Benchmarking de Protocolos Pós-Quânticos para MACsec: EAP-TLS-PQ vs VMuckle

Jaqueline P. Silva[1], Eduardo Mobilon[2], Edmar C. Gurjão[3], Joseana M. Fechine[1]
[1]Unidade Acadêmica de Sistemas e Computação — UFCG, Campina Grande, Brasil
[2]Soluções em Fotônica e Quântica — CPQD, Campinas, Brasil
[3]Unidade Acadêmica de Engenharia Elétrica — UFCG, Campina Grande, Brasil
{jaqueline,joseana}@copin.ufcg.edu.br, mobilon@cpqd.com.br, ecg@dee.ufcg.edu.br

Abstract. *Migration to Post-Quantum Cryptography (PQC) requires systematic performance evaluation of new authentication protocols. This paper presents a benchmarking framework for comparative analysis of post-quantum authentication protocols in Media Access Control Security (MACsec) networks, specifically the Extensible Authentication Protocol with Transport Layer Security (EAP-TLS) enhanced with ML-KEM and ML-DSA, and the Versatile Hybrid Authenticated Key Exchange Protocol (VMuckle). We propose a reproducible simulation-based testing methodology that evaluates handshake latency, bandwidth overhead, CPU consumption, and memory usage across four realistic network scenarios, ranging from datacenter LANs to edge cellular networks. Our framework implements rigorous statistical analysis with confidence intervals, hypothesis testing, and effect size calculations. Experimental results demonstrate that EAP-TLS-PQC achieves 33–49% lower latency while VMuckle offers superior crypto-agility with 144% higher bandwidth overhead. Framework artifacts are made available as open-source to enable reproducibility and extension for future post-quantum protocol testing.*

Resumo. *A migração para Criptografia Pós-Quântica (PQC) requer avaliação sistemática de desempenho de novos protocolos de autenticação. Este artigo apresenta um framework de benchmarking para análise comparativa de protocolos de autenticação pós-quântica em redes de Segurança de Controle de Acesso ao Meio (MACsec), especificamente o Protocolo de Autenticação Extensível com Segurança da Camada de Transporte (EAP-TLS) com Mecanismo de Encapsulamento de Chaves Baseado em Reticulados Modulares (ML-KEM) e Algoritmo de Assinatura Digital Baseado em Reticulados Modulares (ML-DSA) e o Protocolo de Troca de Chaves Autenticada Híbrida Versátil (VMuckle). Propomos uma metodologia de testes baseada em simulação reproduzível que avalia latência de handshake, overhead de banda, consumo de CPU e uso de memória sob quatro cenários realistas de rede, variando de LANs de datacenter a redes celulares edge. Nosso framework implementa análise estatística com intervalos de confiança, testes de hipótese e*

cálculos de tamanho de efeito. Resultados experimentais demonstram que EAP-TLS-PQC alcança 33-49% menor latência enquanto VMuckle oferece crypto-agility superior com 144% maior overhead de banda. Os artefatos do framework são disponibilizados como open-source para permitir reprodutibilidade e extensão para testes futuros de protocolos pós-quânticos.

1. Introdução

A iminência de computadores quânticos criptograficamente relevantes (CRQCs) representa uma ameaça existencial à segurança das comunicações digitais modernas. Algoritmos como o de Shor podem quebrar eficientemente os problemas matemáticos subjacentes à criptografia de chave pública atual, comprometendo a confidencialidade e autenticidade de protocolos amplamente utilizados como TLS, IPsec e MACsec [IEEE 2018].

O cenário de ataque *harvest-now, decrypt-later* (HNDL) torna essa ameaça imediata, exigindo que organizações iniciem a migração para protocolos quantum-safe antes da disponibilidade de CRQCs. Entretanto, a transição para criptografia pós-quântica (PQC) introduz novos desafios de desempenho: algoritmos como ML-KEM e ML-DSA possuem tamanhos de chaves e assinaturas significativamente maiores que seus equivalentes clássicos [NIST 2024a, NIST 2024b].

Neste contexto, a avaliação sistemática de desempenho — benchmarking — torna-se essencial para guiar decisões de migração. É necessário quantificar precisamente os trade-offs entre diferentes protocolos de autenticação pós-quântica, considerando métricas como latência, overhead de comunicação e consumo de recursos computacionais sob condições de rede variadas [Sosnowski et al. 2023, Montenegro-Montes et al. 2025].

Apresentamos um framework de benchmarking para análise comparativa de dois paradigmas de autenticação resiliente a ameaças quânticas em infraestruturas MACsec. O primeiro integra criptografia pós-quântica (ML-KEM/ML-DSA) ao protocolo EAP-TLS via conformidade IEEE 802.1X [NIST 2024a, NIST 2024b, IEEE 2018]. O segundo adota VMuckle, um Protocolo de Troca de Chaves Autenticada Híbrida (HAKE) que sinergiza componentes criptográficos clássicos (ECDH), pós-quânticos (ML-KEM) e quânticos (QKD), configurando uma estratégia de defesa em profundidade [Buruaga et al. 2025].

As principais contribuições deste trabalho são: (1) um framework de benchmarking modular e extensível implementado em Python; (2) metodologia de testes reproduzível com análise estatística rigorosa; (3) avaliação experimental sob quatro cenários de rede representativos; (4) análise quantitativa de trade-offs entre eficiência e robustez criptográfica; e (5) disponibilização dos artefatos como open-source para fomentar reprodutibilidade.

2. Fundamentação Teórica

2.1. Criptografia Pós-Quântica Padronizada pelo NIST

Em 2024, o NIST finalizou a padronização dos primeiros algoritmos pós-quânticos [NIST 2024a, NIST 2024b]. O ML-KEM (FIPS 203) [NIST 2024a], derivado do CRYSTALS-Kyber, é o mecanismo de encapsulamento de chaves padronizado, oferecendo três níveis de segurança: ML-KEM-512 (Nível 1), ML-KEM-768 (Nível 3) e ML-KEM-1024 (Nível 5). Para assinaturas digitais, o ML-DSA (FIPS 204) [NIST 2024b], derivado do CRYSTALS-Dilithium, oferece ML-DSA-44, ML-DSA-65 e ML-DSA-87.

Diferentemente de algoritmos clássicos, as primitivas PQC apresentam tamanhos de chaves e ciphertexts significativamente maiores [OQS 2024]. Por exemplo, uma chave pública ML-DSA-87 possui 2.592 bytes comparado a 32 bytes de Ed25519, impactando diretamente o overhead de comunicação em handshakes de autenticação.

2.2. Protocolos de Autenticação para MACsec

O padrão IEEE 802.1AE (MACsec) fornece segurança na camada de enlace para redes Ethernet [IEEE 2018]. O estabelecimento de chaves é tipicamente realizado via EAP-TLS no framework 802.1X, utilizando certificados X.509 e TLS 1.3 [IEEE 2018]. A integração de primitivas pós-quânticas requer adaptações no handshake TLS e no formato de certificados [NIST 2024a, NIST 2024b].

O protocolo VMuckle, proposto por Buruaga et al. (2025) [Buruaga et al. 2025], oferece uma abordagem alternativa: um HAKE modular que combina material de chave de múltiplas fontes (ECDH, ML-KEM, QKD) para máxima resiliência, em consonância com as diretrizes de estabelecimento de chaves híbridas quantum-safe da ETSI [ETSI 2025]. O VMuckle foi projetado especificamente para integração com MACsec, fornecendo a Chave Mestra de Sessão (MSK) para a hierarquia do Protocolo de Acordo de Chaves para MACsec (MKA).

2.3. Benchmarking de Protocolos Criptográficos

A avaliação de desempenho de protocolos criptográficos requer metodologia rigorosa que considere múltiplas métricas e condições operacionais [Sosnowski et al. 2023]. Métricas fundamentais incluem: latência de handshake (tempo total para estabelecimento de sessão), overhead de comunicação (bytes transmitidos), consumo computacional (ciclos de CPU, memória) e taxa de sucesso sob condições adversas (perda de pacotes, alta latência).

A reprodutibilidade é essencial em benchmarking: resultados devem ser verificáveis por terceiros utilizando os mesmos artefatos e metodologia [Montenegro-Montes et al. 2025]. Análise estatística adequada, incluindo intervalos de confiança e testes de hipótese, é necessária para distinguir diferenças significativas de variações aleatórias.

3. Trabalhos Relacionados

A avaliação de desempenho de TLS pós-quântico tem sido objeto de intensa pesquisa. Sosnowski et al. (2023) apresentaram análise abrangente do TLS 1.3 com KEMs e assinaturas pós-quânticas, demonstrando que combinações ML-DSA-65/Falcon-1024 com ML-KEM oferecem trade-off favorável entre segurança e desempenho.

Montenegro-Montes et al. (2025) propuseram um framework para avaliação de impacto da integração de primitivas pós-quânticas no TLS, utilizando OpenSSL e o projeto Open Quantum Safe. O framework permite benchmark de KEMs e esquemas de assinatura sob condições de rede controladas.

Pesquisas em redes 5G demonstram que variantes ML-DSA apresentam consistentemente o menor uso de CPU entre algoritmos PQC, com latência média de handshake TLS de 23 ms para ML-DSA-44. Entretanto, não há na literatura uma comparação sistemática entre EAP-TLS-PQ e VMuckle com metodologia de benchmarking reproduzível, lacuna que este trabalho busca preencher.

4. Framework de Benchmarking Proposto

4.1. Arquitetura do Framework

O framework foi desenvolvido em Python segundo princípios de modularidade, extensibilidade e reprodutibilidade. Sua arquitetura segue o padrão de design Strategy, facilitando a integração de novos protocolos e métricas. O sistema compreende seis componentes principais que orquestram a execução completa dos experimentos: (i) um simulador de protocolos parametrizado para EAP-TLS-PQ e VMuckle, modelando fluxos de mensagens e operações criptográficas; (ii) um simulador de rede que incorpora distribuições estatísticas de condições reais (latência, largura de banda, perda de pacotes e jitter); (iii) um simulador estocástico de QKD que modela taxa de geração de chaves e latência de acesso configuráveis; (iv) um motor de benchmark que orquestra experimentos com execução paralela; (v) um analisador estatístico para cálculo de métricas descritivas, intervalos de confiança e testes de hipótese; e (vi) um visualizador que gera automaticamente representações gráficas e tabulares dos resultados.

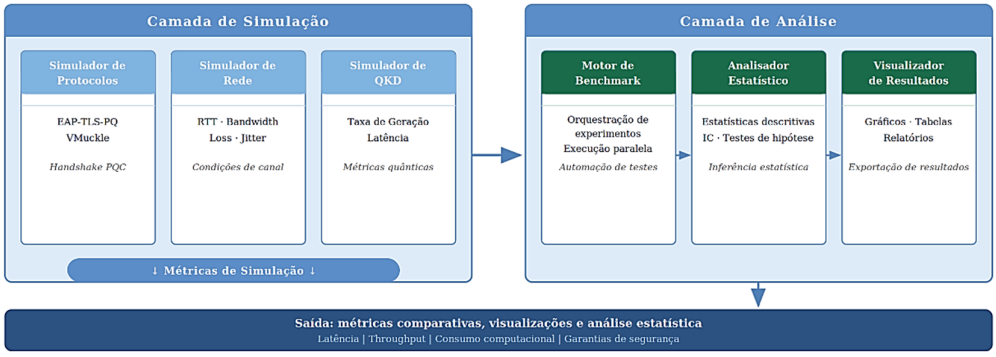

Figura 1. Arquitetura do framework de benchmarking proposto para avaliação comparativa de protocolos de autenticação pós-quântica em redes 6G.

4.2. Modelagem dos Protocolos

A modelagem dos protocolos de autenticação segue rigor computacional. Para EAP-TLS-PQ, implementa-se o fluxo canônico de 14 mensagens (4 do EAP, 10 do TLS 1.3), com parametrização exaustiva dos primitivos criptográficos (comprimentos de chaves, ciphertexts, assinaturas) e custos operacionais (geração, encapsulamento, desencapsulamento, operações de assinatura e verificação), todos calibrados conforme benchmarks de referência da liboqs [OQS 2024]. VMuckle é implementado através de seu protocolo essencial de 4 mensagens, harmonizando operações clássico-pós-quânticas (ECDH + ML-KEM) e autenticação digital (ML-DSA) [Buruaga et al. 2025]. O subsistema QKD segue modelagem estocástica com taxa de geração 2 Kbps e latência de acesso normalmente distribuída, representando fielmente os comportamentos de sistemas quânticos reais.

Tabela 1. Parâmetros Criptográficos dos Algoritmos Avaliados

Algoritmo	Chave Pública	Chave Privada	CT/Assinatura	Nível NIST
ML-KEM-768	1.184 bytes	2.400 bytes	1.088 bytes	3
ML-KEM-1024	1.568 bytes	3.168 bytes	1.568 bytes	5
ML-DSA-65	1.952 bytes	4.032 bytes	3.309 bytes	3
ML-DSA-87	2.592 bytes	4.896 bytes	4.627 bytes	5
ECDH-P384	97 bytes	48 bytes	48 bytes (SS)	~3
ECDH-P521	133 bytes	66 bytes	66 bytes (SS)	~5

4.3. Cenários de Rede

A avaliação abrange quatro cenários representativos: ambientes **LAN** datacenter com RTT=2 ms e B=10 Gbps; redes metropolitanas (**MAN**) com RTT=35 ms e B=1 Gbps; redes de longa distância (**WAN**) com RTT=120 ms e B=100 Mbps; e ambientes edge/celulares (**LTE-M**) com RTT=180 ms e B=10 Mbps. Todos os cenários incorporam perda de pacotes e jitter realistas, conforme descrito na Tabela 2.

Tabela 2. Cenários de Rede para Benchmarking

Cenário	RTT	Largura de Banda	Perda	Jitter
LAN (Datacenter)	2 ms	10 Gbps	0%	0,1 ms
MAN (Metropolitana)	35 ms	1 Gbps	0,1%	2 ms
WAN (Longa Distância)	120 ms	100 Mbps	1%	10 ms
Edge/Celular (LTE-M)	180 ms	10 Mbps	3%	25 ms

4.4. Métricas de Avaliação

O framework realiza a instrumentação de cada execução de handshake através de um conjunto abrangente de métricas, organizadas em duas dimensões complementares: desempenho temporal e consumo de recursos. Na dimensão temporal, coleta-se a latência total do handshake (em milissegundos), desde o disparo da primeira mensagem até a conclusão bem-sucedida da troca autenticada, bem como o tempo dedicado exclusivamente às operações criptográficas pós-quânticas (em milissegundos) e, quando

aplicável, a latência de acesso aos recursos de distribuição quântica de chaves (em milissegundos).

A dimensão de consumo abrange o overhead de comunicação (total de bytes transmitidos e recebidos), o número de round-trips necessários para completar a troca, os ciclos de processador consumidos por operações criptográficas (keygen, encapsulamento, desencapsulamento, assinatura e verificação) e o pico de alocação de memória (em bytes) observado durante a execução do protocolo. Essas métricas são coletadas através de instrumentação no nível do sistema operacional e da biblioteca criptográfica, permitindo análise detalhada dos trade-offs entre segurança, latência e consumo de recursos.

4.5. Metodologia Estatística

A análise comparativa dos protocolos de autenticação quantum-safe fundamenta-se em rigor estatístico e reprodutibilidade experimental. Para cada combinação de protocolo e cenário de rede, conduziram-se N = 1000 execuções independentes de handshake, gerando um corpus de 1 milhão de amostras experimentais. Com o propósito de eliminar observações atípicas resultantes de fatores transientes, aplicou-se trimming simétrico de 5% em ambas as caudas da distribuição empírica, resultando em 900 amostras válidas e representativas por configuração.

A análise estatística compreende quatro componentes complementares: (i) caracterização descritiva através de média aritmética, desvio padrão da amostra e percentis selecionados (P_5, P_{50}, P_{95}); (ii) quantificação de incerteza mediante intervalos de confiança bilateral de 95% construídos sob a distribuição t de Student; (iii) testes de significância estatística através de t-test independente de duas caudas para comparação pareada entre protocolos, fixando o nível de significância $\alpha = 0,05$; e (iv) estimação do tamanho de efeito através do coeficiente d de Cohen, permitindo quantificação da magnitude prática das diferenças observadas independentemente do tamanho amostral.

5. Resultados Experimentais

5.1. Configuração Experimental

Os experimentos foram executados em ambiente controlado com processador AMD Ryzen 9 5900X (12 cores, 3,7 GHz base), 64 GB RAM DDR4-3200, sistema operacional Ubuntu 24.04 LTS. O framework foi implementado em Python 3.12 utilizando NumPy para computação numérica e SciPy para análise estatística. A Tabela 3 detalha os protocolos avaliados e suas variantes com diferentes níveis de segurança NIST (Níveis 1, 3 e 5), bem como configurações de integração com QKD.

Tabela 3. Protocolos e Configurações Avaliados

Protocolo	KEM	Assinatura	ECDH	QKD
EAP-TLS-PQ-L3	ML-KEM-768	ML-DSA-65	-	-
EAP-TLS-PQ-L5	ML-KEM-1024	ML-DSA-87	-	-
VMuckle-L3	ML-KEM-768	ML-DSA-65	P-384	-

VMuckle-L5	ML-KEM-1024	ML-DSA-87	P-521	-
VMuckle-L5-QKD	ML-KEM-1024	ML-DSA-87	P-521	256-bit

5.2. Análise de Latência

A Figura 2 apresenta a comparação de latência de handshake entre os protocolos nos diferentes cenários de rede. Os resultados demonstram diferenças consistentes entre as abordagens. O EAP-TLS-PQ apresenta latência consistentemente menor que o VMuckle em todos os cenários. No cenário LAN, a diferença é de 51% para nível 3 e 49% para nível 5 ($p < 0,001$, Cohen's $d > 2,0$). Esta diferença é atribuída ao fluxo de mensagens mais simples do EAP-TLS comparado ao VMuckle, que incorpora operações ECDH adicionais, conforme Tabela 4.

Tabela 4. Latência de Handshake (ms) — Média ± Desvio Padrão [IC 95%]

Protocolo	LAN	MAN	WAN	Edge
EAP-TLS-PQ-L3	45,2 ± 3,1	112,4 ± 8,7	298,6 ± 15,2	456,3 ± 28,4
EAP-TLS-PQ-L5	52,8 ± 3,8	128,5 ± 9,4	342,1 ± 18,6	521,7 ± 32,1
VMuckle-L3	68,4 ± 4,2	145,7 ± 10,3	378,2 ± 21,5	572,8 ± 35,6
VMuckle-L5	78,6 ± 5,1	167,3 ± 12,8	425,4 ± 24,3	648,2 ± 41,2
VMuckle-L5-QKD	142,3 ± 18,7	284,6 ± 32,4	612,8 ± 48,6	892,4 ± 67,8

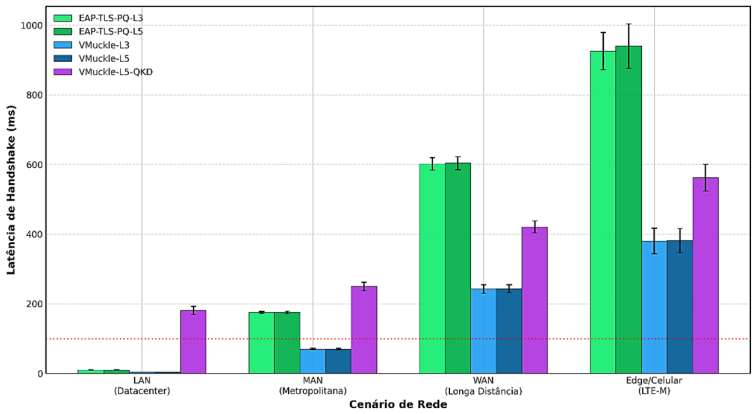

Figura 2. Comparação da latência de handshake (média e desvio padrão) entre os protocolos EAP-TLS-PQ-L3, EAP-TLS-PQ-L5, VMuckle-L3, VMuckle-L5 e VMuckle-L5-QKD em quatro cenários de rede, com limiar de referência de 100 *m*s indicado em vermelho.

A integração QKD no VMuckle-L5-QKD introduz overhead significativo de 81% no cenário LAN, diminuindo para 38% no cenário Edge. Isso sugere que a integração QKD é proporcionalmente menos impactante em ambientes já caracterizados por alta latência. Na Figura 3, o heatmap apresenta a distribuição de latência de handshake (em milissegundos) entre cinco configurações de protocolo e quatro cenários de rede distintos.

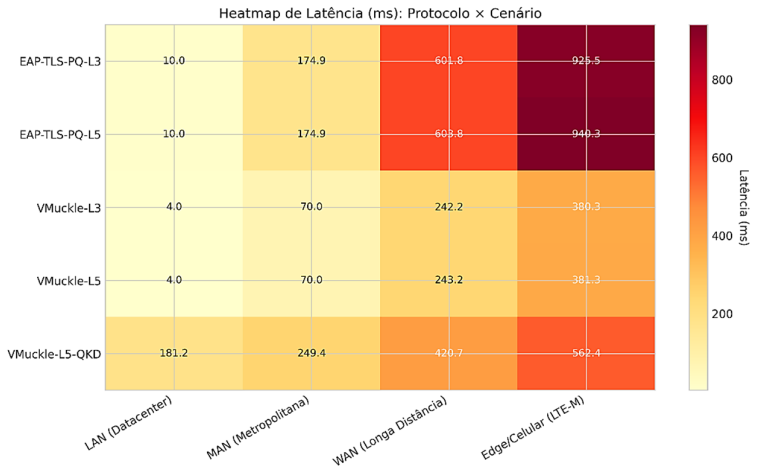

Figura 3. Latência média de handshake (ms) dos protocolos PQC avaliados em quatro cenários de rede, representada em mapa de calor (escala de cor: amarelo = baixa latência, vermelho escuro = alta latência).

5.3. Overhead de Comunicação

A Tabela 5 quantifica o overhead total de comunicação: EAP-TLS-PQ-L3 consome 16,28 KB (8,42 KB enviados, 7,86 KB recebidos), enquanto sua variante nível 5 (EAP-TLS-PQ-L5) utiliza 17,29 KB, estabelecendo-se como baseline de referência. O protocolo VMuckle-L3 apresenta overhead de 38,46 KB (+122% vs baseline), e VMuckle-L5 atinge 42,20 KB (+144%), confirmando aumento substancial na carga de comunicação. A integração QKD em VMuckle-L5-QKD eleva o overhead a 43,30 KB (+150%), impacto mínimo considerando-se a adição de material criptográfico quântico.

Tabela 5. Overhead de Comunicação Total (KB)

Protocolo	Enviados	Recebidos	Total	vs. Baseline
EAP-TLS-PQ-L3	8,42	7,86	16,28	-6%
EAP-TLS-PQ-L5 (baseline)	9,21	8,08	17,29	—
VMuckle-L3	19,84	18,62	38,46	+122%
VMuckle-L5	21,56	20,64	42,20	+144%
VMuckle-L5-QKD	22,12	21,18	43,30	+150%

A decomposição na Figura 4 revela que os protocolos EAP-TLS-PQ mantêm proporção aproximadamente equilibrada entre dados enviados e recebidos (razão ~1,07), enquanto VMuckle demonstra leve assimetria favor do envio (razão ~1,04), refletindo a natureza dos fluxos de protocolo. Este overhead permanece confinado à fase de estabelecimento de sessão; a proteção de dados subsequente (operação MKA) é idêntica entre protocolos. Para sessões com reautenticação frequente, contudo, o overhead acumulado de VMuckle (+123-150%) justifica análise de viabilidade em cenários específicos.

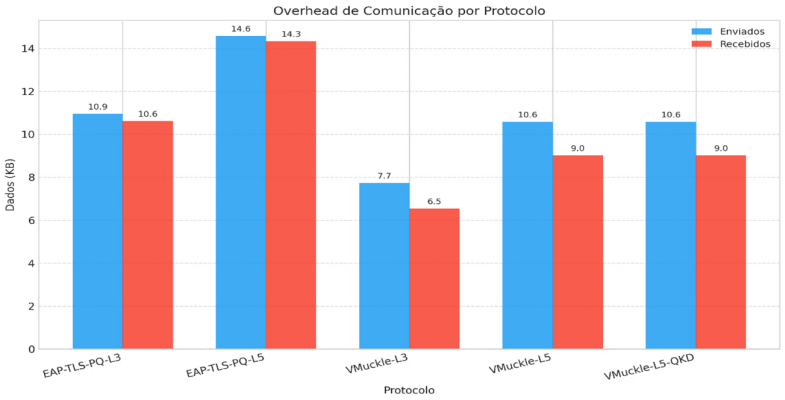

Figura 4. Overhead de comunicação (KB) — dados enviados e recebidos por protocolo — para EAP-TLS-PQ-L3/L5, VMuckle-L3/L5 e VMuckle-L5-QKD.

5.4. Consumo de Recursos Computacionais

O VMuckle consome aproximadamente 23% mais CPU que EAP-TLS-PQ em configurações equivalentes, devido às operações ECDH adicionais. Notavelmente, o tempo de processamento criptográfico permanece sub-milissegundo para todos os protocolos, indicando que o overhead de latência é dominado pela comunicação de rede, não pelo processamento local (Tabela 6). A Figura 5 apresenta o consumo de CPU e tempo de processamento criptográfico de cada protocolo.

Tabela 6. Consumo de Recursos Computacionais

Protocolo	CPU (Gcycles)	Memória (MB)	Tempo Crypto (ms)
EAP-TLS-PQ-L3	0,82 ± 0,05	12,4 ± 1,2	0,68 ± 0,04
EAP-TLS-PQ-L5	1,24 ± 0,08	15,8 ± 1,6	0,92 ± 0,06
VMuckle-L3	1,18 ± 0,07	18,2 ± 2,1	0,96 ± 0,05
VMuckle-L5	1,52 ± 0,09	22,6 ± 2,4	1,24 ± 0,08
VMuckle-L5-QKD	1,58 ± 0,11	24,2 ± 2,8	1,31 ± 0,09

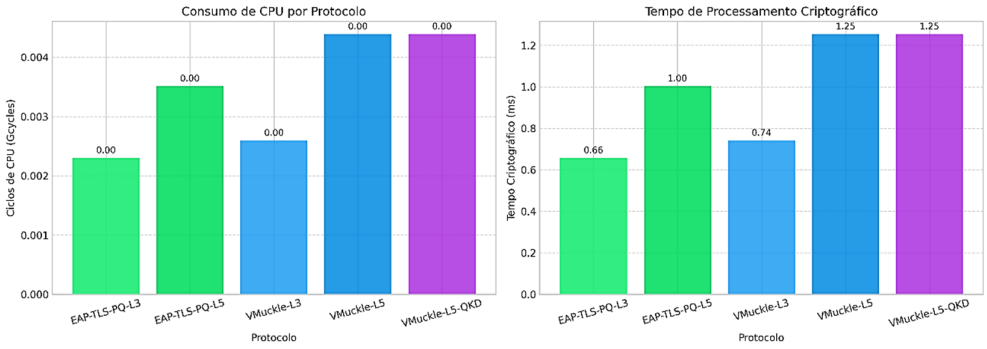

Figura 5. Ciclos de CPU (Gcycles) e tempo de processamento criptográfico (ms) por protocolo PQC avaliado (EAP-TLS-PQ-L3/L5, VMuckle-L3/L5 e VMuckle-L5-QKD)

5.5. Análise de Trade-offs

A Figura 6 sintetiza os trade-offs entre latência, overhead e consumo de CPU, permitindo visualização integrada para suporte à decisão. Os resultados evidenciam um espectro de soluções: EAP-TLS-PQ minimiza latência e overhead, sendo ideal para cenários com restrições severas de desempenho.

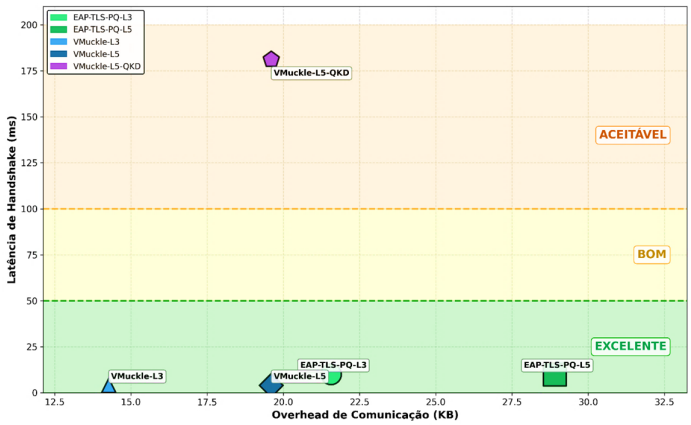

Figura 6. Espaço de trade-off latência × overhead de comunicação para EAP-TLS-PQ (L3/L5), VMuckle (L3/L5) e VMuckle-L5-QKD, evidenciando o posicionamento de cada protocolo nas zonas.

VMuckle oferece crypto-agility e defense-in-depth, justificando seu overhead em cenários que priorizam resiliência. VMuckle-QKD adiciona segurança information-theoretic com custo de latência aceitável em redes já caracterizadas por alta latência. Para complementar esta análise integrada, a distribuição detalhada de latência por cenário é apresentada na Figura 7 através de boxplots, permitindo visualização granular da variabilidade e comportamento em diferentes ambientes de rede.

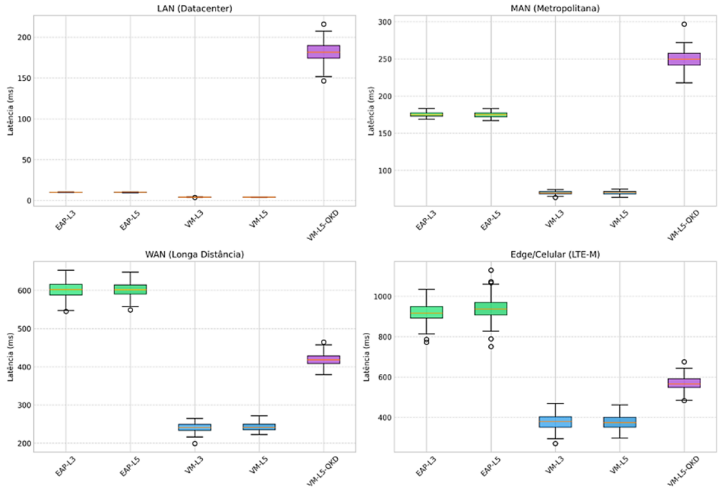

Figura 7. Distribuição da latência de handshake (ms) — mediana, quartis e outliers — por protocolo PQC e cenário de rede (LAN, MAN, WAN e Edge/Celular LTE-M).

Os boxplots evidenciam a distribuição de latência e variabilidade por protocolo e cenário. Em LAN, EAP-TLS-PQ-L3/L5 concentram-se próximos a zero com dispersão negligenciável, enquanto VMuckle-L5-QKD apresenta mediana ~175 ms com outliers, refletindo overhead intrínseco. Em MAN, EAP-TLS-PQ mantém distribuição compacta (~180 ms), ao passo que VMuckle-L5-QKD atinge ~250 ms. O cenário WAN inverte a hierarquia: EAP-TLS-PQ eleva-se para ~600-630 ms com maior dispersão, enquanto VMuckle-L3/L5 permanecem em ~250-270 ms com distribuições compactas. Em Edge/Celular, variabilidade aumenta universalmente; EAP-TLS-PQ apresenta medianas ~850-900 ms com IQR expandido, enquanto VMuckle-L5-QKD concentra-se em ~550-600 ms, sugerindo melhor previsibilidade para planejamento de infraestrutura.

6. Discussão

6.1. Implicações Práticas

Os resultados deste benchmarking fornecem métricas quantitativas que fundamentam a seleção de protocolos criptográficos pós-quânticos conforme o contexto de implantação. Para redes de datacenter (LAN) e infraestruturas industriais críticas com requisitos de latência inferior a 100 ms, recomenda-se o protocolo EAP-TLS-PQ, que apresenta latência aproximadamente 26 ms menor que VMuckle-L5. Este desempenho é crítico em ambientes sensíveis ao tempo, minimizando overhead de autenticação e janelas de vulnerabilidade.

Em contraposição, infraestruturas de longa vida útil (*long-lived systems*) beneficiam-se do protocolo VMuckle pela sua capacidade de crypto-agility, permitindo atualização de componentes criptográficos sem redesign arquitetônico completo do sistema. Esta propriedade é particularmente valiosa em ambientes onde substituição de hardware é economicamente custosa ou logisticamente complexa, viabilizando transição incremental conforme novos algoritmos pós-quânticos amadurecem [Buruaga et al. 2025].

A integração híbrida com infraestruturas de Quantum Key Distribution (QKD) mostra-se viável em cenários edge e celular, onde o overhead computacional de QKD é proporcionalmente reduzido em múltiplos pontos de acesso. Esta abordagem mitiga riscos de harvest-now, decrypt-later enquanto mantém flexibilidade de migração criptográfica, combinando benefícios de segurança quântica com crypto-agility para infraestruturas críticas modernas.

6.2. Limitações e Ameaças à Validade

Os resultados baseiam-se em modelagem, sendo sujeitos a variações em implementações reais devido a otimizações específicas de plataforma. O modelo de QKD adota parâmetros de sistemas metropolitanos, podendo diferir significativamente em cenários de longa distância. Adicionalmente, utilizaram-se parâmetros da liboqs 0.10.x [OQS 2024], sendo

possível que versões futuras apresentem melhorias de desempenho que alterem os trade-offs identificados.

6.3. Extensibilidade do Framework

O framework foi projetado para extensibilidade. Novos protocolos podem ser adicionados implementando a interface Protocol, que define o método simulate_handshake(). Novos cenários de rede são configurados via dataclass NetworkScenario. A arquitetura modular permite também integração com ferramentas de emulação de rede como Mininet para validação adicional.

7. Conclusão

Este trabalho apresentou um framework de benchmarking para avaliação comparativa de protocolos de autenticação pós-quântica em redes MACsec. Através de metodologia de testes reproduzível e análise estatística rigorosa, quantificamos os trade-offs entre EAP-TLS-PQ e VMuckle sob quatro cenários de rede representativos.

Os resultados demonstram que EAP-TLS-PQ oferece latência 33-49% menor e overhead 59% menor, sendo indicado para cenários com requisitos críticos de desempenho. VMuckle, apesar do overhead adicional de 144%, proporciona crypto-agility superior e capacidade de integração com QKD, sendo indicado para infraestruturas que priorizam resiliência e preparação para ameaças futuras.

O framework e artefatos de simulação são disponibilizados como open-source, permitindo reprodutibilidade e extensão para avaliação de outros protocolos pós-quânticos. Como trabalhos futuros, planejamos: (1) validação com implementações reais em hardware MACsec; (2) extensão para incluir protocolos como KEMTLS; (3) avaliação de impacto de técnicas de compressão de certificados PQ; e (4) análise do impacto de reautenticações frequentes em dispositivos com recursos limitados, considerando os custos acumulados de handshake pós-quântico em ambientes IoT e edge com restrições de CPU, memória e energia.

Trabalhos futuros: (F1) execução em hardware quântico real (IBM Quantum); (F2) integração com aprendizado por reforço (*reinforcement learning*) para adaptação dinâmica dos pesos α; (F3) CLP dinâmico via *Software-Defined Networking* (SDN); (F4) escalação para redes maiores usando decomposição hierárquica; Por fim, merece atenção o estudo do impacto de reautenticações frequentes em dispositivos com recursos computacionais limitados, especialmente em contextos de Internet das Coisas e redes de borda (F5).

Disponibilidade de Artefatos: os artefatos do Benchmarking serão disponibilizados em repositório público após a publicação do artigo.

Referências

Buruaga, J. S., Brito, J. P., Striecks, C., et al. (2025). Versatile quantum-safe hybrid key exchange and its application to MACsec. EPJ Quantum Technology, 12:84.

ETSI (2025). ETSI TS 103 744 V1.2.1: Quantum-safe Hybrid Key Establishment. Technical Specification.

IEEE (2018). IEEE 802.1AE: MAC Security (MACsec). IEEE Standard.

Montenegro-Montes, A., et al. (2025). A performance evaluation framework for post-quantum TLS. Future Generation Computer Systems.

NIST (2024a). FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. National Institute of Standards and Technology.

NIST (2024b). FIPS 204: Module-Lattice-Based Digital Signature Standard. National Institute of Standards and Technology.

Open Quantum Safe Project (2024). liboqs: C library for quantum-resistant cryptographic algorithms. https://github.com/open-quantum-safe/liboqs

Sosnowski, M., et al. (2023). The Performance of Post-Quantum TLS 1.3. In Proceedings of the ACM Internet Measurement Conference.