The promise of secure communication based on Quantum Key Distribution (QKD) has resulted in a steady increase of its technological maturity since the first quantum key exchange protocol was proposed in 1984\textsuperscript{1,2}. Advanced protocols such as Decoy State BB84 have demonstrated increased security and reach and commercial QKD equipment for use in optical networks has reached the market\textsuperscript{3–5}. But, QKD networks are still subject to active research\textsuperscript{6–9}. A recent overview of major QKD networks points out that current implementations suffer from detector dark counts constraining the QKD channel length\textsuperscript{10–12}. A detector solution with comparatively few dark counts are superconducting nanowires\textsuperscript{13,14}. However, these operate at extremely low temperatures, requiring expensive cryostats. Thus, the idea of co-locating single photon detectors at a single network node such that cooling resources are shared may hold merit for reducing overall deployment cost. Fundamentally, this changes how QKD is deployed in an existing optical network.

Sharing resources in this manner has been overlooked in studies on QKD equipment placement in optical networks\textsuperscript{15–17}. Consequently, we here establish the benefits of co-locating cooling in a QKD network. We propose a linear programming algorithm and heuristic for cooling placement in a given network and investigate the cost threshold for cooled solutions to become economically favourable to uncooled solutions.

| Mean photon number $\mu$ | 0.1 |
|--------------------------|-----|
| Fibre loss $\alpha$      | 0.2 dB/km |
| Pulse repetition rate $f_{rep}$ | 100 MHz |
| Dark count rate $\tau_{DC}$ | 100 Hz (cold) |
| Detector efficiency $\eta_{DC}$ | 0.85 (cold) |
| Dead time $\tau_{dead}$ | 1 $\mu$s (cold) |

TABLE I. Photon source, fibre and photon detector properties.

The fraction of states not lost due to the detector dead time is\textsuperscript{21,22} $\eta_{dead} = (1 + \tau_{dead} f_{rep} p_{\mu})^{-1}$ resulting in a system gain $Q_{\mu} = p_{\mu} \eta_{dead}$.

For BB84 the Quantum Bit Error Rate (QBER) is\textsuperscript{20} $E_{\mu} = (1 - V)/2$ for a visibility $V$ approximated by $V = \frac{\mu^2 \eta_{f} \eta_{fd}}{\mu \eta_{f} \eta_{fd} + 2P_e}$, with $P_e$ modelled as $P_e = (5.3 \times 10^{-7} + P_{DC})$\textsuperscript{20}. Simultaneously the QBER is given by:

$$E_{\mu} = \frac{\eta_{dead}}{Q_{\mu}} \left( \sum_{n=0} Y_n e^{-\mu} \frac{\mu^n}{n!} e_n \right),$$

which allows fitting of the n-photon state QBER $e_n$.\textsuperscript{17} The resulting secure key rate is\textsuperscript{17}:

$$R = -Q_{\mu} f(E_{\mu}) H_2(E_{\mu}) + Q_1 [1 - H_2(e_1)],$$

with single photon gain $Q_1 = Y_1 e^{-\mu} \eta_{dead}$, Shannon entropy $H_2$ and error correcting code efficiency $f(E_{\mu}) = 1.2$ in our model\textsuperscript{20}. Keyrate over distance is presented in Fig. 1 showing that indeed cooled detectors produce higher keyrates and larger reach than uncooled solutions.
III. GRAPH TOPOLOGY

To assess the usefulness of cooling in a network, we define the following model. A network is represented by a directed graph \( g = (N, E) \) consisting of a set of communicating trusted nodes \( N \) and edges \( E \) representing optical channels. Nodes are randomly placed in a 100 × 100 km box. Edges are placed by successively connecting each node to its nearest neighbour if no connection already exists. Then, each node is connected to their second to nearest neighbour etc. When a critical average node degree is reached, no further connections are placed.

As long links can have low or zero capacity, we introduce additional nodes that bisect an edge if it cannot support a minimum key rate in the uncooled case. These nodes, understood as trusted relays, require transmission and receiving equipment which increases overall cost. Hence, the cost-minimising algorithm introduced in the next section can omit equipping a relay.

IV. COST MINIMISING ALGORITHM

Given a graph \( g \), we implement a linear programming algorithm to find the cheapest solution which can support a demand matrix \( K \) whose elements \( K_{ij} \) represent the key material which node \( i \) must exchange with node \( j \). The hop-by-hop keys exchange is modelled as a multi-commodity flow\(^{14,16,23} \) with variables \( x_{nm}^{ij} \) describing the amount of key material flowing along the edge \((n, m)\) with source node \( i \) and destination node \( j \). The set of all source-destination pairs is \( K \). Each edge has a capacity \( c_{nm}^{\text{warm}} \) and \( c_{nm}^{\text{cool}} \) given by Eq. (1). Furthermore, we introduce integer variables \( \delta_{nm} \), indicating the number of links equipped with communications equipment and binary variables \( \xi_n \) which represent if a node is cooled. Only cost associated with equipping links with QKD equipment and cooling are considered (no operational cost).

Cost per link is normalised to unity and the cooling cost relative to the link cost is denoted as \( C_C \). The complete linear program is:

\[
\begin{align*}
\text{minimise : } & \sum_{(n,m) \in E} \delta_{nm} + \sum_{n \in N} \xi_n C_C \\
\text{subject to : } & \\
& \sum_{(i,j) \in K} (x_{nm}^{ij}) - \delta_{nm} c_{nm}^{\text{cool}} \leq 0 \\
& \sum_{(i,j) \in K} (x_{nm}^{ij}) - \xi_n K_{ij} - \delta_{nm} c_{nm}^{\text{warm}} \leq 0 \\
& \sum_n (x_{ni}^{(i,j)}) + \sum_n (x_{ni}^{(j,i)}) = K_{ij} + K_{ji} \\
& \sum_m (x_{nm}^{ij}) - \sum_m (x_{mn}^{ij}) = 0, \forall n \in N \setminus \{i, j\} \\
& x_{nm}^{ij} = 0, \forall n \in N \text{ with } (n, i) \in E \\
& x_{nm}^{ij} = 0, \forall n \in N \text{ with } (j, n) \in E \\
& \xi_n \in \{0, 1\}, \delta_{nm} \in \mathbb{N}_0, x_{nm}^{ij} \in \mathbb{N}_0
\end{align*}
\]

Unless otherwise stated, each line is valid for all \((i, j) \in K\) and \((n, m) \in E\). The first two constraints combined ensure that the correct link capacity is utilised whereas the other constraints ensure key flow conservation\(^{23}\). Source-destination pair \((i, j)\) and \((j, i)\) are treated symmetrically mirroring the symmetric key cipher\(^{16}\).

Cooled Nodes Placement Heuristic. Further to the presented optimal algorithm, we propose a heuristic for placing cooling in a given network. The idea is that cooling will benefit the most links if it is placed at the node with the most connections. Hence, the heuristic strategy sequentially places cooling at the nodes with the highest degree for a given number of cooled nodes. Then, the algorithm in (2) with fixed \( \xi_n \) is invoked. This method converges faster than the algorithm with dynamic cooling placement. The optimal topology for a given cooling cost is determined in post-processing by finding the minimum of the cost-function over the topologies with any number of cooled nodes.

V. RESULTS AND DISCUSSION

For our simulations, we use IBM Cplex\(^{24}\) to solve (2) on graphs with mean node degree of 3.5. Trusted relays are deployed such that every link can support at least 4 kbit/s. We assume a full traffic matrix with \( K_{ij} = 8/(|N| - 1) \) kbit/s where \(|N|\) is the number of communicating nodes (excl. trusted relays). So, each trusted node introduces 8 kbit/s of traffic to the network, indicating a linear traffic growth with \(|N|\). For simplicity, we exclusively considered single link networks letting \( \delta_{nm} \) be binary. Only graphs which could support the demand matrix without cooling under this constraint were analyzed limiting \(|N|\) to 10.

FIG. 1. Quantum secure key rates calculated using Eq. (1).
Figure 2 shows the calculated total cost against the cooling cost for graphs containing 5 to 9 communicating nodes. Focusing on the solid lines, their gradient corresponds to the number of cooled nodes in the optimal network. As a different topology becomes optimal, the gradient changes. Thus, high cooling costs induce flat curves indicating no cooled nodes. Equivalently, for cheap cooling the gradient is greatest as a large number of nodes is cooled. Fig. 2 also shows how the heuristic strategy compares against the optimal placement. Mostly, the heuristic solution agrees with the optimum. However, some deviations from the optimum are observed, indicating that the placement heuristic is not always optimal. Sub-optimal performance may occur if the graph has a low-degree node requiring a lot of trusted relays. Despite that, the heuristic performs well within 10% of the optimal solution.

Following our validation efforts, we investigated the critical cooling cost for which cooling a single trusted node reduces overall cost. The resulting data, shown in the box plot in Fig. 3, indicate that the median critical cooling cost grows from 2 to 8 with the number of communicating nodes. This correlates with the increased traffic which more communicating nodes introduce to the network. Similarly, the minimum critical cost shifts from 1 to 3, the maximum from 6 to 11 for more communicating nodes.

We estimate current cryostat cost at about $0.6-0.7$ in our units. In addition, cooled detectors are about $5 \times$ more expensive than uncooled detectors which are an estimated $5\%$ of an uncooled link’s cost. For a single cooled node, we can combine these costs to an effective cooling cost $C_C$ which lies between 1 and 2 reaching the upper bound with increased number of co-located detectors. Even in the worst case, these results show that median savings up to 5 link costs can be expected which can increase to 9-10 link costs in certain topologies. Further economic benefits of co-location of cryogenically cooled detectors can be expected in the future as the cooling technology matures, and prices reduce.

VI. CONCLUSIONS AND OUTLOOK

We have proposed an optimal and heuristic placement algorithm for applying cooling in a QKD network. The heuristic provides good results within less than 10% of the optimum solution. Co-locating shared cooling equipment is then considered from an economic perspective. We provide evidence that a cooled solution can provide significant savings in the current technology landscape. Our data suggest that the cost benefit increases with the number of communicating nodes and network traffic. An optimisation including cooled, high-performance sources offering extended link reach, presents an interesting research opportunity as further link savings are expected.

VII. ACKNOWLEDGEMENTS

We thank The Royal Society (INF-PHD-180021), EPSRC (EP/V519662/1) and BT for their support.

---

1 C. H. Bennett and G. Brassard, Theoretical Computer Science 560, 7 (2014).
2 W. Y. Hwang, Physical Review Letters 91, 057901 (2003).
3 Y. Zhao, B. Qi, X. Ma, H. K. Lo, and L. Qian, Physical Review Letters 96, 070502 (2006).
4 I. Quantique, “Cerberis3 QKD System - Product Brochure,” (2020).
5. C. Elliott and H. Yeh, “DARPA Quantum Network Testbed,” Tech. Rep. (BBN Technologies, Cambridge, Massachusetts, 2007).
6. R. Alléaume et al., Theoretical Computer Science 560, 62 (2014).
7. M. Sasaki et al., Optics Express 19, 10387 (2011).
8. J. Qiu, Nature 508, 441 (2014).
9. Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, Optics Express 26, 24260 (2018).
10. M. Mebec et al., ACM Computing Surveys 53, 96 (2020).
11. R. H. Hadfield, Nature Photonics 3, 696 (2009).
12. N. R. Gemmell et al., Superconductor Science and Technology 30, 11LT01 (2017).
13. R. Alléaume, F. Roueff, E. Diamanti, and N. Lütkenhaus, New Journal of Physics 11, 075002 (2009).
14. Q. Li, Y. Wang, H. Mao, J. Yao, and Q. Han, Optics Express 28, 9419 (2020).
15. Y. Wang, Q. Li, H. Mao, Q. Han, F. Huang, and H. Xu, Optics Express 28, 26348 (2020).
16. F. Pederzolli, F. Faticanti, and D. Siracusa, Quantum Reports 2, 114 (2020).
17. H. K. Lo, X. Ma, and K. Chen, Physical Review Letters 94, 230504 (2005).
18. C. H. F. Fung, K. Tamaki, and H. K. Lo, Physical Review A - Atomic, Molecular, and Optical Physics 73, 012337 (2006).
19. P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, New Journal of Physics 12, 063027 (2010).
20. C. Gobby, Z. L. Yuan, and A. J. Shields, Applied Physics Letters 84, 3762 (2004).
21. Quantique, “ID Qube NIR Free-running - Product Brochure,” (2021).
22. Quantique, “ID281 Superconducting nanowire system - Product Brochure,” (2021).
23. A. Ravindra, T. Magnati, and J. Orlin, Network flows: Theory, algorithms and applications (Prentice Hall Inc., New Jersey, 1993).
24. IBM, “IBM ILOG CPLEX 12.10 User’s Manual,” (2020).