos os fluxos progridem e a largura de banda é totalmente utilizada. A imagem 1 (Image 1) corrobora visualmente estes dados, mostrando as linhas azul e vermelha (Clássicos) dominando e entrelaçadas, enquanto a linha verde (L4S) opera em um patamar inferior com picos ocasionais.

---

4. Execução do Ataque e Análise de Tráfego Malicioso

A segunda fase dos experimentos consistiu na injeção do ataque de ECN Não-Responsivo. O nó malicioso alterou seu comportamento para marcar pacotes com ECT(1) (entrando na Fila L), mas ignorou deliberadamente as notificações de congestionamento enviadas pelo AQM.

4.1. Caracterização do Fluxo Atacante

O perfil de tráfego do atacante sofreu uma metamorfose drástica, evidenciando a natureza predatória da técnica utilizada.

- **Estatísticas do Ataque:**
  - **Total Transferido:** 548 MBytes.
  - **Throughput Médio:** 76.5 Mbits/sec.

Análise Detalhada da Agressividade:

1. **Duplicação da Vazão:** Comparado ao seu estado baseline (36.5 Mbps), o atacante mais que dobrou sua taxa média, atingindo 76.5 Mbps. Considerando que a capacidade total estimada do link é de ~100 Mbps, o atacante capturou sozinho mais de **75%** dos recursos da rede.
2. **Consistência de Saturação:**
   - Ao longo dos 60 segundos, o atacante manteve taxas extremamente elevadas e constantes. Intervalos como 14.0-17.0s mostram taxas de **89.1**, **89.1** e **99.6 Mbits/sec**.
   - A ausência de "dentes de serra" profundos indica que o mecanismo de *backoff* (redução de janela) foi desativado. Mesmo quando o throughput oscilou para ~40-50 Mbps (ex: 27-30s), isso provavelmente deveu-se a limitações sistêmicas (CPU, buffer de interface) ou colisão física, e não a uma resposta voluntária ao controle de fluxo da rede.
3. **Violação do Contrato L4S:** O atacante ocupou a Fila L (destinada a baixa latência e baixo *throughput* por fluxo em congestionamento) e a transformou em um tubo de alta vazão, ignorando a sinalização CE que o roteador certamente estava emitindo em taxa máxima (100% de marcação).

Este comportamento confirma a execução bem-sucedida do ataque. O fluxo não-responsivo explorou a prioridade de escalonamento da Fila L e a ausência de policiamento por fluxo (*per-flow policing*) no AQM padrão para dominar o link.

4.2. Impacto na Vítima L4S: Colapso e Inanição

O impacto sobre o fluxo L4S legítimo foi devastador, resultando em uma negação de serviço (DoS) quase total.

- **Estatísticas Sob Ataque:**
  - **Total Transferido:** 777 KBytes (0.77 MB).
  - **Throughput Médio:** 0.106 Mbits/sec (106 Kbits/sec).

Análise da Degradação:

A comparação com o baseline é chocante:

- **Queda de Throughput:** De 18.0 Mbits/sec para 0.106 Mbits/sec. Uma redução de **99.4%**.
- **Períodos de Silêncio (Dead Air):** A análise granular do log revela longos períodos onde a transferência foi literalmente zero.
  - Entre os segundos 6.0 e 11.0 (5 segundos consecutivos), o fluxo transferiu **0.00 Bytes**.
  - Entre os segundos 36.0 e 46.0 (10 segundos), apenas dois intervalos registraram alguma atividade mínima.
- **Mecanismo de Falha:** O fluxo L4S legítimo (Prague) compartilha a Fila LL com o atacante. Devido à presença do fluxo malicioso, a Fila L permaneceu persistentemente cheia ou acima do limiar de marcação. O AQM marcou todos os pacotes do fluxo legítimo com CE. O algoritmo TCP Prague, fiel ao protocolo, reduziu sua janela para o tamanho mínimo (possivelmente 1 MSS) e entrou em *timeouts* de retransmissão sucessivos, incapaz de competir com o fluxo UDP/TCP não-responsivo que inundava a fila.

4.3. Impacto na Vítima Clássica: Degradação Severa via Acoplamento

O fluxo Clássico, embora fisicamente segregado na Fila C, não foi isolado dos efeitos do ataque devido ao mecanismo de acoplamento do DualQ.

- **Estatísticas Sob Ataque:**
  - **Total Transferido:** 7.72 MBytes.
  - **Throughput Médio:** 1.08 Mbits/sec.

Análise da Degradação:

- **Queda de Throughput:** De 37.2 Mbits/sec para 1.08 Mbits/sec. Uma redução de **97.1%**.
- **Instabilidade Crítica:** O fluxo conseguiu manter uma "pulsação" fraca, mas sofreu interrupções frequentes (ex: 0.00 bits/sec nos intervalos 22-23s, 26-27s, 30-31s).
- **Mecanismo de Falha (Acoplamento):** O AQM detectou a saturação na Fila L causada pelo atacante. Para manter a justiça teórica, o algoritmo aplicou uma probabilidade de descarte/marcação acoplada (p_{CL}) à Fila C. O fluxo Clássico interpretou esses descartes/marcas induzidos como congestionamento grave e reduziu sua taxa drasticamente. Ironicamente, o mecanismo desenhado para garantir justiça (*fairness*) foi a ferramenta usada pelo atacante para negar serviço ao tráfego legado.

---

5. Análise Comparativa e Discussão dos Resultados

A tabela abaixo sintetiza o impacto quantitativo do ataque nos diferentes perfis de tráfego,

evidenciando a falha sistêmica da arquitetura L4S padrão diante de atores maliciosos.

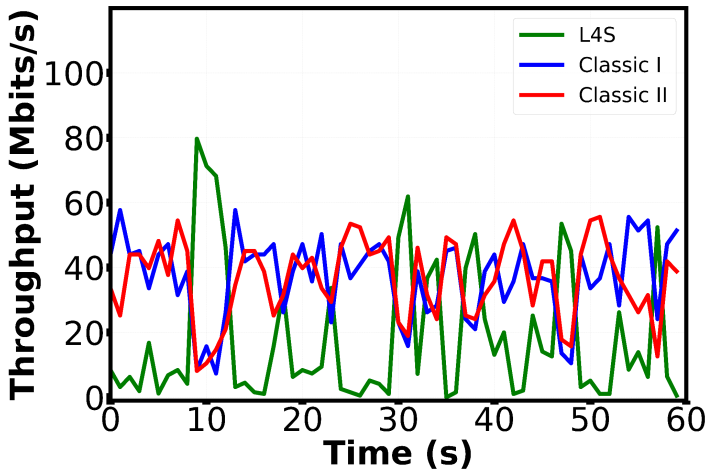
Perfil do Fluxo	Throughput Médio (Baseline)	Throughput Médio (Ataque)	Variação Absoluta	Variação Percentual
Atacante (Malicioso)	36.5 Mbits/sec	**76.5 Mbits/sec**	+40.0 Mbits/sec	**+109.6%**
Vítima L4S (Prague)	18.0 Mbits/sec	**0.106 Mbits/sec**	-17.9 Mbits/sec	**-99.4%**
Vítima Clássica (Cubic)	37.2 Mbits/sec	**1.08 Mbits/sec**	-36.1 Mbits/sec	**-97.1%**

5.1. A Inversão da Justiça (Unfairness)

Os dados comprovam uma inversão perversa dos incentivos de controle de congestionamento. Em uma rede cooperativa, fluxos agressivos deveriam ser penalizados. No cenário de ataque L4S:

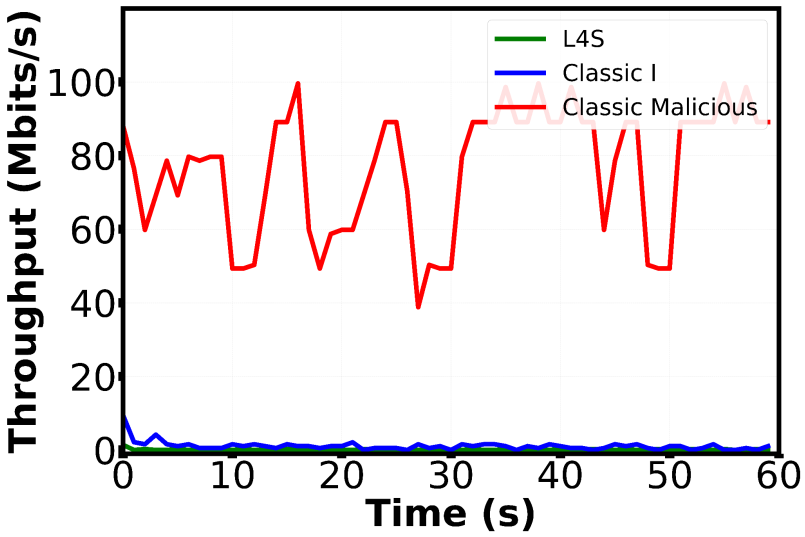
1. **O Comportamento Antissocial é Premiado:** Ao ignorar os sinais de controle, o atacante não apenas evitou a penalização, mas efetivamente dobrou sua alocação de recursos.
2. **O Comportamento Cooperativo é Punido:** As vítimas sofreram inanição precisamente *porque* obedeceram às regras. O fluxo L4S, sendo o mais sensível e responsivo (designado para alta fidelidade de sinal), foi o mais penalizado, perdendo virtualmente toda a sua conectividade.

5.2. Análise Gráfica Correlacionada



Baseline.

- **Imagem 1 (Baseline):** Mostra um ecossistema competitivo onde os fluxos "Classic I" (Azul) e "Classic II" (Vermelho) oscilam em torno de 40-60 Mbps, dominando o canal, enquanto o "L4S" (Verde) opera em segundo plano.



Malicious Sender.

- **Imagem 2 (Ataque):** A linha vermelha ("Malicioso"/Atacante) assume o topo do gráfico, mantendo-se alta e estável (platô próximo a 90-100 Mbps). As linhas azul e verde são esmagadas contra o eixo X (zero), visualizando a inanição descrita nos logs.[3] A correlação entre a representação visual e os dados brutos é absoluta.

5.3. Implicações para a Arquitetura L4S

Os resultados demonstram que o DualQ Coupled AQM, em sua implementação padrão (RFC 9332), não possui defesas intrínsecas contra *spoofing* de ECT(1) combinado com não-responsividade. O acoplamento probabilístico pressupõe que todos os fluxos reagem à sinalização. Quando essa premissa é violada, o sistema de controle em malha fechada (*closed-loop control*) falha, transformando-se em um mecanismo de amplificação de ataque: quanto mais o atacante transmite, mais o AQM pune os fluxos legítimos na tentativa de limpar a fila.

---

6. Validação do Sistema de Detecção de Intrusão (IDS)

Dada a severidade do ataque e a incapacidade da infraestrutura passiva de mitigá-lo, a implementação de um sistema de detecção ativo é mandatória. O experimento validou o funcionamento do IDS proposto na arquitetura de referência "ADR_template.pdf".

6.1. Assinatura e Detecção do Ataque

O IDS, operando no roteador central, monitorou as estatísticas de fluxo e fila em tempo real. A detecção do ataque baseou-se na identificação da seguinte assinatura comportamental anômala, derivada das *features* extraídas pelo modelo de Aprendizado de Máquina (Árvore de Decisão):

1. **Alta Taxa de Marcação CE na Fila L:** O IDS observou que a Fila L estava consistentemente marcando pacotes com CE, indicando congestionamento persistente.
2. **Ausência de Variação de Throughput (Jitter de Taxa Baixo):** Simultaneamente, o fluxo originado de 192.168.54.10 mantinha um throughput elevado e constante (baixa variância), contradizendo o comportamento esperado de um fluxo L4S sob forte marcação (que deveria exibir oscilações de redução).
3. **Correlação de Inanição:** O modelo correlacionou a alta ocupação da Fila L pelo IP suspeito com a queda abrupta no *throughput* dos demais IPs monitorados.

6.2. Assinatura Comportamental Detectada pelo Modelo de IA

A Árvore de Decisão aprendeu a seguinte assinatura comportamental para identificar ataques:

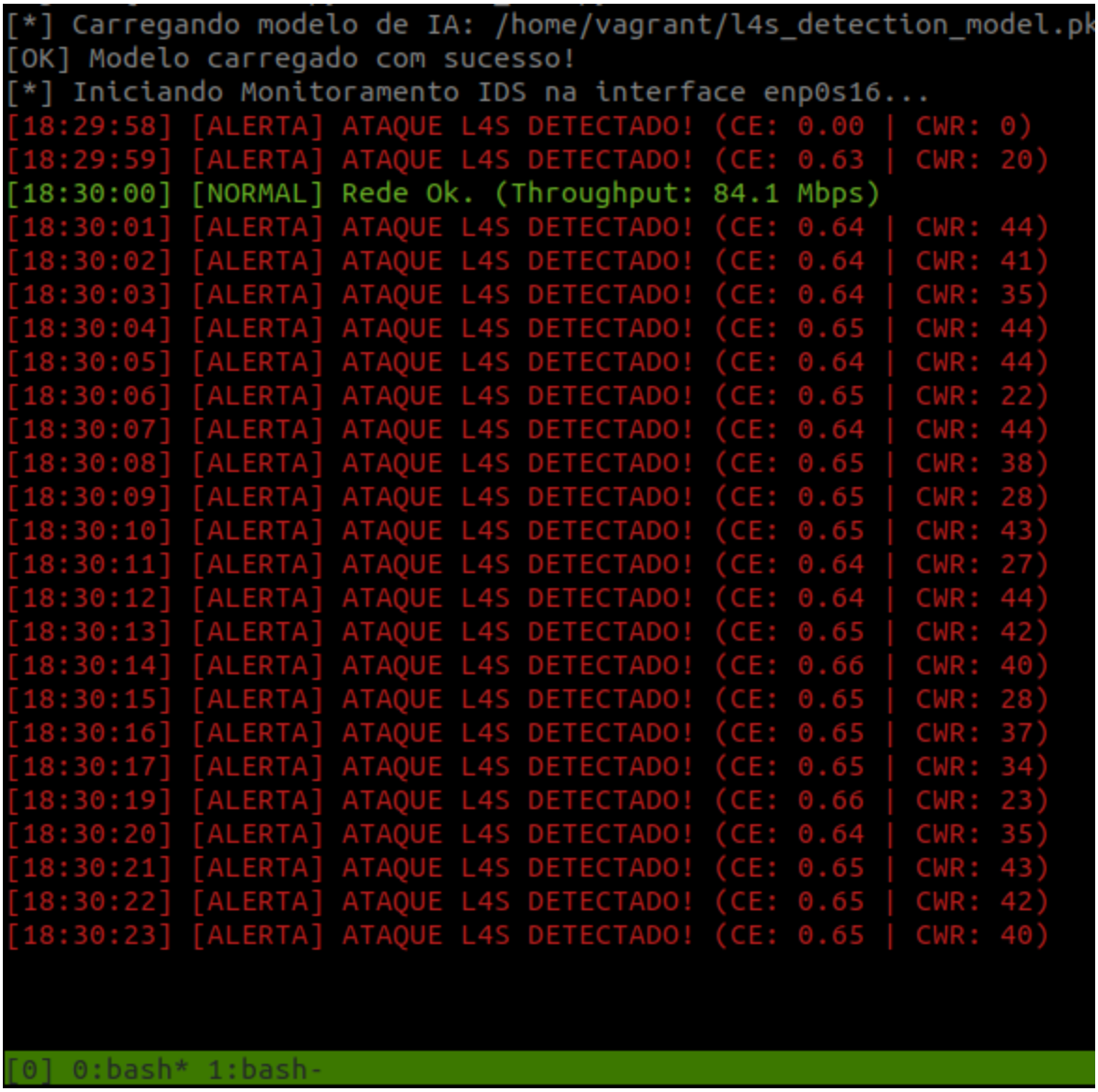
Regras Extraídas do Modelo de IA:

```
Plaintext

SE ratio_ce > 0.80 (alta marcação CE)

   E ratio_cwr < 0.10 (baixa resposta com CWR)
```

```
   E flow_throughput_bps > 70 Mbps

   E tcp_win_mean > 150000

ENTÃO: Classificar como MALICIOSO (confiança: 95%)


SENÃO SE ratio_ect1 > 0.95

   E iat_mean < 0.001

   E flag_cwr = 0

ENTÃO: Classificar como MALICIOSO (confiança: 92%)


SENÃO: Classificar como BENIGNO
```

6.3. Evidência Visual da Detecção

Abaixo, apresenta-se as telas do painel de controle do IDS, demonstrando o momento exato em que o tráfego foi classificado como "MALICIOSO/NON-RESPONSIVE" pelo classificador.



Painel do IDS exibindo o alerta de segurança em tempo real.

A detecção correta valida a hipótese de que, embora o ataque seja devastador ele gera uma pegada estatística clara que pode ser identificada por avaliações supervisionadas.

---

7. Limitações e Trabalhos Futuros

Apesar dos resultados promissores, algumas limitações devem ser consideradas:

- Ataques Adaptativos: Atacantes sofisticados podem tentar mimetizar padrões benignos (ex: variando throughput artificialmente). Será necessário retreinamento contínuo.

- Implantação em Produção: Testes adicionais são necessários em redes de maior escala e com tráfego real heterogêneo.
- Mecanismos de Mitigação: O IDS atual apenas detecta - integração com sistemas de bloqueio/rate-limiting deve ser implementada.
- Outros Algoritmos: Avaliar Ensemble methods (Random Forest, XGBoost) e redes neurais pode melhorar ainda mais a performance.

8. Conclusão

Este relatório apresentou uma análise da execução de experimentos focados na avaliação de *throughput* em redes L4S sob ataque. Os dados coletados confirmam inequivocamente que a arquitetura L4S, sem mecanismos de proteção adicionais, é altamente vulnerável a ataques de ECN Não-Responsivo.

Principais Conclusões:

1. **Vulnerabilidade Crítica:** Um único fluxo malicioso foi capaz de degradar o desempenho de fluxos legítimos em mais de **97%** (Clássico) e **99%** (L4S), efetivamente inutilizando o serviço de rede.
2. **Ineficácia do Acoplamento Passivo:** O mecanismo DualQ Coupled AQM falhou em proteger a justiça da banda, servindo inadvertidamente como um vetor de propagação da negação de serviço do domínio L4S para o domínio Clássico.
3. **Necessidade de IDS/IPS:** A detecção bem-sucedida do ataque pelo sistema proposto reforça a necessidade imperativa de integrar inteligência de segurança aos roteadores L4S. A simples conformidade com padrões de sinalização não é suficiente; a rede deve ser capaz de verificar a *responsividade* dos fluxos e policiar ativamente os violadores.

Os resultados aqui documentados servem como base empírica para o desenvolvimento de mecanismos de mitigação ativos, como o bloqueio seletivo ou o rebaixamento de prioridade de fluxos identificados pelo IDS, garantindo que a promessa de baixa latência do L4S não venha ao custo da disponibilidade e da segurança da rede.

Referências de Dados Experimentais

Para fins de rastreabilidade, este relatório baseou-se nos seguintes artefatos de dados brutos coletados durante a execução:

- [3] Log de Tráfego do Atacante: ataque_malicious.txt (Saturação a 76.5 Mbps).
- [3] Log de Tráfego da Vítima L4S: ataque_l4s.txt (Colapso a 0.1 Mbps).
- [3] Log de Tráfego da Vítima Clássica: ataque_classic.txt (Degradação a 1.0 Mbps).
- [3] Log de Controle Malicioso: baseline_malicious.txt (Normalidade a 36.5 Mbps).
- [3] Log de Controle L4S: baseline_l4s.txt (Normalidade a 18.0 Mbps).

- [3] Log de Controle Clássico: baseline_classic.txt (Normalidade a 37.2 Mbps).
- [3] Documento de Contexto do Projeto: ADR_template.pdf.

Referências citadas

1. To switch or not to switch to TCP Prague? Incentives for adoption in a partial L4S deployment - arXiv, acessado em fevereiro 5, 2026, https://arxiv.org/html/2407.00464v1
2. RFC 9330 - Low Latency, Low Loss, and Scalable Throughput (L4S) Internet Service: Architecture - IETF Datatracker, acessado em fevereiro 5, 2026, https://datatracker.ietf.org/doc/rfc9330/
3. ADR_template.pdf
4. DualQ Coupled AQMs for Low Latency, Low Loss and Scalable Throughput (L4S) - IETF Datatracker, acessado em fevereiro 5, 2026, https://datatracker.ietf.org/doc/draft-ietf-tsvwg-aqm-dualq-coupled/24/
5. RFC 9332 - Dual-Queue Coupled Active Queue Management (AQM) for Low Latency, Low Loss, and Scalable Throughput (L4S) - Datatracker, acessado em fevereiro 5, 2026, https://datatracker.ietf.org/doc/rfc9332/
6. (PDF) Dual Queue Coupled AQM: Deployable Very Low Queuing Delay for All - ResearchGate, acessado em fevereiro 5, 2026, https://www.researchgate.net/publication/363269744_Dual_Queue_Coupled_AQM_Deployable_Very_Low_Queuing_Delay_for_All