Key Rate Partitioning for Enhanced Security in QKD-over-WDM Networks

F. G. S. Ribeiro, K. D. R. Assis, R. C. Almeida Jr, C. M. S. do Nascimento, M Gil de Oliveira and V. L. da Silva

***Abstract*— Quantum key distribution (QKD) offers a secure communication paradigm based on the principles of quantum physics, but its deployment is constrained by photon losses, distance limitations, and vulnerabilities in trusted nodes. This paper shows a Linear Programming-based model for QKD-over-WDM networks that jointly considers routing, wavelength assignment, and trusted-node placement. Two strategies are analyzed: single-path allocation, which minimizes resource usage, and partitioned disjoint routing, which distributes secret keys across multiple paths. Results show that while single-path solutions can be cost-efficient, partitioning enhances significantly strengthens security, as an eavesdropper would need to compromise several independent key streams simultaneously.**

***Keywords*— Quantum Networks, Optical Networks, Optimization.**

I. Introduction

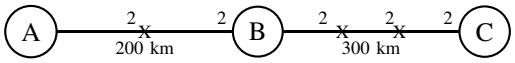
This paper explains a mathematical model for quantum networks that addresses a basic formulation by focussing on the joint optimisation of routing, trusted node placement, and QKD [1], [2]. The model utilises a mixed integer linear programming (MILP) approach, which effectively captures the initial idea of routing in quantum networks. However, we proposed a new strategy for partitioning the rate of keys of a request.

Specifically, the MILP model (reproduced and inspired by [2]) incorporates the partitioning of secret-key demands across multiple disjoint paths. Beyond minimizing deployment costs and satisfying planning constraints, this partitioning strategy enhances security, forcing a potential eavesdropper to compromise several independent streams simultaneously in order to retrieve the protected information.

II. Statement Problem

In WDM backbone networks, classical channels will use an erbium-doped fiber amplifier (EDFA) to enable optical signals to propagate through the optical fiber over a long distance. EDFAs are deployed approximately every 80 km on fiber links. In order to enable quantum and classical channels to coexist in the same fiber, an EDFA bypass scheme can be adopted for QKD integration in WDM backbone networks, as shown in [2]. The EDFA bypass scheme allows quantum channels to bypass the EDFA by using special multiplexer (MUX) and demultiplexer (DEMUX) components to separate quantum and classical channels, which is beneficial to suppress the noise that results from the EDFA's amplified spontaneous emission (ASE) [2].

F. G. S. Ribeiro and K. D. R. Assis are with UFBA, Salvador-BA, Brazil. R. C. Almeida Jr is with UFPE, Recife-PE, Brazil. C. M. S. do Nascimento, M Gil de Oliveira and V. L. da Silva are with QuIIN-Quantum Industrial Innovation, EMBRAPII CIMATEC, Salvador, BA, Brazil. E-mail:karcius.assis@ufba.br



$r^k = 100\ kbps$, $k = 1$, ($D_{max} = 100\ km$, $SKR = 50\ kbps$)
X=trusted node, transceivers=2x5=10.

Fig. 1. Example of strategy

In the optical layer, optical cross-connects (OXCs) are interconnected by optical links. EDFAs are deployed on optical links to enable optical signals to propagate a long distance. In the QKD layer, QKD nodes are interconnected by QKD links (i.e., quantum channels). TRNs (trusted nodes) are deployed on QKD links to enable long-distance QKD. For all the incoming QKD requests from multiple distant QKD users, each QKD node acts as an end node, and each TRN acts as an intermediate node. QKD nodes in the QKD layer are co-located with OXCs in the optical layer. Moreover, optical links can use the produced secret keys on QKD links to enhance optical layer security.

In this paper, we use WDM technology, which allows multiple quantum channels to share the same optical fibre using different wavelengths. Figure 1 illustrates a network that includes three QKD nodes (A, B, and C) that are 200 km and 300 km apart. The diagram specifies a request k=1 with a key rate r^k=100 kbps from A to C. It is assumed that a trusted node, named X, is inserted after a distance D, for which a generated Qubit rate may be especified. In this paper, we have assumed a secret key rate SKR = 50kbps for D=100km.

For 100 kbps transmission from A to C, two quantum channels (w_1, w_2) must operate between A and X to satisfy this demand, which requires two transceivers for the connection A-X (where a trusted node is mandatory, since the distance reached is already D = 100 km). A similar configuration is required between X and B, between B and the first X in the BC segment, between both X in BC, and between the second X in BC and C, each with two quantum channels.

In short, to satisfy the need for trusted nodes between A and C, one trusted node is needed between A and B, and two trusted nodes are necessary between B and C. A total of 10 transceivers are required between A and C to comply with all these specifications.

III. Methodology

In this section, we show the main idea inspired by the mathematical formulation of [2]. Let K be the number of QKD requests from a source node to a destination node. The

TABELA I

UNIT COST PARAMETERS, [2]

Parameter	Unit Cost (USD)	Unit / Meaning
C_1	\$40,000	per QKD transceiver
C_2	\$20,000	per TRN (trusted node)
C_3	\$8	per km × wavelength channel
C_4	\$30,000	per QKD node

network model is represented by a set V of vertices (nodes) and a set E of links. Let $dist_{ij}$ be the distance of the link (i, j) and Let D be the physical distance between two neighboring quantum nodes. SKR be the rate corresponding to the physical distance D and r^k be the secret-key rate of QKD request k.

The aim is to reduce the total expenditure of the QKD backbone (1). This includes four components: the cost of QKD transceivers across all QKD nodes ($C_1 N_{transc}$), the cost of additional QKD equipment for every TRN ($C_2 N_{trusted}$), the cost of the QKD links ($C_3 N_{opt}$), and the cost of additional QKD equipment for all QKD nodes ($C_4|V|$). The calculation of N_{transc}, $N_{trusted}$, and N_{opt} can be derived from the formulation presented in [2].

$$\min \quad C_1 N_{transc} + C_2 N_{trusted} + C_3 N_{opt} + C_4|V| \qquad (1)$$

IV. RESULTS AND DISCUSSION

This section outlines the environment employed to evaluate the MILP formulation from [2] with some adittional constraints. The MILP was solved with IBM ILOG CPLEX v.11.0, executed on an Intel i7 machine operating at 3.6 GHz and equipped with 32GB of RAM. The tests utilized the Hypothetical Brazilian Topology, depicted in Fig.2, which amalgamates optical and quantum communication capabilities.

To assess the efficiency of the MILP formulation, two different request configurations were considered: (i) a single end-to-end QKD request of r^k=100 kbps from node 1 to node 12 (K=1), and (ii) a partitioned QKD demand where two disjoint requests of 50 kbps were simultaneously established between node 1 and node 12 (K=2). SKR=50kbps and D=100km for both configurations. Table I shows the cost parameters.

A. Case K=1 with 100 kbps Request

The distribution of (trusted nodes/repeaters) required along the physical links is (1-2) = 7 trusted nodes, (2-3) = 4 trusted nodes, (3-8) = 16 trusted nodes and (8-12) = 14 trusted nodes. The results also reveal that to sustain a 100 kbps secret-key rate, two parallel channels are required per segment due to the SKR constraint of 50 kbps per link. Specifically, the direct path from node 1 to node 12 traverses segments that demand additional transceivers to respect the 100 km reach. Moreover, the number of quantum channels allocated increases in order to aggregate sufficient capacity, with two channels established per link. This confirms the necessity of wavelength multiplexing to scale the key distribution rate beyond the physical SKR limit of individual links.

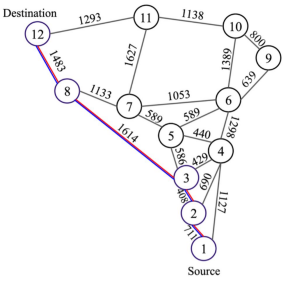


Fig. 2. Brazilian Network Topology with K=1

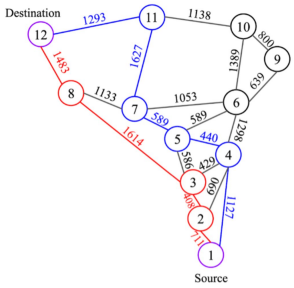


Fig. 3. Brazilian Network Topology with K=2

TABELA II

OBJECTIVE FUNCTION COST BREAKDOWN

Cost Component	K=1 (100 kbps)	K=2 (2 × 50 kbps)
$C_1 N_{transc}$	\$3,360,000	\$3,720,000
$C_2 N_{trusted}$	\$820,000	\$1,780,000
$C_3 N_{opt}$	\$67,136	\$74,176
$C_4\|V\|$	\$360,000	\$360,000
Total Cost	**\$4,607,140**	**\$5,934,180**

B. Case K=2 with Two Partitioned Requests

In this scenario the original 100 kbps key rate is split into two independent requests of 50 kbps each, both from node 1 to node 12. While this partitioning naturally avoids the need for wavelength (since each request can be supported within the SKR limitation of 50 kbps per link) it also introduces a security advantage. Specifically, by distributing the secret-key rate across two disjoint requests, the model increases the difficulty of a potential eavesdropper. Any adversary attempting to compromise the communication would need to intercept and reconstruct both independent keys, associated with the two requests, to obtain the full 100 kbps key rate. The distribution of trusted nodes is spread across different segments of the network, reflecting the link-disjoint routing enforced by the model. Importantly, this configuration strengthens the overall security posture, since an eavesdropper is required to compromise two independent paths and secret-key streams rather than a single aggregated channel.

V. CONCLUSION

Under the cost parameters of Table I and the result of the objective function in Table II, K = 1 is cost optimal for a 100 kbps request 1-12. On the other hand, K=2 provides robustness but increases CAPEX by 22.4%; whether this premium is acceptable depends on required security targets. As future work, the model can be extended to include multiple source–destination pairs and more dynamic traffic scenarios, offering deeper insights into the design of scalable and secure quantum communication infrastructures.

REFERÊNCIAS

[1] Assis, Karcius DR. "Infraestrutura Óptica para Comunicação Quântica: Planejamento e Otimização" *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*. SBC, 2025.

[2] CAO, Yuan et al. "Cost-efficient quantum key distribution (QKD) over WDM networks" *Journal of Optical Communications and Networking*, v. 11, n. 6, p. 285-298, 2019.