Particionamento Não-Uniforme de Tráfego Sensível à Vulnerabilidade em Redes QKD

Fernanda G. S. Ribeiro[1], **Raul C. Almeida Jr**[2], **Karcius D. R. Assis**[1,3]

[1] Universidade Federal da Bahia (UFBA), Salvador–BA, Brasil
[2] Universidade Federal de Pernambuco (UFPE), Recife–PE, Brasil
[3] QuIIN - Quantum Industrial Innovation, EMBRAPII CIMATEC, Salvador–BA, Brasil.

karcius.assis@ufba.br

Resumo. *Redes quânticas com nós confiáveis permitem ampliar o alcance da taxa de geração de chaves, porém aumentam a extensão de ataque decorrente do possível comprometimento de nós intermediários. Em cenários multipath, a distribuição da demanda por múltiplos caminhos disjuntos melhora a robustez da comunicação, mas o particionamento uniforme do tráfego pode ser subótimo quando os diferentes caminhos apresentam graus distintos de vulnerabilidade. Neste artigo, propomos uma formulação matemática compacta para o particionamento não-uniforme do tráfego de taxa de chaves, que minimiza a exposição esperada, impondo simultaneamente um limiar de vulnerabilidade para restringir a concentração de tráfego em subconjuntos de caminhos. Os resultados obtidos evidenciam que a formulação proposta promove uma redução sistemática da exposição do tráfego de chaves em comparação com o particionamento uniforme.*

1. Introdução

A Distribuição Quântica de Chaves (*Quantum Key Distribution*, QKD) viabiliza a troca de chaves criptográficas com elevados requisitos de segurança da informação. Contudo, a implementação de redes QKD em larga escala demanda decisões de roteamento e alocação de recursos que afetam diretamente a *exposição* do tráfego da chave ao longo da infraestrutura [Bennett and Brassard 2014, Mehic et al. 2020, Ahmadian et al. 2025].

Em arquiteturas baseadas em nós confiáveis (*Trusted Nodes*, TNs), grandes distâncias são particionadas em múltiplos enlaces elementares; entretanto, cada TN se torna um ponto adicional de vulnerabilidade potencial, o que aumenta o risco de comprometimento parcial e de interceptação de frações do tráfego da chave.

Abordagens *multipath* particionam a demanda por múltiplos caminhos disjuntos, exigindo que um ”espião”comprometa todos os caminhos para, com base nessas informações, identificar e reconstruir a chave final [Ahmadian et al. 2025].

Apesar dessa necessidade de obter informações de todos os caminhos, mesmo uma interceptação parcial pode reduzir as margens práticas de segurança, especialmente se grandes frações de tráfego ficarem concentradas em subconjuntos de caminhos mais vulneráveis. Uma prática recorrente é dividir o tráfego igualmente entre caminhos disjuntos; porém, em redes com heterogeneidade de tamanhos de enlace, quantidade de TNs e probabilidades de comprometimento, essa divisão pode aumentar a exposição esperada do tráfego. Neste artigo, nossas principais contribuições/propostas são:

*Autor de correspondência: karcius.assis@ufba.br

(a) Definição de um modelo probabilístico de exposição de tráfego por caminho a partir do comprometimento de TNs ao longo de enlaces;
(b) Uma formulação via Programação Linear Inteira Mista (*Mixed Integer Linear Programming,* MILP) compacta para particionamento não-uniforme que minimiza a exposição esperada;
(c) Inclusão de um *limiar de vulnerabilidade* para limitar a concentração de tráfego em subconjuntos de caminhos;
(d) Avaliação em cenários didáticos e realísticos, comparando os particionamentos uniforme e não-uniforme.

2. Trabalhos Relacionados

A distribuição de chaves quânticas em redes ópticas evoluiu de enlaces ponto a ponto para arquiteturas que incorporam nós de confiança (TNs) e integração à infraestruturas WDM, trazendo consigo desafios de coexistência entre sinais quânticos e clássicos, bem como de planejamento de rede [Patel et al. 2012, Geng et al. 2021, Kong et al. 2023]. Abordagens de QKD multipercurso (multipath) têm sido investigadas visando aumentar a robustez e a segurança, recorrendo a tráfego particionado com combinações por concatenação ou operações bit a bit, com avaliação de desempenho por meio de indicadores-chave (KPIs), como probabilidade de bloqueio, confiabilidade, entre outros.

Todavia, a maior parte da literatura analisa estratégias de particionamento pré-definidas (por exemplo, divisão uniforme) e não aborda explicitamente a otimização do particionamento sob uma métrica formal de exposição de tráfego que leve em conta a heterogeneidade de vulnerabilidade dos caminhos [Ahmadian et al. 2025, Assis et al. 2026]. Este trabalho concentra-se na modelagem probabilística da exposição do tráfego pelos caminhos e sugestões de otimização do particionamento multipercurso sob restrições de vulnerabilidade da exposição.

3. Modelo de Vulnerabilidade e Exposição

Seja um grafo $G = (V, E)$. Considere um conjunto de demandas D, e para cada demanda $d \in D$ um conjunto P_d de caminhos candidatos *link-disjuntos* entre origem e destino (obtidos por pré-processamento). A demanda nominal é h_d (p.ex., taxa de chave secreta requerida). Seja $X_{d,p}$ a variável de decisão principal, em que $X_{d,p} \geq 0$ representa o tráfego (fragmento de chave) alocado no caminho $p \in P_d$. Dessa forma, a partição deve satisfazer as seguintes restrições:

- **Restrição de fluxo:**

$$\sum_{p \in P_d} X_{d,p} = h_d \qquad \forall d \in D. \tag{1}$$

A soma dos tráfegos nas partições é igual a demanda nominal.

- **TNs por enlace e probabilidade de comprometimento:**

Para cada enlace $e \in E$, com comprimento físico dist_e, assume-se um alcance máximo $D_{\max}$ sem TN. O número de TNs ao longo de e é aproximado por:

$$T_e = \left\lceil \frac{dist_e}{D_{\max}} \right\rceil - 1 \qquad \forall e \in E. \tag{2}$$

Se P_e é a probabilidade de um TN ser comprometido, então a probabilidade de o enlace e estar comprometido por pelo menos um TN ao longo dele é:

$$A_e = 1 - (1 - P_e)^{T_e} \qquad \forall e \in E. \tag{3}$$

- **Segurança por caminho e exposição:**

Para cada demanda d e caminho p, seja $\delta_{e,p}^d \in \{0, 1\}$ o indicador de que o enlace e pertence ao caminho p. Assumindo independência entre enlaces, a probabilidade do caminho não ser comprometido (segurança do caminho) é:

$$PS_{d,p} = \prod_{e \in E} (1 - A_e \, \delta_{e,p}^d) \qquad \forall d \in D, \forall p \in P_d. \tag{4}$$

Logo, definimos a exposição do caminho como:

$$ES_{d,p} = 1 - PS_{d,p} \qquad \forall d \in D, \forall p \in P_d. \tag{5}$$

Na prática, o valor de $ES_{d,p}$ pode ser previamente computado a partir de $dist_e$, $D_{\max}$, P_e e do conjunto de caminhos candidatos.

- **Exposição esperada**

Portanto, adota-se a função objetivo ϕ abaixo para minimizar o volume de tráfego potencialmente exposto à espionagem. Considerando as propriedades estatísticas da distribuição de Bernoulli, escrevemos o valor médio de tráfego espionado para P_d caminhos e D demandas como:

$$min \sum_{d \in \mathcal{D}} \sum_{\substack{S \subseteq \{1,\ldots,P_d\} \\ S \neq \emptyset}} \left[\left(\prod_{p \in S} ES_{d,p} \right) \left(\prod_{q \in \{1,\ldots,P_d\} \setminus S} (1 - ES_{d,q}) \right) \cdot \left(\sum_{p \in S} X_{d,p} \right) \right] \tag{6}$$

Para qualquer P_d, pode-se expressar a formulação como a soma sobre todos os subconjuntos não vazios $S \subseteq \{1, \ldots, P_d\}$.

3.1. Limiar de vulnerabilidade (concentração controlada)

Conforme explicitado anteriormente, mesmo sem reconstrução total da chave, a interceptação de frações grandes pode ser indesejável e indicar perigo iminente. Logo, introduzimos um limiar $\gamma \in (0, 1]$ que limita a fração de tráfego que pode ficar concentrada em subconjuntos de caminhos. Para manter o modelo compacto, adotamos a restrição por pares (adequada ao caso típico $|P_d| = 3$):

$$X_{d,p_i} + X_{d,p_j} \leq \gamma \, h_d \qquad \forall d \in D, \; \forall p_i \neq p_j \in P_d. \tag{7}$$

Esta restrição indica que nenhum par de caminhos pode carregar mais do que γh_d, evitando que a maior parte do tráfego fique concentrada em apenas dois caminhos (o que aumenta a exposição parcial sob cenários de comprometimento parcial).

4. Avaliação Numérica

Para realizar uma validação inicial da formulação MILP proposta, conduzimos um conjunto de experimentos numéricos empregando uma topologia simplificada constituída por três caminhos disjuntos para um único par origem–destino e, posteriormente, uma rede maior com 11 nós. O problema de otimização foi modelado e resolvido utilizando o solver IBM ILOG CPLEX [Nickel et al. 2020], assegurando a obtenção de soluções ótimas para cada cenário analisado.

4.1. Cenário didático (3 caminhos disjuntos)

Considere uma demanda de tráfego $h = 100$ kbps e três caminhos com exposições distintas (por exemplo, decorrentes de diferentes quantidades de TNs), conforme ilustrado na Figura 1. Assumindo uma $P_e = 0{,}1$, obtêm-se $ES_{d,1} = 0{,}10$, $ES_{d,2} = 0{,}19$, $ES_{d,3} = 0{,}47$ e $\gamma = 0{,}8$. A divisão uniforme $(33.3, 33.3, 33.3)$ gera exposição esperada: $\phi_{eq} \approx 0.10 \cdot 33.3 + 0.19 \cdot 33.3 + 0.47 \cdot 33.3 \approx 25.3$. Já a formulação proposta tende a concentrar mais tráfego em caminhos menos expostos, respeitando (7). Para esse exemplo, uma solução com particionamento desigual seria $(60, 20, 20)$, com $\phi_{opt} = 0.10{\cdot}60 + 0.19{\cdot}20 + 0.47{\cdot}20 = 19.2$, reduzindo a exposição esperada em relação a partição uniforme.

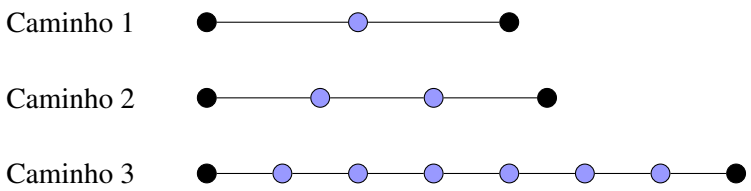

Figura 1. Exemplo de QKD com partição multipath com diferentes números de trusted nodes (azul). Os nós pretos representam a origem e o destino.

Tabela 1. Exemplo didático com $h = 100$ kbps, $|P| = 3$, $\gamma = 0.8$.

Partição	$X_{d,1}$	$X_{d,2}$	$X_{d,3}$	ϕ
Uniforme	33.3	33.3	33.3	≈ 25.3
Otimizada (MILP)	60	20	20	19.2

4.2. Topologia Pan-Europeia (11 nós)

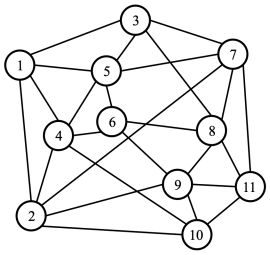

Figura 2. Topologia Pan-Europeia.

Para avaliar o comportamento em rede, pode-se usar a topologia Pan-Europeia [Wosinska et al. 2009], apresentada na Figura 2, e gerar, para cada par origem–destino,

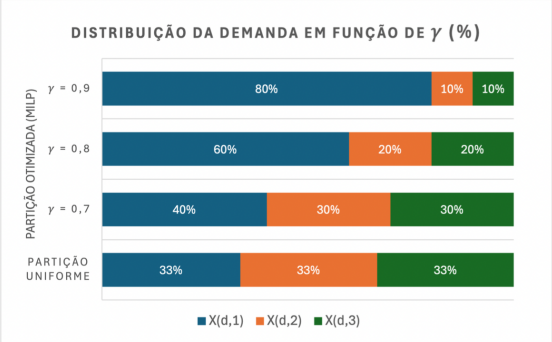

Figura 3. Distribuição da Demanda

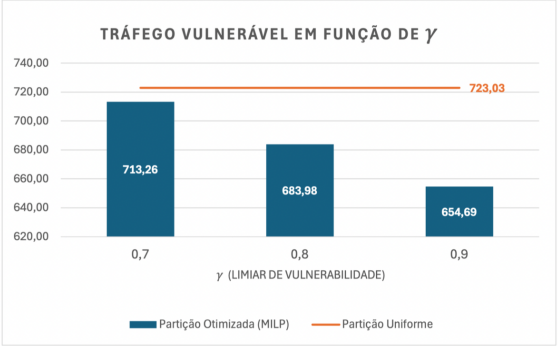

Figura 4. Tráfego vulnerável em função de γ

três caminhos link-disjuntos pré-computados (p.ex., via extrações sequenciais de caminhos mínimos). Como os caminhos resultam em diferentes números de enlaces/TNs, $ES_{d,p}$ torna-se heterogêneo por demanda, e o objetivo (6) favorece automaticamente os caminhos menos expostos. Em geral, observa-se padrão recorrente de alocação com maior peso no caminho de menor exposição (por exemplo, $(60, 20, 20)$ em diversas demandas com heterogeneidade moderada), reduzindo ϕ frente ao particionamento uniforme. Para avaliação númerica baseada na topologia Pan-Europeia, foram consideradas 10 demandas, cada uma associada a três caminhos *link-disjuntos*. O parâmetro D_{max} foi fixado em 80 km, valor de referência presente na literatura para o alcance máximo de sinais quânticos sem a necessidade de regeneração [Cao et al. 2019]. Variou-se o γ para explorar como a partição otimizada, com o estabelecimento de uma fração máxima admissível de tráfego passível de exposição, impacta na distribuição das demandas e na exposição da rede.

A Figura 3 apresenta a distribuição da demanda entre os links disjuntos em porcentagem. Observa-se que, à medida que o valor de γ aumenta, o modelo MILP tende a concentrar uma fração maior do tráfego no caminho de menor exposição (aquele com o menor número de *Trusted Nodes*). Isso ocorre porque, com um γ maior, permite-se que uma maior parcela do tráfego seja concentrada, possibilitando que o *solver* priorize a rota estatisticamente mais segura. Em contraste, quando o valor de γ é reduzido, a solução converge para um comportamento similar ao do particionamento uniforme, no qual a demanda é dividida igualmente entre os caminhos, ignorando a heterogeneidade das vulnerabilidades físicas de cada rota.

A Figura 4 ilustra a comparação do tráfego vulnerável total (ϕ) em função de γ frente à partição uniforme ($\phi \approx 723,03$). Os resultados demonstram que o aumento de γ permite uma redução sistemática na exposição das chaves. Enquanto o particionamento uniforme apresenta uma exposição elevada, por não distinguir a vulnerabilidade dos caminhos, o modelo proposto utiliza da heterogeneidade para priorizar as rotas com menor número de trusted nodes, concentrando a maior parte da demanda em caminhos estatisticamente mais seguros e reduzindo o risco de interceptação.

5. Conclusão

Apresentamos uma formulação compacta para particionamento multipath não-uniforme em redes QKD com nós confiáveis, focada exclusivamente em vulnerabilidade/exposição. O modelo minimiza a exposição esperada ponderando o tráfego pela exposição por caminho,

e impõe um limiar para limitar a concentração de fragmentos em subconjuntos de caminhos. Resultados ilustrativos mostram redução consistente de exposição em comparação à divisão uniforme, explorando heterogeneidade de risco entre caminhos. Uma extensão natural para esse trabalho é integrar o particionamento a decisões de roteamento e/ou alocação espectral.

Agradecimentos

Os autores agradecem ao PIBIC/CNPq pelo suporte financeiro a este trabalho.

Referências

Ahmadian, M., Arpanaei, F., Carlos Hernandez-Hernandez, J., Lin, R., and Monti, P. (2025). Enhancing the reliability of multipath qkd over multi-band systems. *Journal of Optical Communications and Networking*, 17(12):1105–1116.

Assis, K. D. R., Almeida Jr., R. C., et al. (2026). Security-aware non-uniform multipath traffic partitioning for qkd networks: a milp-based vulnerability minimization approach. Manuscript submitted to Optical Fiber Technology, Elsevier.

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.

Geng, J.-Q., Fan-Yuan, G.-J., Wang, S., Zhang, Q.-F., Hu, Y.-Y., Chen, W., Yin, Z.-Q., He, D.-Y., Guo, G.-C., and Han, Z.-F. (2021). Coexistence of quantum key distribution and optical transport network based on standard single-mode fiber at high launch power. *Optics Letters*, 46(11):2573–2576.

Kong, W., Sun, Y., Gao, Y., and Ji, Y. (2023). Coexistence of quantum key distribution and optical communication with amplifiers over multicore fiber. *Nanophotonics*, 12(11):1979–1994.

Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., Schauer, S., Poppe, A., Pacher, C., et al. (2020). Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, 53(5):1–41.

Nickel, S., Steinhardt, C., Schlenker, H., Burkart, W., and Reuter-Oppermann, M. (2020). Ibm ilog cplex optimization studio. In *Angewandte Optimierung mit IBM ILOG CPLEX Optimization Studio: Modellierung von Planungs-und Entscheidungsproblemen des Operations Research mit OPL*, pages 9–23. Springer.

Patel, K., Dynes, J., Choi, I., Sharpe, A., Dixon, A., Yuan, Z., Penty, R., and Shields, A. (2012). Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2(4):041010.

Wosinska, L., Jirattigalachote, A., Monti, P., Tzanakaki, A., and Katrinis, K. (2009). Light-path routing considering differentiated physical layer constraints in transparent wdm networks. In *2009 Asia Communications and Photonics conference and Exhibition (ACP)*, volume 2009, pages 1–8. IEEE.