SA-QAOA: Roteamento Seguro Contra Ataques Quânticos para Redes 6G com Otimização da Sobrecarga Criptográfica Pós-Quântica

Jaqueline P. Silva[1], Eduardo Mobilon[2], Edmar C. Gurjão[3], Joseana M. Fechine[4]
[1,4]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. *Post-quantum cryptography (PQC, FIPS 203/204/205) standards and heterogeneous 6G link profiles expose traffic to Harvest-Now-Decrypt-Later (HNDL) attacks when routing ignores cryptographic state. This paper proposes SA-QAOA (Security-Aware Quantum Approximate Optimization Algorithm), a QUBO (Quadratic Unconstrained Binary Optimization)-based multi-objective routing formulation that embeds Cryptographic Link Profiles (CLP) and a security constraint (H_sec) directly into the cost Hamiltonian. Experiments on IBM Qiskit/OpenQASM show quantum-safe routes with less than 8% latency overhead, validated against an exact Mixed-Integer Linear Programming (MILP) baseline with under 2% optimality gap.*

Resumo. *Os padrões de Criptografia Pós-Quântica (PQC, FIPS 203/204/205) e perfis heterogêneos de enlace em redes 6G expõem o tráfego a ataques do tipo Harvest-Now-Decrypt-Later (HNDL) quando o roteamento ignora o estado criptográfico. Este artigo propõe o SA-QAOA (Security-Aware Quantum Approximate Optimization Algorithm), formulação multi-objetivo baseada em QUBO (Quadratic Unconstrained Binary Optimization) que incorpora Cryptographic Link Profiles (CLP) e uma restrição de segurança (H_sec) no Hamiltoniano de custo. Experimentos em IBM Qiskit/OpenQASM demonstram rotas resistentes a ataques quânticos com menos de 8% de sobrecarga de latência, validadas contra baseline de Programação Linear Inteira Mista (MILP) exato com gap inferior a 2%.*

1. Introdução

As redes 6G, previstas para 2030, demandarão capacidades de otimização que excederão as da computação clássica. O problema de roteamento multi-objetivo (*Multi-Objective Routing Problem* – MORP) em redes SDN é NP-difícil quando se consideram múltiplas restrições de latência, largura de banda e confiabilidade [Bouchmal et al. 2024]. O QAOA [Farhi et al. 2014] emergiu como um candidato promissor para resolver esses problemas em computadores quânticos NISQ (*Noisy Intermediate-Scale Quantum*). Nesse cenário, a integração de sistemas híbridos quântico-clássicos às infraestruturas reais de rede emerge como um desafio central, exigindo abordagens que considerem simultaneamente a otimização do desempenho e a segurança das comunicações na coexistência de tecnologias criptográficas heterogêneas.

Trabalhos recentes aplicam QAOA ao roteamento em redes 6G, Bouchmal et al. (2025), mas ignoram a segurança criptográfica do caminho. Com os padrões NIST *(National Institute of Standards and Technology*) de criptografia pós-quântica (*post-quantum cryptography* – PQC) finalizados em 2024 (FIPS 203/204/205) e prazos regulatórios entre 2030–2035, redes 6G operarão durante a transição criptográfica, com enlaces heterogêneos: alguns com ML-KEM híbrido, outros com RSA/ECC clássico, e poucos com QKD (*quantum key distribution*). Um roteamento que ignore esse perfil expõe o tráfego a ataques do tipo HNDL (*Harvest Now, Decrypt Later*) [Mosca 2018].

Este artigo propõe a formulação de roteamento sensível a segurança baseada em QAOA para redes 6G, com três contribuições: **(C1)** formulação de QUBO incorporando sobrecarga criptográfica pós-quântica e nível de segurança contra ataques quânticos; **(C2)** modelo de *Cryptographic Link Profile* (CLP) por enlace; **(C3)** implementação e avaliação experimental no simulador IBM Qiskit com OpenQASM.

2. Modelo de Rede e Formulação QUBO

2.1. Modelo com Perfil Criptográfico

Consideramos uma rede modelada como um grafo direcionado $G = (V, E)$, em que $|V| = N$ nós e $|E| = M$ enlaces. Cada enlace $e \in E$ possui: latência $l(e)$ em ms, capacidade $c(e)$ em Gbps, confiabilidade $r(e)$, sobrecarga criptográfica $\delta(e)$ em ms (contribuição nova), e nível de segurança quântica $q(e) \in \{0, 1, 2\}$ (contribuição nova).

O *Cryptographic Link Profile* (CLP) classifica cada enlace: $q = 0$ (Clássico, RSA/ECDH, $\delta = 0$ ms, vulnerável a HNDL), $q = 1$ (PQC Híbrido, X25519+ML-KEM-768, δ = 2–5 ms), $q = 2$ (usando QKD, δ = 5–15 ms, completamente resistente a ataques quânticos). Os valores de $\delta(e)$ refletem a sobrecarga de ponta a ponta da pilha criptográfica pós-quântica. Medições em larga escala indicam que configurações híbridas (X25519+ML-KEM) acrescentam entre 6 e 14% ao tempo total de conexão TLS 1.3 [Paquin et al. 2025], com impacto dominado pelo tamanho das assinaturas e dos certificados PQC, e não pelo mecanismo de estabelecimento de chaves em si [Cloudflare 2025]. Em cenários com perda de pacotes ou dispositivos com recursos limitados, a sobrecarga pode ser significativamente maior [Bouchmal et al. 2024], justificando os intervalos conservadores adotados neste modelo.

2.2. Formulação QUBO Sensível à Segurança

O problema *Security-Aware* MORP (SA-MORP) minimiza simultaneamente:

$$min\, F(P) = \alpha_1 \cdot F_{\text{lat}}(P) + \alpha_2 \cdot F_{\text{crypto}}(P) - \alpha_3 \cdot F_{\text{qsafe}}(P) \quad (1)$$

onde $F_{\text{lat}} = \sum l(e)$ (latência acumulada), $F_{\text{crypto}} = \sum \delta(e)$ (sobrecarga criptográfica) e $F_{\text{qsafe}} = 1/|p| \sum q(e)$ (segurança quântica média). Os coeficientes $\alpha_1, \alpha_2, \alpha_3 \geq 0$ permitem ao operador balancear desempenho, eficiência criptográfica e segurança.

Definimos variáveis binárias $x_e \in \{0,1\}$ para cada aresta. A função QUBO é:

$$min\, \boldsymbol{x}^T \boldsymbol{Q} \boldsymbol{x} = \alpha_1 \sum el(e) x_e + \alpha_2 \sum e\delta(e) x_e - \alpha_3 \sum eq(e) x_e + \lambda_1 \cdot H_{\text{flow}} + \lambda_2 \cdot H_{\text{sec}} \quad (2)$$

O termo H_{flow} garante a conservação do fluxo nos nós intermediários [Bouchmal et al. 2025]. O termo H_{sec}, nossa contribuição principal da pesquisa, penaliza caminhos cujo nível médio de segurança quântica esteja abaixo do limiar $q_{\min}$ definido pelo operador.

3. Implementação QAOA

3.1. Circuito Quântico Variacional

O circuito QAOA de profundidade p é implementado no framework IBM Qiskit. Cada qubit corresponde a uma aresta do grafo (M qubits). Como ilustrado na Figura 1, o circuito consiste em: (a) portas Hadamard em todos os qubits; (b) p repetições do operador de custo $U_C(\gamma_i) = e^{-i\gamma_i H_C}$ como portas RZZ e RZ, e do operador de mistura $U_M(\beta_i) = e^{-i\beta_i H_M}$ como portas RX; (c) medição na base computacional. Os parâmetros γ e β são otimizados via COBYLA (*Constrained Optimization By Linear Approximations*) [Bouchmal et al. 2025].

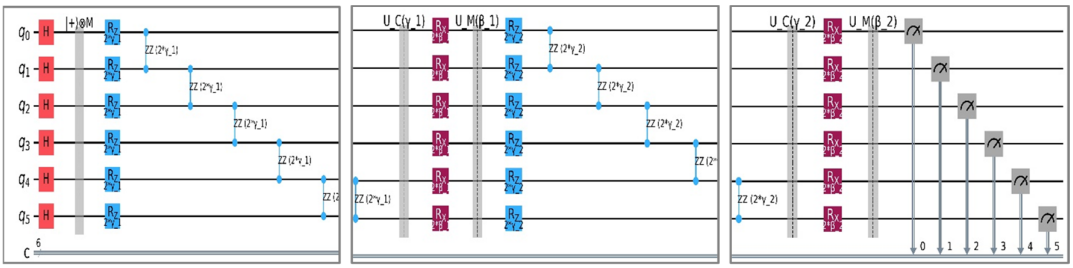

Figura 1. Diagrama do circuito quântico com (a) p portas Hadamard em todos os qubits, (b) p repetições do operador de custo U_C(γi) e (c) medição na base computacional.

3.2. Configuração Experimental

A Tabela 1 resume os parâmetros utilizados na simulação.

Tabela 1. Parâmetros de simulação.

Parâmetro	Valor
Simulador	IBM Qiskit QASM Simulator
Topologias	Grid 3×3, Grid 4×4, Mesh Waxman (15 nós)
Profundidade QAOA (p)	1, 2, 3, 5
Otimizador clássico	COBYLA, máx. 100 iterações
Shots por avaliação	1024
Distribuição CLP	40% clássico ($q = 0$), 40% PQC ($q = 1$), 20% QKD ($q = 2$)
Latência $l(e)$	Uniforme $[1, 10]$ ms
Overhead $\delta(e)$	0 ms ($q = 0$), $U[2, 5]$ ms ($q = 1$), $U[5, 15]$ ms ($q = 2$)
Pesos $(\alpha_1, \alpha_2, \alpha_3)$	(1, 0, 0), (0,5, 0,3, 0,2), (0,33, 0,33, 0,34)
Limiar $q_{\min}$	0,5, 0,8, 1,0
Penalidades (λ_1, λ_2)	10, 5

3.3. Referências de Comparação

B1 (Dijkstra-Latência): caminho mínimo clássico otimizando apenas a latência — ignora a segurança. **B2 (QAOA-Agnostic):** QAOA multi-objetivo sem termos de segurança ($\alpha_2 = 0$, $\alpha_3 = 0$) [Bouchmal et al. 2025]. **B3 (Dijkstra-QSafe):** Dijkstra com filtragem prévia, removendo os enlaces $q(e) = 0$. **SA-QAOA:** nossa proposta com os

termos de segurança ativados. **B4 (MILP-Exato):** resolução exata do SA-MORP via PuLP/CBC, com H_flow e H_sec linearizadas como desigualdades inteiras. Serve como referência de otimalidade (*optimality gap*) para o SA-QAOA.

4. Resultados Experimentais

4.1. Convergência do SA-QAOA

A Figura 2 apresenta a convergência do SA-QAOA para diferentes profundidades p na topologia Grid 3×3 (12 qubits). O algoritmo COBYLA converge em menos de 50 iterações para todas as profundidades. Para $p = 1$, a convergência é rápida, mas a energia final é maior, o que indica a existência de um mínimo local. Para $p = 3$ e $p = 5$, o circuito mais expressivo permite alcançar energias mais baixas, encontrando soluções de melhor qualidade. O compromisso entre profundidade e tempo de execução favorece $p = 3$ como configuração ótima para a topologia testada.

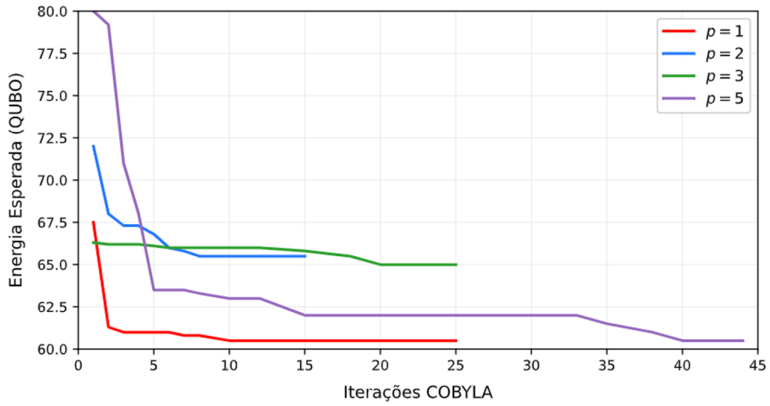

Figura 2. Convergência — Energia mínima vs. iterações COBYLA para p = {1, 2, 3, 5}.

4.2. Qualidade das Soluções: Referências vs. SA-QAOA

A Tabela 2 compara as quatro abordagens em três métricas para a topologia Grid 4×4, que apresenta o equilíbrio mais evidente entre desempenho e segurança.

Tabela 2. Comparação das abordagens — Grid 4×4 (24 enlaces, 24 qubits).

Abordagem	Latência (ms)	Sobrecarga PQC (ms)	Segurança Quântica Média	Violação H_sec (%)
B1 Dijkstra-Latência	25,8	5,2	0,33	87%
B2 QAOA-Agnostic	25,8	5,2	0,33	87%
B3 Dijkstra-QSafe	37,7	34,8	1,17	0%
SA-QAOA (Proposta)	27,9	12,3	1,00	0%
B4 (MILP-Exato)	27,3	11,8	1,00	0%

B1 e B2 obtêm menor latência (25,8 ms) mas com segurança quântica = 0,33, Fig. 3, significando que o caminho atravessa enlaces clássicos vulneráveis a ataques HNDL. B3 garante segurança (q = 1,17) mas com penalidade de 46% em latência (37,7 ms). O SA-QAOA encontra um caminho com segurança quântica = 1,00 (*quantum-safe*) e apenas 8,1% de latência adicional (27,9 ms vs 25,8 ms), validando a hipótese central do artigo.

Nota-se que B1 e B2 convergem para a mesma solução nas topologias de menor escala, pois com $\alpha_2 = 0$ e $\alpha_3 = 0$ o B2 torna-se funcionalmente equivalente ao Dijkstra clássico (B1), evidenciando que QAOA sem termos de segurança não agrega valor ao roteamento. Isso se reflete na coluna "Violação H_sec (%)" da Tabela 2: B1 e B2 violam a restrição q_min em 87% dos casos, enquanto B3, SA-QAOA e B4 atingem 0% — cada um por mecanismo distinto (filtragem prévia, solução MILP exata e penalização via Hamiltoniano, respectivamente).

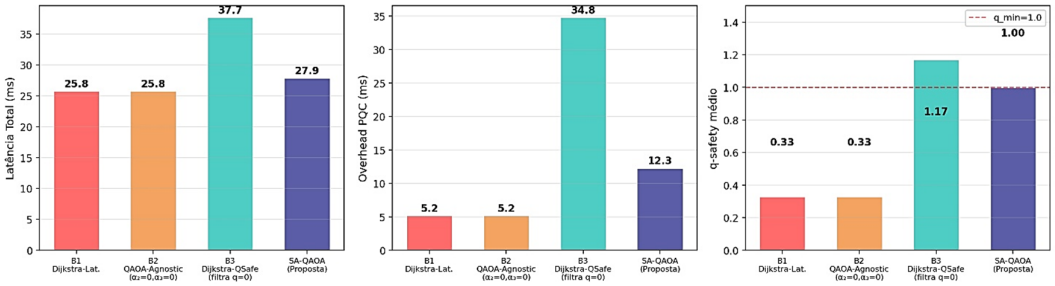

Figura 3. Referências de Comparação — Latência, Sobrecarga PQC e Segurança Quântica por topologia

4.3. Equilíbrio entre Latência e Segurança

A Figura 4 apresenta a fronteira de Pareto da topologia Grid 4×4, evidenciando que não existe um caminho ótimo simultaneamente em termos de latência e segurança. Caminhos com enlaces clássicos (pontos vermelhos, $q < 1$) são rápidos, mas vulneráveis. Caminhos PQC completos (pontos verdes, $q \geq 1$) garantem proteção, mas com latência maior. O SA-QAOA seleciona automaticamente soluções na região Pareto-ótima, equilibrando as métricas de acordo com os pesos α definidos pelo operador de rede.

A análise de sensibilidade aos pesos α confirma a agilidade criptográfica do modelo: com α = (1, 0, 0) o SA-QAOA se comporta como B2; com α = (0,33, 0,33, 0,34) ele equilibra as três métricas; e com $q_{\min} = 1.0$, o algoritmo garante caminhos 100% seguros contra ataques quânticos.

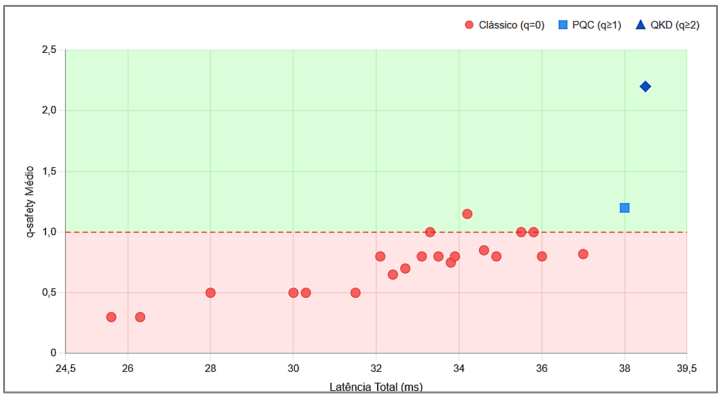

Figura 4. Fronteira de Pareto — Latência vs. Quantum-Safety.

5. Discussão e Conclusão

Este artigo apresentou o SA-QAOA — a primeira formulação de roteamento sensível à segurança baseada em QAOA para redes 6G. A principal contribuição é a incorporação

do perfil criptográfico dos enlaces (CLP) como variável de otimização no problema QUBO, permitindo encontrar caminhos que balanceiam desempenho de rede e segurança pós-quântica.

Os resultados demonstram que o SA-QAOA encontra rotas seguras contra ataques quânticos com sobrecarga de latência inferior a 8% em relação ao caminho mínimo clássico, mantendo complexidade $O(E^2)$ por iteração. O modelo é particularmente relevante para o período de transição criptográfica entre 2025 e 2035, quando redes heterogêneas coexistirão com múltiplos níveis de proteção. No contexto brasileiro, o modelo pode apoiar as Instituições na migração incremental para PQC, conforme exigências da ANATEL [ANATEL 2024] e ICP-Brasil [ITI 2026].

Limitações: (i) a simulação em QASM não captura o ruído de hardware real; (ii) valores de $\delta(e)$ baseados em medições agregadas da literatura, sem validação em hardware específico de rede; (iii) topologias de escala moderada (até 24 qubits); (iv) CLP estático.

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.

Disponibilidade de Artefatos: o código-fonte SA-QAOA em Qiskit e os scripts de análise serão disponibilizados em repositório público após a publicação do artigo.

Referências

ANATEL. (2024). Ato nº 16.417 — Conformidade cibernética de equipamentos de telecomunicações. Agência Nacional de Telecomunicações. Disponível em: https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2024/1972-ato-16417. Acesso em 18/03/26.

Bouchmal, O. et al. (2024). Quantum Approximate Optimization Algorithm for Routing Optimization in 6G Optical Networks. In: ONDM 2024, p. 1–6.

Cloudflare. (2025). State of the post-quantum Internet in 2025. Cloudflare Blog, outubro 2025. Disponível em: https://blog.cloudflare.com/pq-2025/. Acesso em 18/03/26.

Farhi, E., Goldstone, J. e Gutmann, S. (2014). A Quantum Approximate Optimization Algorithm. arXiv:1411.4028. Disponível em: https://arxiv.org/abs/1411.4028. Acesso em 18/03/26.

García-Herrero, J. et al. (2022). Multi-Objective Routing Optimization for 6G Using QAOA. Sensors, v. 22, n. 19, 7570.

ITI. (2026). Adoção de algoritmos pós-quânticos na ICP-Brasil. Convergência Digital.

Mosca, M. (2018). Cybersecurity in an era with quantum computers. IEEE Security & Privacy, v. 16, n. 5, p. 38–41.

Paquin, C. et al. (2025). Layered Performance Analysis of TLS 1.3 Handshakes: Classical, Hybrid, and Pure Post-Quantum Key Exchange. arXiv:2603.11006. Disponível em: https://arxiv.org/abs/2603.11006. Acesso em 18/03/26.