Roteamento e Alocação de Comprimentos de Onda para Canais Quânticos: Uma Proposta de Formulação Linear

Karcius D. R. Assis[1], Joao Muchanga[1], Ange Njanda[1], William F. Giozza[2]

[1]Escola Politécnica – Universidade Federal da Bahia (UFBA), Salvador – BA – Brasil

[2]Faculdade de Tecnologia – Universidade de Brasília (UnB), Brasília – DF – Brasil

karcius.assis@ufba.br

Abstract. *This paper proposes an optimization model for Quantum Communication Infrastructures (QCI), aiming to minimize capital costs in terms of quantum channels. By employing Integer Linear Programming (ILP), the model optimizes resource allocation under routing and wavelength assignment constraints for quantum channels. Simulations conducted in the AMPL/CPLEX environment demonstrate the relationship between secret key demands, quantum channels, and wavelengths.*

Resumo. *Este artigo propõe um modelo de otimização para Infraestruturas de Comunicação Quântica (QCI), visando minimizar os custos em termos de canais quânticos. Utilizando Programação Linear Inteira (ILP), o modelo otimiza a alocação de recursos sob restrições de roteamento e alocação de comprimentos de onda. Simulações realizadas no ambiente AMPL/CPLEX demonstram a relação entre demandas de chaves secretas, canais quânticos e comprimentos de onda.*

1. Introdução

Um dos principais problemas no planejamento de redes quânticas é que a taxa de chave secreta dos protocolos de distribuição de chaves quânticas (*Quantum Key Distribution* - QKD) diminui exponencialmente com a distância devido à menor quantidade de fótons que chegam ao detector, e quando a perda de fótons é alta, a relação sinal-ruído (SNR) cai, tornando a troca de chaves inviável ou insegura [Patel et al. 2012], [Wenning et al. 2023].

Para atender à elevada demanda por chaves secretas em redes de QKD, que pode superar a capacidade de um único canal quântico, uma possível solução é implementar múltiplos canais quânticos entre os nós (fonte e destino). Isso eleva a oferta de chaves seguras.

Neste artigo, utilizamos a tecnologia de multiplexação por divisão de comprimento de onda (*Wavelength Division Multiplexing* - WDM), que possibilita que diversos canais quânticos compartilhem uma mesma fibra óptica através de comprimentos de onda distintos. Por exemplo, se um canal quântico em λ_1 gera 10 kbps de chaves secretas e a necessidade é de 50 kbps, cinco canais quânticos (λ_1, λ_2, λ_3, λ_4, λ_5) podem ser ativados para suprir essa demanda.

A esse respeito, a otimização dos recursos da rede é fundamental para tornar viável a implantação prática da Infraestrutura de Comunicação Quântica (*Quantum Communication Infrastructure* - QCI) [Maity et al. 2024]. Métodos que utilizam técnicas de

otimização, como a Programação Linear Inteira (*Integer Linear Programming* - ILP) [Maity et al. 2024, Wenning et al. 2023, Cao et al. 2019], têm-se mostrado eficazes para minimizar diferentes tipos de custo no planejamento de redes quânticas. Esses modelos possibilitam a consideração de aspectos da infraestrutura óptica, geralmente reduzindo os custos de capital sem afetar o desempenho da rede.

A formulação ILP para problemas de roteamento em geral (incluindo roteamento de qubits) pode ser abordada de duas formas principais: formulação por caminhos pré-definidos (path formulation) e formulação sem caminhos pré-definidos (node-link formulation). Essas abordagens diferem na forma como modelam a escolha dos caminhos e na complexidade da resolução de um determinado problema.

Na formulação por caminhos pré-definidos, um conjunto de caminhos viáveis entre a fonte e o destino é previamente gerado. A decisão do modelo envolve selecionar quais desses caminhos serão utilizados para o roteamento dos qubits. Essa abordagem reduz significativamente o número de variáveis de decisão, pois considera apenas os caminhos previamente definidos em vez de todas as possíveis combinações de enlaces. Além disso, permite uma estimativa direta dos percursos utilizados, facilitando a interpretação e a simulação do problema. Entretanto, sua principal limitação é a necessidade de definir previamente os caminhos, o que pode restringir a flexibilidade da solução e afetar sua qualidade, especialmente em redes com tráfego variável ou de grande escala.

Por outro lado, na formulação sem caminhos pré-definidos, o roteamento é modelado considerando os fluxos de qubits em cada enlace da rede, sem definir previamente quais caminhos serão utilizados. Nesse caso, a variável de decisão indica se um enlace específico faz parte da solução. Como consequência, não é possível prever antecipadamente qual será o caminho resultante, tornando o problema mais desafiador de resolver devido ao maior espaço de busca e ao aumento do número de restrições e variáveis. No entanto, essa abordagem oferece maior flexibilidade, permitindo encontrar soluções potencialmente melhores, especialmente em cenários onde as condições da rede podem variar.

Este trabalho apresenta uma abordagem para o planejamento e otimização de QCIs, utilizando uma formulação ILP sem caminhos pré-definidos, para minimizar o número de canais quânticos enquanto atende às demandas de QKD sob restrições de distância (mais especificamente número de $hops$) e números de comprimentos de onda disponíveis. Diferente de outros trabalhos, a formulação proposta é linear, o que torna possível resolver o problema em um tempo computacional razoável. Simulações realizadas no ambiente AMPL/CPLEX [IBM 2023] demonstram a eficiência do ILP em cenários com diferentes números de comprimentos de onda disponíveis. Os resultados obtidos destacam o impacto direto da variação de comprimentos de onda no custo de implantação, fornecendo subsídios fundamentais para o planejamento de QCIs que sejam, ao mesmo tempo, eficientes, viáveis economicamente e escaláveis.

2. Formulação do Problema

O objetivo do ILP proposto, sem caminhos pré-definidos, é implantar uma QCI com custo mínimo de quantidade de canais quânticos e atendendo às demandas de QKD. A definição dos parâmetros e variáveis, assim como a formulação matemática, é apresentada a seguir:

Tabela 1. Descrição dos Termos Utilizados na Formulação do Problema

Símbolo	Descrição
Parâmetros	
$G(N, E)$	Topologia física com N nós e E arcos.
F	Conjunto de todas as demandas ij de QKD.
V_{ij}	Taxa de chave secreta demandada (qubits) pela requisição ij pertencente a F.
k_h	Taxa de chave secreta para demandas de h $hops$ de um conjunto H, ou seja, $h \in H$.
C	Conjunto de comprimentos de onda λ disponíveis, $\lambda \in$ C.
d_h	Número máximo de $hops$ permitidos para elementos do conjunto H.
χ	Um número grande.
Variáveis	
ρ_{ij}^h	Variável binária indicando se um canal quântico ij usa taxa para h $hops$.
$q_{ij,\lambda}$	Variável binária indicando se demmanda ij usa o comprimento de onda λ.
$Q_{mn,\lambda}^{ij}$	Variável binária indicando se o canal quântico ij em λ passa pelo link m-n.
N_{ij}	Nº de canais quânticos necessários para atender V_{ij}.

2.1. Modelo ILP

Objetivo

A função objetivo visa minimizar o número total de canais quânticos no planejamento da rede quântica, referente à implantação da infraestrutura.

$$Minimizar \sum_{ij} N_{ij}, \tag{1}$$

Restrições:

– **Roteamento e Alocação de Comprimentos de Onda para QKD:**

Restrição (2) garante que os fluxos de dados de QKD, qubits, sejam balanceados entre a fonte i e o destino j. A quantidade de canais quânticos necessários (cada qual em um comprimento de onda) é dado pela equação (3).

$$\sum_n Q_{mn,\lambda}^{ij} - \sum_n Q_{nm,\lambda}^{ij} = \begin{cases} q_{ij,\lambda} & m = i \\ -q_{ij,\lambda} & m = j \\ 0 & m \neq i, j \end{cases} \quad \forall ij \in F, m \in N, \lambda \in C \tag{2}$$

$$\sum_\lambda q_{ij,\lambda} = N_{ij} \qquad \forall ij \in F \tag{3}$$

Restrição (4) garante unicidade de comprimento de onda para cada demanda no canal quântico ij.

$$\sum_{ij} Q_{mn,\lambda}^{ij} \leq 1 \qquad \forall mn \in E, \lambda \in C \tag{4}$$

Restrição (5) limita a viabilidade do planejamento de acordo com o número de comprimentos de onda disponíveis para atender todas as demandas QKD.

$$\sum_{ij,\lambda} Q_{mn,\lambda}^{ij} \leq |C| \qquad \forall mn \in E \tag{5}$$

– **Quantidades de Módulos QKD (canais quânticos):**

As restrições de (6) a (11) determinam a quantidade de canais quânticos necessários para a equação (3). Isso deve estar em conformidade com a taxa de chave secreta disponível para os h $hops$ da demanda ij através da restrição (12).

$$N_{ij} \geq \left(\frac{V_{ij}}{k_h}\right) - \left(1 - \rho_{ij}^h\right) \chi \qquad \forall ij \in F, h \in H \tag{6}$$

$$N_{ij} \leq \left(\frac{V_{ij}}{k_h}\right) + 1 + \left(1 - \rho_{ij}^h\right) \chi \quad \forall ij \in F, h \in H \tag{7}$$

$$N_{ij} \leq \chi \sum_h \rho_{ij}^h \qquad \forall ij \in F \tag{8}$$

$$\sum_h \rho_{ij}^h \leq 1 \qquad \forall ij \in F \tag{9}$$

$$\sum_h \rho_{ij}^h \leq \chi V_{ij} \qquad \forall ij \in F \tag{10}$$

$$\sum_h \rho_{ij}^h \geq \frac{V_{ij}}{\chi} \qquad \forall ij \in F \tag{11}$$

$$\sum_{mn} Q_{mn,\lambda}^{ij} \leq \sum_h d_h \rho_{ij}^h \qquad \forall ij \in F, \lambda \in C \tag{12}$$

Utilizando o ILP, o modelo busca minimizar a necessidade de links quânticos através de WDM, enquanto atende às restrições de roteamento e alocação de comprimentos de onda. Note que as restrições de (6) a (11) são gerais e poderiam servir para casos em que V_{ij} é uma variável. Elas foram inspiradas nas restrições de alcance para diferentes formatos de modulação em redes ópticas elásticas, conforme proposto em [Assis et al. 2019].

3. Simulações e Resultados

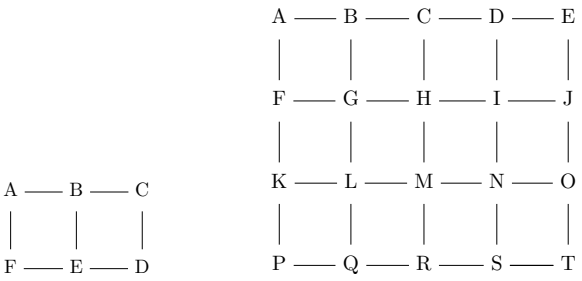
As simulações foram realizadas no ambiente de otimização AMPL [IBM 2023], com resolução utilizando o solver CPLEX [IBM 2023], devido à sua eficiência em resolver problemas ILP. Nós assumimos que há o protocolo BB84 [Bennett and Brassard 2014] para QKD, um dos protocolos mais amplamente estudados e implementados, devido à sua robustez e simplicidade em contextos práticos.

3.1. Configuração Inicial

Para simulação, foram utilizadas duas redes, uma de 6 nós (Figura 1a) e outra de 20 nós (Figura 1b). Ambas consistindo de enlaces de fibras interconectados e nós equipados com multiplexadores de comprimentos de onda. A simulação é caracterizada pelas seguintes propriedades específicas:

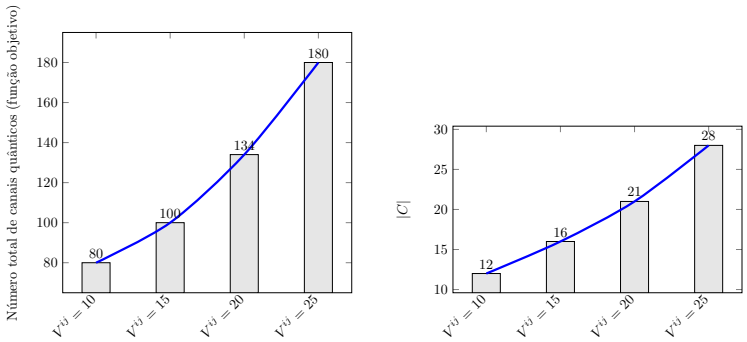
- **Requisitos de Distribuição de Chaves-Rede de 6 nós**: Canais de comunicação seguros são estabelecidos usando demandas QKD, com taxas de chave de V_{ij} = 10, 15, 20 ou 25 kb/s entre todos os pares de nós.
- **Requisitos de Distribuição de Chaves-Rede de 20 nós**: Canais de comunicação seguros são estabelecidos usando demandas QKD, com taxas de chave de V_{ij} = 10, 15, 20 ou 25 kb/s entre 20 pares de nós, escolhidos aleatoriamente.
- **Outros Parâmetros de Simulações para Ambas as Redes**: A máxima taxa de chaves suportada dependerá do número de $hops$ realizados por cada demanda na otimização e será: k_h = 8Kb/s para h=1 (1 salto), k_h = 4Kb/s para h=2 (2 $hops$), k_h = 2.7 Kb/s para h=3 (3 $hops$) e k_h = 2Kb/s para $h \geq 4$ (4 ou mais $hops$).

Para a rede de 6 nós, a Figura 2a demonstra uma tendência crescente no número de links quânticos N_{ij} à medida que o tráfego V_{ij} aumenta. Para valores baixos de V_{ij}, o número de links cresce de forma relativamente lenta, mas a partir de V_{ij}=20 kbps, a taxa de crescimento se acelera.



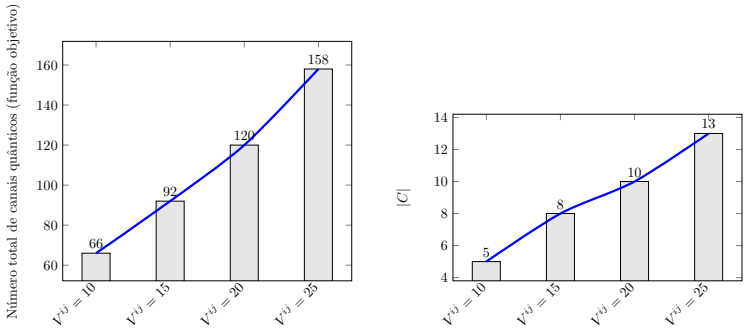
(a) Rede de 6 nós (b) Rede de 20 nós

Figura 1. Topologias físicas utilizada para simulação



(a) Número total de canais quânticos em função das requisições QKD (b) Quantidade de comprimentos de onda necessários em função das requisições QKD

Figura 2. (Rede de 6 nós) QCI obtida com diferentes requisições de QKD, os V_{ij} são para todos os pares ij de uma matriz de tráfego com [(NxN) - N)] elementos da Figura 1a, ou seja (6x6)-6=30 demandas ij



(a) Número total de canais quânticos em função das requisições QKD (b) Quantidade de comprimentos de onda necessários em função das requisições QKD

Figura 3. (Rede de 20 nós) QCI obtida com diferentes requisições de QKD, os V_{ij} são para todos 20 pares ij da matriz de tráfego, elementos da Figura 1b, escolhidos aleatoriamente, ou seja 20 demandas ij.

Essa relação pode ser explicada pela necessidade de atender a um volume crescente de requisições de QKD. Com o aumento da demanda, mais canais quânticos precisam ser estabelecidos, pois cada canal tem uma capacidade limitada de transmissão

segura. Também, observa-se que o crescimento não é linear, indicando que, em determinados pontos, a infraestrutura atinge um limite crítico onde a quantidade de links adicionais cresce de forma mais acentuada. A curva sugere um comportamento de saturação, onde a adição de novos links pode tornar-se ineficiente.

A Figura 2b mostra que o número de comprimentos de onda $|C|$ necessários também cresce com V_{ij}, mas de forma mais suave em comparação à Figura 2a. Isso sugere que a multiplexação por comprimento de onda melhora a eficiência da rede, reduzindo a necessidade de criar novos links físicos. Para elementos com demandas QKD igual V_{ij}=10 kbps, poucos comprimentos de onda são necessários (cerca de 12), pois há baixa concorrência nos canais. À medida que V_{ij} aumenta, a necessidade de mais comprimentos de onda cresce de maneira aproximadamente linear. Para V_{ij} =25 kbps, a infraestrutura atinge uma zona onde o número necessário de comprimentos de onda se aproxima de um limite superior, o que sugere uma possível saturação da multiplexação. Isso evidencia que o uso eficiente dos comprimentos de onda pode reduzir significativamente os custos de infraestrutura, pois permite atender mais demandas sem a necessidade de instalar novos links físicos.

A Figura 3 apresenta os resultados das simulações para a rede de 20 nós. Em relação aos resultados da rede de 6 nós, percebe-se que, na rede de 20 nós, o crescimento no número de canais quânticos (Figura 3a) é mais destacado, enquanto o crescimento na necessidade de comprimentos de onda (Figura 3b) é mais gradual. Isso sugere que, em redes maiores, a multiplexação por comprimento de onda tem um impacto mais significativo na eficiência do uso da infraestrutura.

4. Conclusão

Os resultados indicam que a alocação eficiente de comprimentos de onda pode reduzir significativamente os custos de infraestrutura ao minimizar o número de canais quânticos e considerar as características de distância. A otimização via ILP utilizada no estudo permitiu avaliar a requisição de chaves para diferentes configurações de distância, fornecendo observações valiosas para o planejamento de QCIs. A análise sugere que redes futuras devem focar na otimização de multiplexação espectral antes de expandir a infraestrutura física, garantindo escalabilidade e eficiência econômica. Devido à limitação de espaço, não são apresentadas simulações para redes de grande dimensão.

Referências

Assis, K. D., Almeida Jr, R., Waldman, H., Santos, A., Alencar, M. S., Reed, M. J., Hammad, A., and Simeonidou, D. (2019). Sla formulation for squeezed protection in elastic optical networks considering the modulation format. *Journal of optical communications and networking*, 11(5):202–212.

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11.

Cao, Y., Zhao, Y., Wang, J., Yu, X., Ma, Z., and Zhang, J. (2019). Cost-efficient quantum key distribution (qkd) over wdm networks. *Journal of Optical Communications and Networking*, 11(6):285–298.

IBM (2023). *IBM ILOG CPLEX Optimization Studio*. IBM Corporation.

Maity, I., ur Rehman, J., and Chatzinotas, S. (2024). Taqnet: Traffic-aware minimum-cost quantum communication network planning. *IEEE Transactions on Quantum Engineering*.

Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., and Shields, A. J. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2:041010.

Wenning, M., Samonaki, M., Patri, S. K., Fehenberger, T., and Mas-Machuca, C. (2023). Multi-layer optimization for qkd and key management networks. *Journal of Optical Communications and Networking*, 15(11):938–947.