Cost Optimisation using Switching in Realistic Quantum Network Models

Vasileios Karavias[(1)], Andrew Lord[(2)], Mike Payne[(1)]

[(1)]University of Cambridge, Dept. of Physics, CB3 0HE, Cambridge, UK vk330@cam.ac.uk
[(2)] BT, Adastral Park, Martlesham Heath, IP5 3RE Ipswich, UK

Abstract *A paradigm for quantum network (QN) design involves using switching to share devices. This paper presents a node selection and detector placement strategy for switched QNs. Investigations show that switching is beneficial when the required key transmission rate in a graph is below a threshold.*

Introduction

There has been remarkable progress in quantum networks in recent years, both practically[1]–[5] and through theoretical optimisations[6]–[13] focusing on using mixed integer linear programs (MILPs) to investigate entanglement quantum networks (QNs)[6]–[8], to optimise the cost of trusted node QNs[9]–[11] and define metrics to assess their quality[12]. Work on investigating optimal building strategies in regular, symmetric QNs has also been carried out[14].

While switching has been investigated practically to combat denial of service attacks[15],[16] and implemented in small networks[17], there has been little focus on the cost reduction benefits. Switches can be used to share devices thus reducing the required number in the network.

In this paper, we consider two QN models, Trusted Node (TN) and Twin Field Quantum Key Distribution (TF-QKD) models[18], presented in the next section, and design MILPs to optimise the cost given a traffic requirement matrix. For each model, we use these MILPs to investigate the benefits of switching on network graphs including the BT Core Network graph[19].

Quantum Network Models

We first consider the TF-QKD model, described in[18]. Detectors are collocated on single nodes allowing the use of superconducting nanowire single photon detectors (SNSPDs) in QNs without incurring large cooling costs. Keys are generated using the asymmetric TF-QKD protocol[20],[21].

We also consider the TN model. Users are untrusted and connected via intermediate trusted nodes using the Decoy State BB84 protocol[22].

Figure 1 plots the capacities as a function of connection length for cold (SNSPDs) and warm detectors (SPADs) calculated using methods described in[18].

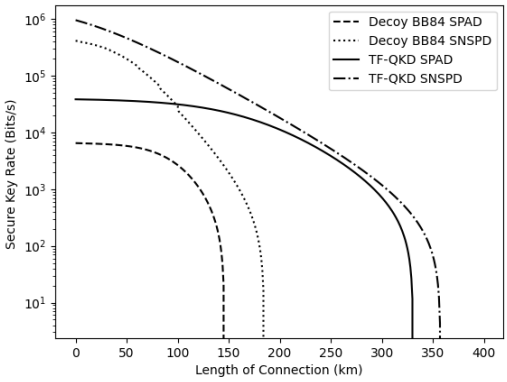

Fig. 1: Secure key rates used in the investigation. TF-QKD rates shown for symmetric setup.

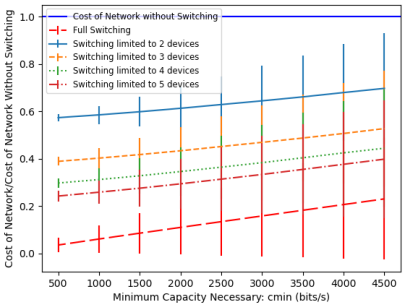

Fig. 2: Ratio of switched to not-switched graph cost against increasing key transmission requirement for TF-QKD model.

Methods

TF-QKD Model: We consider a network graph $G = (V, E)$, where vertices are separated into user nodes $S \subset V$ and potential detector sites $D \subset V$ for cooled (SNSPD) and uncooled (SPAD) detectors $m \in \{u, c\}$. We further assume the existence of a mapping of distances to capacities based on asymmetric TF-QKD[21] $R^m : (d, d_d) \rightarrow c^m : \ m \in \{u, c\}$, where d is the total dB loss between nodes and d_d is the dB loss between one of the nodes and the detector including switch loss. Given a transmission requirement matrix T_{ij} between user nodes, a cost for adding detector pairs C^m_{det} and a cost for turning 'on' a detector site C^m_{on}, a maximum number of detectors on each site Λ

and a parameter M_{ij} defining the minimum required number of unique paths with transmission T_{ij} for rigidity, we find the cheapest way to build the connected network.

We define $K = \{(i,j)|i,j \in S\}$ as the set of users that wish to connect and $Y = \{(i,j,d)|(i,j) \in K, d \in D\}$ as all possible connecting paths. We assume the shortest distance between users and detectors is used. f_s is the fraction of total time used in network calibration.

Variables: We denote the 'on/off' state of the detector site by $\delta_d^m \in \{0,1\}$, $\lambda_d^m \in \mathbb{N}^+$ as the number of detectors on site (d,m) and $Q_k^m \in \mathbb{R}^+$ as the fraction of time the detector is generating keys for path $k \in Y, m \in \{u,c\}$. We define the MILP as:

$$\text{min}: \sum_{\substack{d\in D \\ m\in\{u,c\}}} (C_{det}^m \lambda_d^m + C_{on}^m \delta_d^m)$$

subject to :

$$\lambda_d^m \leq \Lambda \delta_d^m \ \forall d \in D, m \in \{u,c\}$$

$$\sum_{\substack{d\in D \\ m\in\{u,c\}}} Q^m_{k=(i,j,d)} c^m_{(i,j,d)} \geq M_{ij} T_{ij} \ \forall i,j \in K \quad (1)$$

$$c^m_{(i,j,d)} Q^m_{k=(i,j,d)} \leq T_{i,j} \ \forall k \in Y, m \in \{u,c\}$$

$$\sum_{i,j\in K} Q^m_{k=(i,j,d)} \leq \alpha \lambda_d^m \ \forall d \in D, m \in \{u,c\}$$

The objective is to minimise the cost of adding detectors and turning detector sites 'on'. Constraint 1 ensures up to Λ detectors are placed in 'on' sites and none in 'off' sites. Constraint 2 ensures the total key flow for each commodity satisfies the traffic requirement matrix, constraint 3 ensures M_{ij} unique paths are taken[9], while constraint 4 ensures there are enough detectors on the site for the required key flow. The factor $\alpha = 1 - f_s$ is added to account for the calibration time.

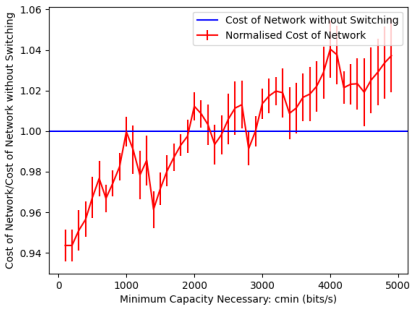

Fig. 3: Ratio of switched to not-switched graph cost against increasing key transmission requirement for TN model

Trusted Node Model: We consider a graph $G = (V,E)$, where vertices are split into untrusted user node $S \subset V$, and trusted node $T \subset V$ sets. We further assume the existence of a mapping for key rates $R : d \to c$, dependent on the loss of the connection. Given T_{ij} $\forall i,j \in S$, a maximum number of devices on each node Λ, M_{ij}, the cost of each detector C^D and source C^S and the cost of turning 'on' a trusted node $i \in T$: $C_{tn,i}$, we find the cheapest way to build the connected network.

We further define $\mathcal{K} = \{i,j|i,j \in S, i > j\}$ and $\mathcal{N}(i)$ as the neighbours of i in G.

Variables: Denoting the 'on/off' state of a trusted node by $\delta_i \in \{0,1\}$, $x_{i,j}^k \in \mathbb{R}^+$ as the qubit flow from source i to detector j for commodity k and $X_{i,j}^k = x_{i,j}^k + x_{j,i}^{k_R} \in \mathbb{R}^+$ as the flow of logical keys across edge i,j for commodity k. Note that $x_{j,i}^{k_R}$ is the logical key flow in the i,j direction but a qubit flow in the j,i direction. Further defining $N_i^D, N_i^S \in \mathbb{N}^+$ as the number of detectors and sources on node i respectively, the MILP is defined as:

$$\begin{array}{lll}
\text{min} \sum_{j\in T}(C_{tn,j}\delta_j + C_i^D N_i^D) & + \sum_{i\in V} C_i^S N_i^S & \\
\text{s.t. } N_i^D \leq \Lambda \delta_i & \forall i \in T & 1 \\
N_i^S \leq \Lambda \delta_i & \forall i \in T & 2 \\
\sum_{j\in\mathcal{N}(i)} \frac{\sum_{k\in K} x_{i,j}^k}{c_{i,j}} \leq \alpha N_i^S & \forall\, i \in V & 3 \\
\sum_{j\in\mathcal{N}(i)} \frac{\sum_{k\in K} x_{j,i}^k}{c_{i,j}} \leq \alpha N_i^D & \forall\, i \in T & 4 \\
\sum_{j\in\mathcal{N}(i)} \frac{\sum_{k\in K} x_{j,i}^k}{c_{i,j}} \leq 0 & \forall\, i \in S & 5 \\
\sum_{m\in\mathcal{N}(n)} \chi_{n,m}^{k=(i,j)} = 0 & \forall\, n \in V \setminus \{i,j\} & 6 \\
\sum_{m\in\mathcal{N}(n)} X_{n,m}^{(n,j)} \geq M_{nj} T_{nj} & & 7 \\
X_{(i,j)}^{k=(n,m)} = 0 & \forall\, j \in S \setminus \{m\} & 8 \\
X_{(n,i)}^{k=(i,j)} = 0 & \forall n \in \mathcal{N}(i) & 9 \\
X_{(j,n)}^{k=((i,j)} = 0 & \forall n \in \mathcal{N}(j) & 10 \\
\sum_{j\in\mathcal{N}(i)} X_{i,j}^{(n,m)} \leq T_k & \forall\, i \in V \setminus \{n\} & 11
\end{array} \quad (2)$$

where $\chi_{n,m}^{k=(i,j)} = X_{n,m}^{k=(i,j)} - X_{m,n}^{k=(i,j)}$ and constraints $6-11$ are over $k \in \mathcal{K}$. The objective is to minimise the cost of turning trusted nodes 'on' and adding sources and detectors. Constraints 1-2 ensure that no detectors or sources respectively are placed in 'off' nodes and their number does not exceed Λ. Constraint 3 ensures there are enough sources on a node to accommodate the key flow through it. Constraints 4-5 do the same for detectors. We assume no detectors are placed on user nodes. Constraint 6 is the conservation of key flow[12]. Constraint 7 ensures the key requirement is met and constraint 11 ensures M_{ij} unique paths are used[9]. Constraint 8 enforces that users in the network are untrusted. Constraints 9-10 prevent loops[13].

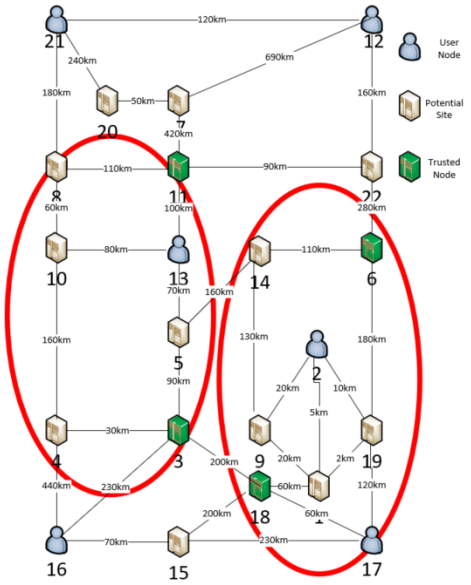

Fig. 4: BT Core Network[19]. The two subnets in ellipses are connected using the TF-QKD model. The green nodes are TNs connecting to the rest of the network. Outside the subnets, the TN model is used, where for long connections TNs are added every $50km$ to ensure connectivity.

Results

We first investigate random mesh graphs, enclosed in a $100km \times 100km$ square, with average connectivity 3.5, and uniform $T_{ij} = c_{min}$. We use Cplex[23] to solve the models assuming $\Lambda = 12$, $M_{ij} = 2$, $f_s = 0.1$, a switch loss of $1dB$, fibre attenuation of $0.2dB/km$, $C^c_{on} = 3.27$, $C^u_{on} = 1.68$, $C^c_{det} = 1.136$, $C^u_{det} = 1$, $C^D_i = 0.1$, $C^S_i = 0.02$ and $C_{tn,i} = 1$. Figure 2 shows the relative cost of the switched compared to the not-switched network for the TF-QKD model for graphs with $|S| = 40, |D| = 10$. At low T_{ij}, the ability to share detectors results in costs reduced by $> 60\%$ of the not-switched cost even when switching is limited to 2 devices, while cost reductions $> 20\%$ can be expected even at $T_{ij} = 4.5kbits/s$. Figure 3 shows the relative cost of the switched compared to the not-switched network for the TN model for graphs with $|T| = 19, |S| = 6$. Switching only reduces the network cost by up to 6% at low T_{ij} while at high T_{ij} switched networks are more expensive, a result of the switch loss and calibration time. The dips can be attributed to the fact that sharing detectors is least effective when an integer number of detectors per connection is needed and some saving can be expected when we go above this integer. However this is not as significant as the original dip. The TF-QKD model benefits from switching at higher T_{ij} than the TN model.

Next, we consider the BT Core network model shared under the IDEALIST EU Collaborative project[19] illustrated in Figure 4. T_{ij} is given in Table 1 and we set $M_{ij} = 1$. The nodes in the circles are connected using the TF-QKD model, as two separate subnets, and nodes outside these subnets are connected with the TN model. For long distance connections we add TNs every $50km$. Figure 5 shows the ratio between switched and not-switched network cost for this graph for various scalings of T_{ij}. We scale the costs in the TN model by 8 to comply with the TF model costs. We see the graph follows similar trends to the TN model graph, demonstrating that the dominant cost comes from the TN section and that the results can be extended to real networks. At low T_{ij}, up to $2.5kbits/s$ average, savings of $\sim 4\%$ can be expected from switching. However, at higher T_{ij} the switching graph becomes more expensive.

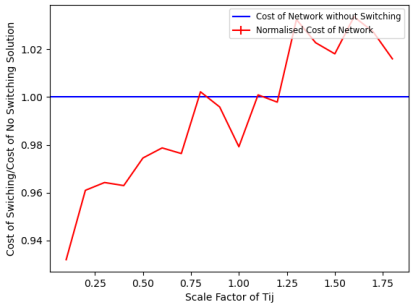

Fig. 5: Ratio of switched to not-switched graph cost against scalings of T_{ij} from Table 1 for the graph in Figure 4

T_{ij}	$i = 12$	$i = 13$	$i = 16$	$i = 17$	$i = 21$
$j = 2$	5.7	5.3	2.4	0.8	2.7
$j = 12$	0	17.1	7.7	2.6	8.8
$j = 13$	0	0	7.2	2.5	8.2
$j = 16$	0	0	0	1.1	3.7
$j = 17$	0	0	0	0	1.3

Tab. 1: T_{ij} in $kbits/s$ for the graph in Figure 4.

Conclusions

We have proposed MILP models to optimise the cost of building quantum networks for a given transmission requirement between users with switching for both the TN QN model and TF-QKD QN model[18].

Investigations show that switching can result in significant cost savings when the user key rates are below a given threshold, which is higher for the TF-QKD model than the TN model. We further show that the benefits of switching at low transmission requirements generalises to a real network. Development of heuristic algorithms provides an avenue for future research.

Acknowledgements

This work was supported by EPSRC and BT through grant EP/V519662/1.

References

[1] M. Peev, C. Pacher, R. Alléaume, *et al.*, "The SECOQC quantum key distribution network in Vienna", *New Journal of Physics*, vol. 11, 7 Jul. 2009, ISSN: 1367-2630. DOI: 10.1088/1367-2630/11/7/075001.

[2] M. Sasaki, M. Fujiwara, H. Ishizuka, *et al.*, "Field test of quantum key distribution in the Tokyo QKD Network", *Optics Express*, vol. 19, 11 May 2011, ISSN: 1094-4087. DOI: 10.1364/OE.19.010387.

[3] D. Stucki, M. Legré, F. Buntschu, *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment", *New Journal of Physics*, vol. 13, 12 Dec. 2011, ISSN: 1367-2630. DOI: 10.1088/1367-2630/13/12/123001.

[4] J. F. Dynes, A. Wonfor, W. W. Tam, *et al.*, "Cambridge quantum network", *npj Quantum Information*, vol. 5, 1 Dec. 2019, ISSN: 20566387. DOI: 10.1038/s41534-019-0221-4.

[5] Y.-A. Chen, Q. Zhang, T.-Y. Chen, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres", *Nature*, vol. 589, 7841 Jan. 2021, ISSN: 0028-0836. DOI: 10.1038/s41586-020-03093-8.

[6] M. Pant, H. Krovi, D. Towsley, *et al.*, "Routing entanglement in the quantum internet", *npj Quantum Information*, vol. 5, p. 25, 1 Dec. 2019, ISSN: 2056-6387. DOI: 10.1038/s41534-019-0139-x.

[7] K. Chakraborty, D. Elkouss, B. Rijsman, and S. Wehner, "Entanglement distribution in a quantum network: A multicommodity flow-based approach", *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–21, 2020, ISSN: 2689-1808. DOI: 10.1109/TQE.2020.3028172.

[8] J. Rabbie, K. Chakraborty, G. Avis, and S. Wehner, "Designing quantum networks using preexisting infrastructure", *npj Quantum Information*, vol. 8, p. 5, 1 Dec. 2022, ISSN: 2056-6387. DOI: 10.1038/s41534-021-00501-3.

[9] F. Pederzolli, F. Faticanti, and D. Siracusa, "Optimal Design of Practical Quantum Key Distribution Backbones for Securing CoreTransport Networks", *Quantum Reports*, vol. 2, 1 Jan. 2020, ISSN: 2624-960X. DOI: 10.3390/quantum2010009.

[10] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-Efficient Quantum Key Distribution (QKD) Over WDM Networks", *Journal of Optical Communications and Networking*, vol. 11, p. 285, 6 Jun. 2019, ISSN: 1943-0620. DOI: 10.1364/JOCN.11.000285.

[11] G. Savva, K. Manousakis, M. Gunkel, and G. Ellinas, "Quantum Key Distribution: An Optimization Approach for the Management Plane", IEEE, May 2022, pp. 5737–5743, ISBN: 978-1-5386-8347-7. DOI: 10.1109/ICC45855.2022.9838813.

[12] Q. Li, Y. Wang, H. Mao, J. Yao, and Q. Han, "Mathematical model and topology evaluation of quantum key distribution network", *Optics Express*, vol. 28, p. 9419, 7 Mar. 2020, ISSN: 1094-4087. DOI: 10.1364/OE.387697.

[13] T. Schaich, V. Karavias, M. Sich, S. Dufferwiel, M. Payne, and A. Lord, "Influence of Cooling on Quantum Network Deployment", *arXiv:2110.15005*, Oct. 2021.

[14] R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, "Topological optimization of quantum key distribution networks", *New Journal of Physics*, vol. 11, p. 075 002, 7 Jul. 2009, ISSN: 1367-2630. DOI: 10.1088/1367-2630/11/7/075002.

[15] E. Hugues-Salas, F. Ntavou, Y. Ou, *et al.*, "Experimental Demonstration of DDoS Mitigation over a Quantum Key Distribution (QKD) Network Using Software Defined Networking (SDN)", OSA, 2018, ISBN: 978-1-943580-38-5. DOI: 10.1364/OFC.2018.M2A.6.

[16] E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks", *Journal of Optical Communications and Networking*, vol. 11, A209–A218, 2 Feb. 2019, ISSN: 19430620. DOI: 10.1364/JOCN.11.00A209.

[17] R. S. Tessinari, A. Bravalheri, E. Hugues-Salas, *et al.*, "Field Trial of Dynamic DV-QKD Networking in the SDN-Controlled Fully-Meshed Optical Metro Network of the Bristol City 5GUK Test Network", *ECOC*, 2019. DOI: 10.1049/cp.2019.1033.

[18] V. Karavias, A. Lord, and M. Payne, "Reducing Network Cooling Cost Using Twin-Field Quantum Key Distribution", *arXiv:2107.02665*, Jul. 2021.

[19] P. Wright, M. C. Parker, and A. Lord, "Minimum- and Maximum-Entropy Routing and Spectrum Assignment for Flexgrid Elastic Optical Networking [Invited]", *Journal of Optical Communications and Networking*, vol. 7, A66, 1 Jan. 2015, ISSN: 1943-0620. DOI: 10.1364/JOCN.7.000A66.

[20] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters", *Nature*, vol. 557, 7705 May 2018, ISSN: 0028-0836. DOI: 10.1038/s41586-018-0066-6.

[21] W. Wang and H.-K. Lo, "Simple method for asymmetric twin-field quantum key distribution", *New Journal of Physics*, vol. 22, 1 Jan. 2020, ISSN: 1367-2630. DOI: 10.1088/1367-2630/ab623a.

[22] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution", *Physical Review Letters*, vol. 94, 23 Jun. 2005, ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.94.230504.

[23] "Cplex, IBM ILOG, v20.1: Users manual for CPLEX", *International Business Machines Corporation*, 2020.