Optimization of Secure Quantum Key Distribution Backbones in Core Transport Networks

Federico Pederzolli, Marco Savi, Domenico Siracusa, Elio Salvadori

FBK CREATE-NET, Via alla Cascata, 56/D, 38123 Trento, Italy

{*fpederzolli, m.savi, dsiracusa, esalvadori*}*@fbk.eu*

Abstract: We present a Mixed Integer Linear Programming formulation to perform optimal placement of Quantum Key Distribution devices to protect active/planned traffic at minimal cost, thus securing active core transport networks.

OCIS codes: 060.4256, 270.5568.

1. Introduction and Problem Statement

Quantum Key Distribution (QKD) has, for many years, been the tip of the spear in the field of Quantum Communications, being the first and by far the most technologically ready application of Quantum technologies to telecommunication networks. In essence, QKD devices [1] and protocols exploit a number of "quirks" of quantum mechanics to achieve the continuous exchange of a random bit stream between two communicating parties, with an *arbitrarily low upper bound on the probability that an adversary eavesdropped the communication*, making it an ideal choice to generate key material for cryptography (especially session keys).

From the initial proposal of BB84 [2], through the overcoming of practical limitations (e.g. [3]), to the most promising recent advances towards real deployments and security guarantees [4], QKD is inching closer to becoming a viable security technology in both terrestrial and satellite [5] communications. Despite the security guarantees, several practical limitations still prevent the widespread adoption of QKD: (*i*) devices are strictly point-to-point (or rely on a central distributor), (*ii*) reach is limited to 120-150 Km (in fibers, twice if a central distributor is used, much greater for satellites but with intermittent service due to weather [5]), (*iii*) the key rate is low (in the order of Mb/s for state-of-the-art devices, at short distances) and decreases steadily with distance, (*iv*) QKD protocols do not support authentication, (*v*) the cost of devices is still high (but improving), and (*vi*) deployment requires highly qualified physicists. Irrespective of all these limitations, QKD-based products are finally close to commercial deployment in core transport networks [1], thus making the investigation of their optimal employment a relevant problem.

In this preliminary work we attempt to answer the following question: *if we were to deploy QKD in a terrestrial core transport network tomorrow, how would we do it?* That is, we want to optimize the use of costly QKD devices in a medium-large distance fiber network. Implied by this question are two important constraints: (*i*) we assume to rely on an existing fiber plant, utilizing one or more dark fibers/channels to implement QKD quantum channels, and (*ii*) we assume to use technology available today. To answer this, we firstly explain our assumptions regarding the technology stack we envision, then we present a Mixed Integer Linear Programming (MILP) formulation to compute the optimal (i.e., cheapest) placement of QKD devices given an existing fiber plant and traffic matrix (i.e., set of connections to be encrypted using the keys distributed using the QKD sub-network), and we analyze its behavior.

2. Technological Scenario and Assumptions

We assume to deal with existing or planned core (national/international, with links longer than the reach of QKD devices) optical networks, employing WDM or flexi-grid technology, and to have access to a map of deployed/planned optical connections to be secured via QKD. We consider BB84-style point-to-point QKD devices (already on the market); a daisy-chain of such devices is, in general, necessary to cross a long link (and multiple chains in parallel can be used to achieve greater key rates). Since devices process signals electronically, acting as *trusted relays* and storing intermediate keys securely as outlined in [6], a network of such QKD-secured links is by its nature opaque. As a consequence, QKD device placements in individual links can be independently optimized as shown in [7], balancing the cost of additional devices with the higher key rate of shorter QKD spans. We also consider the chance that an attacker may compromise one or more nodes, by ensuring that N node-disjoint QKD paths are available between each node couple (if the key is generated through all available paths, an attacker must compromise at least N nodes to retrieve it). Intuitively, if the key rate of a QKD chain exceeds that required to secure a connection, it may be preferable to route the QKD exchanges between distant nodes to utilize the capacity of QKD chains outside the shortest path between those nodes, rather than deploy more devices.

3. MILP Formulation for QKD Device Placement

Our formulation takes as input a graph $G = (V, E)$ representing the fiber plant, an integer N representing the desired path multiplicity, and functions $C : V \times V \to \mathbb{N}$, $Q : E \to \mathbb{N}$ and $D : E \to \mathbb{N}$ mapping each node couple to the key material bit-rate needed to secure the traffic flowing between them, the key rate of a locally-optimized QKD chain in an edge, and the number of devices needed to implement it, respectively. Q and D depend on the length of the links and the longest distance between QKD devices local to the link, while C encodes the current (or near-term) traffic of the core network.

The formulation contains three families of variables: (*i*) C_e: integer counting the number of parallel QKD chains deployed on edge e; (*ii*) S_e: continuous representing the number of selected QKD paths crossing edge e; (*iii*) $R^{u,v}_{s,d}$: binary representing whether edge $(u,v) \in E$ is used to generate keys between nodes s and d. The objective function is:

$$\min \sum_{e \in E} D(e) \cdot C_e \tag{1}$$

I.e., minimize the number of QKD chains, weighted by their length in terms of devices, and subject to constraints:

$$\forall e \in E \qquad C_e \geq 1/Q(e) \cdot S_e \tag{2}$$

$$\forall e \in E \qquad 1/Q(e) \cdot S_e - C_e \leq 1 - \varepsilon \tag{3}$$

$$\forall e \in E, e = (u,v) \qquad S_e = \sum_{(s,d) \in V \times V} R^{u,v}_{s,d} \cdot C(s,d)/N \tag{4}$$

$$\forall (s,d) \in V \times V, \forall v \in V \setminus \{s,d\} \qquad \sum_{u \in V} R^{u,v}_{s,d} = \sum_{u \in V} R^{v,u}_{s,d} \tag{5}$$

$$\forall (s,d) \in V \times V \qquad \sum_{u \in V} R^{u,d}_{s,d} \geq N \tag{6}$$

$$\forall (s,d) \in V \times V \qquad \sum_{v \in V} R^{s,v}_{s,d} \geq N \tag{7}$$

$$\forall (s,d) \in V \times V \qquad \sum_{v \in V} R^{d,v}_{s,d} = 0 \tag{8}$$

$$\forall (s,d) \in V \times V \qquad \sum_{u \in V} R^{u,s}_{s,d} = 0 \tag{9}$$

$$\forall (s,d) \in V \times V, \forall v \in V \setminus \{s,d\} \qquad \sum_{u \in V} R^{u,v}_{s,d} \leq 1 \tag{10}$$

$$\forall (s,d) \in V \times V, \forall u \in V \setminus \{s,d\} \qquad \sum_{v \in V} R^{u,v}_{s,d} \leq 1 \tag{11}$$

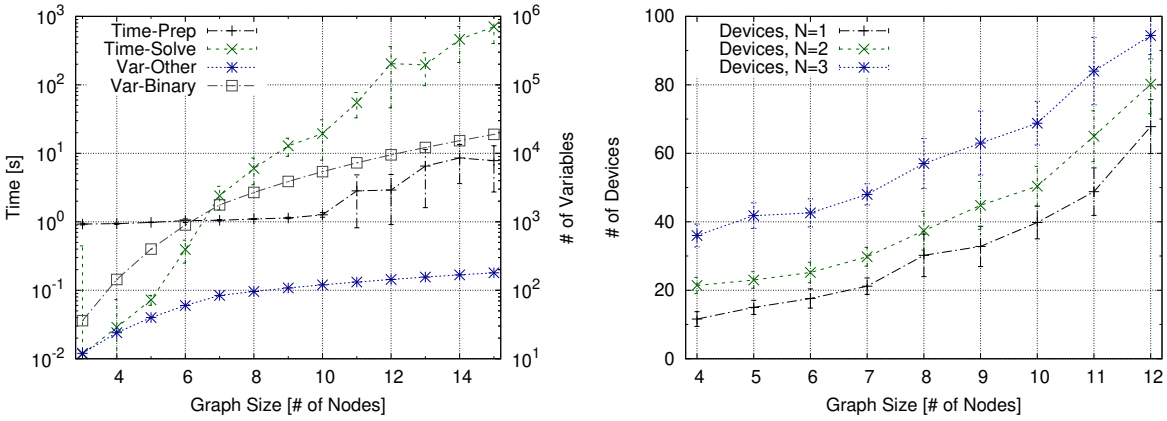
Constraints 2 and 3 (ε represents the usual arbitrarily small quantity) linearize the relation $C_e = \lceil 1/Q(e) \cdot S_e \rceil$, where $1/Q(e)$ represents the fraction of the key rate generated by a QKD chain on edge e consumed by an optical demand. Constraint 4 states that each S_e variable represents the sum of the required key bit-rates for all the (chosen) paths crossing edge e. Finally, constraints 5-11 implement routing: constraint 5 prevents black holes, constraints 6-7 enforce the selection of the required number of alternative paths (N), constraints 8-9 prevent looping past the source and destination nodes, and constraints 10-11 enforce the selection of node-disjoint paths.

In this formulation the size of the problem is dominated by the $R^{u,v}_{s,d}$ variables, which is upper bounded by $|V|^2 \cdot |E| \leq |V|^4$, a large but manageable number on modern hardware, especially since modern solvers like Gurobi [8], which we used to implement our formulation, can be configured to stop after a pre-defined time and report both the best current solution and its worst-case gap to the optimum. Once optimized, it is trivial to retrieve both how many QKD devices need to be installed in each link (i.e., $D(e) \cdot C_e$), and which paths were selected (to route the key material).

4. Behavior Analysis

We evaluated the results of our proposed MILP formulation both on random graphs and two real topologies from Germany [9] and Spain [10]. In order to study its behavior we firstly ran it on 10 randomly generated (using the Erdős-Rényi model and known seeds) graphs with a predefined number of nodes, $|E| = 3 \cdot |V|$ (complete graph for very small $|V|$), and edge lengths drawn uniformly from $[50, 350]$ Km. We assumed one QKD device pair every 80 Km (greater than the ~20 Km reported in [7], but closer to the distance preferred by operators due to the range of amplifiers), and that the key rate of each link can provide material for encrypting 10 optical connections. We also assumed a uniform traffic matrix between all nodes. All experiments were performed on a laptop equipped with a 2.60 GHz Intel i7-6600U CPU and 8 GB of RAM.

In Fig. 1a we report the average running time for the model setup (Time-Prep) and solver (Time-Solve), including standard deviation, for a path multiplicity of 2 as a function of the graph size, and also the model complexity in terms of variables (constant across all graphs of the same size, as they depend on the number of nodes and edges). The rather large variances in time are a consequence of the rather small sample size, but Fig. 1a clearly indicates a roughly exponential (note the log scale) solve time (the dominant contributor), which is in line with the expected complexity of solving a MILP problem (known to be NP-Hard). Fig. 1b shows instead the average ($\pm\sigma$) value of the objective



(a) (b)

Fig. 1: Average Time & Number of Variables (a), and Optimal Number of QKD devices (b) vs. graph size.

Topology	Nodes	Links	Avg. N. Deg.	Avg. Sh. Path Len.	Diam.	Sol. ($N = 2$)	Time
GER [9]	14	23	3.28571	2.34066	5	304	~40 s
SPA [10]	30	56	3.73333	3.30575	7	756 (gap 1.76%)	~3600 s*

Table 1: MILP Results for the German and Spanish topologies.

function vs. the graph size for a required path multiplicity (N) of 1, 2 and 3. Note how, by carefully placing QKD devices and routes, significant savings can be achieved when using path multiplicities greater than one for additional security and redundancy: the data points for $N = 2, 3$ are $\ll$ than twice/thrice (expected with a very naïve approach) those for $N = 1$. The results for the real topologies, under the same assumptions, can be found in Table 1. Note that for the Spanish topology the solver was interrupted after one hour and the worst-case gap to the optimal solution reported.

5. Conclusions & Future Works

We proposed a MILP formulation for finding the optimal (i.e., cheapest) placement of QKD devices to create a QKD backbone for securing an existing fiber plant (with existing or planned optical connections), with a desired level of path redundancy. We analyzed its behavior, showing that significant savings can be achieved in multipath scenarios.

There is still much to be done before QKD becomes a truly mature technology, on both the hardware and networking sides. With respect to the latter, we plan to extend this formulation to also cover the local optimization of links (to save resources on unloaded ones), investigate heuristics to tackle large networks in a shorter time, and tackle the problems of employing central QKD distributors and of co-designing the fiber plant and QKD sub-network.

References

1. ID Quantique, SK Telecom and Nokia press release, 2018. [online] Available at: https://marketing.idquantique.com/acton/attachment/11868/f-032a/1/-/-/-/-/IDQ-SKT-Nokia
2. C. H. Bennett and G. Brassard, "*Quantum cryptography: Public key distribution and coin tossing*," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.
3. Hoi-Kwong Lo, Xiongfeng Ma, Kai Chen, "*Decoy State Quantum Key Distribution*," Phys. Rev. Lett., June 2005, 10.1103/PhysRevLett.94.230504.
4. Hoi-Kwong Lo, Marcos Curty, Bing Qi, "*Measurement-Device-Independent Quantum Key Distribution*," Phys. Rev. Lett., March 2012, 10.1103/PhysRevLett.108.130503.
5. Sheng-Kai Liao et al., "*Satellite-to-ground quantum key distribution*," Nature, August 2017.
6. P. Schartner, S. Rass, M. Schaffer, "*Quantum Key Management*," in book: Applied Cryptography and Network Security, March 2012, 10.5772/35400.
7. R. Allaume, F. Roueff, E. Diamanti, N. Ltkenhaus, "*Topological optimization of quantum key distribution networks*," New Journal of Physics, 2009.
8. Gurobi Optimization, LLC, "*Gurobi Optimizer*," 2018. [online] Available at: https://www.gurobi.com
9. F. Agraz et al., "*Experimental demonstration of centralized and distributed impairment-aware control plane schemes for dynamic transparent optical networks*," in Proc. OFC, 2010.
10. F. Rambach et al., "*A Multilayer Cost Model for Metro/Core Networks*," J. Opt. Commun. Netw., 2013.