Trusted Node Deployment Strategies for Long-Haul Quantum Key Distribution Networks

Sai Kireet Patri
ADVA Optical Networking SE
Martinsried, Germany
spatri@adva.com

Mario Wenning
ADVA Optical Networking SE
Martinsried, Germany
mwenning@adva.com

Shivraj Hanumant Gonde
Chair of Communication Networks
Technical University of Munich
Munich, Germany
sh.gonde@tum.de

Achim Autenrieth
ADVA Optical Networking SE
Martinsried, Germany
aautenrieth@adva.com

Jörg-Peter Elbers
ADVA Optical Networking SE
Martinsried, Germany
jelbers@adva.com

Carmen Mas-Machuca
Chair of Communication Networks
Technical University of Munich
Munich, Germany
cmas@tum.de

***Abstract*—The technological maturity of Quantum Key Distribution (QKD) products have generated high demand for secure key distribution in transmitting sensitive data. To provide this service, long-haul network operators are exploring strategies for network-wide deployment of QKD devices while utilizing existing infrastructure. One approach is to place trusted nodes at existing in-line amplifier huts in the network. In this study, we present a near-optimal fiber span aggregation algorithm, which effectively minimizes the number of trusted nodes between Points-of-Presences (PoPs) in the network. In this study, we evaluate six different topological QKD network deployments and eight different technological QKD network deployments in terms of the total secure key rate, as well as the number of QKD fiber pairs deployed. Our results indicate that the span aggregation algorithm increases the distance between each trusted node by up to 20%, thereby reducing the overall number of trusted nodes. Capacity planning for various topologies and technology deployments on simulated Secure Application Entity (SAE) requests is undertaken. Our proposed capacity planning shows that a baseline deployment with span aggregation using a QKD device with a cut-off distance of 140 km can save up to 3 times the number of QKD deployed fibers as compared to a minimum spanning tree-based low-cost deployment.**

***Index Terms*—Quantum Key Distribution, Optical Networks, Classical-Quantum co-existence, Network capacity planning**

I. Introduction

With the growing interest and research in the field of quantum computing, solutions to computationally intensive problems can now be achieved in polynomial time. This also poses a threat to any information encrypted by computationally intensive cryptographic algorithms like Rivest-Shamir-Adleman (RSA) algorithm [1]. Therefore, quantum-safe solutions for securing highly sensitive data amongst both private and governmental organizations are needed. Quantum Key Distribution (QKD) has emerged as one of the commercially viable options to deploy a quantum-safe network. QKD enables an information-theoretic secure exchange of symmetric keys between communicating entities [2]. QKD devices can be integrated into existing Optical Transport Network (OTN) infrastructure and need a quantum channel and a classical channel for key exchange (qubit transmission) and key establishment (basis comparison, information reconciliation, and privacy amplification) respectively [3]. However, QKD devices have two limitations that need to be considered before deployment. Firstly, the QKD signal cannot pass through in-line amplifiers in the OTN network; and secondly, QKD devices have a reach limitation based on several physical and device-based parameters. Since network operators prefer to reuse pre-existing network infrastructure locations for cost reductions, each amplifier location in the network can be a potential location to have QKD device endpoints. These physically secure locations are called trusted nodes (TRNs). Therefore, the challenge faced by network operators planning to deploy QKD networks is to minimize the number of trusted nodes and dark-fiber usage so as to ensure key-exchange capability across the network.

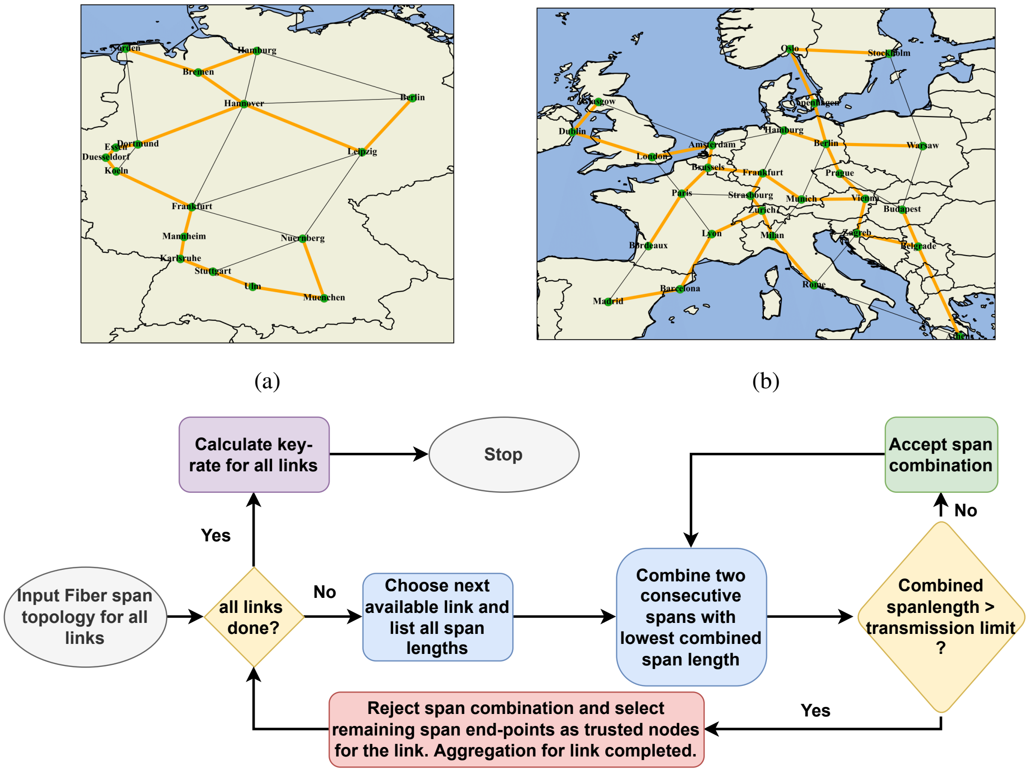
In order to evaluate various QKD network planning strategies, we study the effect of network deployment types, number of trusted nodes, and types of QKD technologies on two long-haul OTNs under study. To this end, we introduce a near-optimal span aggregation algorithm that tries to minimize the number of TRNs on each link. Then, simulating the number of QKD demands in the network, we undertake a capacity planning study assuming a single QKD dark fiber pair between each TRN to compare different topological strategies. Finally, we compare the effect of four different QKD technology types and undertake a multiple fiber capacity planning study to compare the number of deployed QKD fibers for each topological and technological combination.

II. Literature Survey

QKD network deployment over OTN was first studied over a specific network deployment, where a Minimum Spanning Tree (MST) and a single source shortest path-based heuristic

This work has been partially funded by the German Ministry of Education and Research in the project QuNET+ML (**#16KISQ066**).

978-3-903176-54-6 © 2023 IFIP



(a)

(b)

(c)

Fig. 1: (a) and (b) Nobel-Germany and Nobel-EU topology with MST (yellow highlighted) respectively, (c) Span aggregation algorithm flowchart.

was proposed [4]. However, no insights were provided on the applicability on different-sized reference networks. An "out-of-band" QKD deployment heuristic was presented in [5]. Since most of the networks operate a C-Band optical line system, deploying such an algorithm would also demand the installation of band splitters and combiners at each TRN location. Recently, field trials of QKD infrastructure based on untrusted repeater nodes have been conducted. However, such a deployment is suitable only for limited-range metropolitan networks [6]. For planning QKD networks with existing technologies, two mixed-integer linear programming-based solutions are introduced to minimize the number of parallel QKD fibers in the network [7]. However, this work assumes that the trusted nodes are pre-assigned and known to the planning algorithm. Further, the resulting solution space is vast which leads to large computation times. Finally, Li et. al. introduce a mathematical model for topology evaluation of QKD networks [8]. Using a flow-based model, two long-haul networks are simulated and evaluated in terms of the achievable secure key rates. Despite providing an initial algorithm for adding intermediate nodes to the QKD chain, the authors treat the study of relationship between QKD device reach distance, topology, and other link parameters as part of future work.

Overcoming these challenges, our work highlights the practical challenges of deploying a TRN-based QKD network over existing OTN infrastructure and examines strategies used to reduce the number of TRNs in the network. Since every method to reduce TRNs would lead to lower secure key rates, the compromise of lowering the number of TRNs in the network with the decrease in the achievable secure key rates in the network is studied. The deployment strategies compared in our work vary in terms of topology as well as technology.

III. QKD Deployment Strategies

To plan a QKD network, the fiber topology of the existing OTN network needs to be available. Fiber span information is confidential, however, estimates on span lengths can be made based on open-source fiber deployment data, as well as span length optimization experiments [9]. Using such data, we model a distribution of fiber-span lengths with a mean of 80 km (optimized for long-haul optical transmission) and a standard deviation of 10 km. To generate fiber span information for each link in the networks under study, namely, Nobel-Germany (Fig. 1a) and Nobel-EU (Fig. 1b) [10], we draw span lengths from the modeled distribution. For reproducibility, the generated network information is made available online [11].

Fig. 2 shows the QKD architecture example which is used in this work. Each QKD device requires one dark fiber pair (quantum channel) and one classical fiber pair (service channel) [2]. Since QKD is a symmetric key distribution system, the keys need to be stored symmetrically in the KMEs at each TRN. Therefore, a secure key rate (SKR) is used

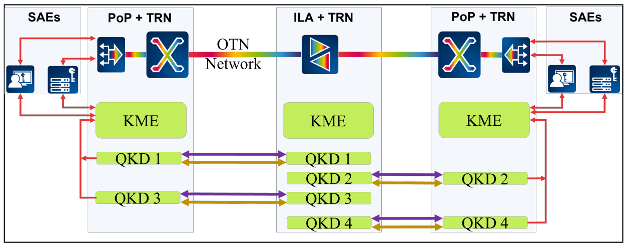


Fig. 2: Secure Application Entities (SAEs) request keys from Key Management Entity (KME) at each trusted node (TRN) location to encrypt data before sending it on the OTN network.

as a performance metric to measure the rate of information exchange between a pair of QKD devices. SKR is highly dependent on not only the fiber span parameters like length and attenuation but also on the QKD device itself, where each device has its own parameters, i.e., QKD protocol, pulse repetition rate, dark count, etc. [3].

From a network capacity planning perspective, the choice of network topology, trusted nodes, as well as the choice of QKD devices needs to be explored in order to find a solution that is suitable for each network. Therefore, we broadly define two deployment strategies, namely *topological* and *technological* strategies, and evaluate each one of them.

A. Topological Strategies

The existing OTN infrastructure consists of traffic generating nodes called *Points-of-Presence (PoPs)* and amplifier nodes called *In-line amplifier locations (ILAs)*. PoPs and ILAs are connected to each other using several bundles of optical fiber cables. The unused optical fibers between any two ILAs or a PoP and an ILA are called as dark fiber. Further, a consecutive collection of optical fibers connecting any two PoPs is defined as a link.

Since SAEs, which generate key requests are located only at PoP locations, there are two ways of routing these demands between any two PoPs. The first is to use any available link in the network to find the shortest path. This method is addressed as ***baseline*** in our work. The second method is to use only links on the network's minimum spanning tree based on link lengths (***MST_dist***). As discussed in [4], MST_dist reduces the number of links on which trusted nodes need to be deployed thereby bringing down the network cost. The disadvantage however, is the lack of protection paths and reduced SKR. Figs. 1a and 1b show the MST links for Nobel-Germany and Nobel-EU network respectively.

Since the assumption that every ILA location is co-located with a trusted node potentially increases the expected operation and installation costs for operators, we introduce a span aggregation (SA) algorithm as described in Fig 1c and create further two strategies, namely ***baseline_SA*** and ***MST_SA***.

The span aggregation algorithm, as described in Fig. 1c can be applied to all links in the given network topology. First, all the fiber spans of the link are listed. Then, using a binary-search method, two consecutive spans with the minimal combined span length are chosen. The combined span length is then verified to be below the transmission limit of the QKD device [3]. If that is the case, the span aggregation is accepted and the intermediate ILA is bypassed. This process continues, till a combination of span length results in exceeding the transmission limit. At this stopping condition, the aggregated span end-points are assigned as TRNs and the link is considered aggregated.

Deployment Strategy (Topological)	Topology type	Span aggregation
baseline	Full network	None
baseline_SA	Full network	ref. Fig
baseline_full	Full network	Full-depth search
MST_dist	Minimum Spanning Tree	None
MST_dist_SA	Minimum Spanning Tree	ref. Fig
MST_dist_full	Minimum Spanning Tree	Full-depth search

TABLE I: Overview of topological deployment strategies

Finally, since the span aggregation algorithm is a suboptimal approach, a full-depth search method to minimize the number of TRNs on each link is also implemented. The full-depth search gives an optimal solution for sapn aggregation by combining consecutive span lengths till the stopping condition of QKD device transmission limit is reached. The deployment strategies ***baseline_full*** and ***MST_full*** implement the full-depth search on the baseline and MST topologies respectively. Table I summarizes the discussed strategies. Hence we evaluate six different topology-based deployment strategies on two networks under study and compare them in Section V.

B. Technological Strategies

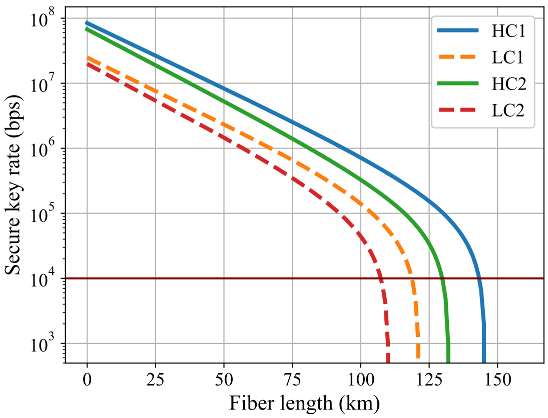


Fig. 3: Secure key rate (SKR) versus fiber length for four different QKD technologies [12].

In recent years, long-haul applications for QKD transmission have led to the development of commercially available QKD devices which claim transmission distances of up to 150 km, while ensuring SKR of at least 1 kbps [3]. We assume that the ability of a QKD device to transmit at longer distances is directly proportional to its cost. Therefore, we envision four different types of QKD technologies as follows:

- LC1 - The first low-cost device assumes QKD BB84 Decoy-state protocol with fiber attenuation of $0.2\ dB/km$, dark-count rate of $10000\ s^{-1}$, APD quantum efficiency of 20% and a repetition rate of $1.25\ GHz$.
- LC2 - The second low-cost device assumes QKD BB84 Decoy-state protocol with fiber attenuation of $0.22\ dB/km$, dark-count rate of $10000\ s^{-1}$, APD quantum efficiency of 20% and a repetition rate of $1\ GHz$.
- HC1 - The first high-cost device assumes QKD BB84 Ideal protocol with fiber attenuation of $0.2\ dB/km$, dark-count rate of $10000\ s^{-1}$, APD quantum efficiency of 20% and a repetition rate of $1.25\ GHz$.
- HC2 - The second high-cost device assumes QKD BB84 Ideal protocol with fiber attenuation of $0.22\ dB/km$, dark-count rate of $10000\ s^{-1}$, APD quantum efficiency of 20% and a repetition rate of $1\ GHz$.

The design choice of QKD protocols, the range of fiber attenuation constant, as well as QKD device parameters are obtained from product data sheets of QKD devices [3], [13]. For HC1 and HC2, using BB84 Ideal protocol [14] is justified as a stop-gap for better algorithms and advancements in photonic transceivers.

As seen in Fig. 3, each of the QKD devices has an SKR value associated with the fiber length. Therefore, we also define a cut-off length for each of the four technologies, which is used as an input to the span aggregation algorithm. To derive the cut-off length, we first fix the lower-bound on the SKR of each fiber span to 10 kbps. This implies that none of the spans in the network deployed with LC1, LC2, HC1 and HC2 can be greater than 120, 105, 140, and 130 km respectively. The impact of the four different QKD devices is analyzed in detail in Section V.

IV. QKD Network Capacity Planning

In order to evaluate the topological and technological strategies, we devise a methodology for QKD network capacity planning. As shown in Fig. 2, SAEs request keys from KMEs, which in turn refresh their key store by symmetrically loading keys from each QKD device pair. The generation of these keys is highly dependent on the achievable SKR of each QKD fiber pair along a chosen path in the network. Therefore, we simulate the addition of SAE requests in the network and route each incoming request onto the QKD fiber pairs. The objective of the capacity planning is to accommodate as many SAE requests as possible in the network, for a given topological and technological (LC1, LC2, HC1, HC2) strategy.

The capacity planning considering only topological strategies assumes a single fiber pair between any two TRNs whereas the capacity planning considering both topological and technological strategies allows for the addition of new QKD fiber pairs. For the multiple fiber capacity planning, in case any QKD fiber pair serving pre-existing SAEs reaches its maximum capacity, a new QKD fiber pair is added between the TRNs.

To simulate the effects of adding SAE requests to the six topological deployment strategies, we model a QKD demand simulator, which first finds up to $k = 5$ shortest paths for the baseline topologies and the first shortest path for the MST_dist topologies for all end-to-end PoPs in the network. Then, the SAE requests are sorted from the longest to shortest paths. To simulate the requested SKR for each SAE, we use a Gaussian distribution with a mean of 100 kbps. Similar to [5], we also assume that SAE requests have an infinite holding time. Each simulation run, however, is restricted to 1000 SAE requests.

Each incoming SAE request is routed on the path with the highest capacity out of the k-shortest paths thereby avoiding greedy filling of the first shortest path links. In case of the single-fiber planning, the SAE request is dropped if it cannot be assigned to any of the paths. For the multi-fiber approach, after each SAE request is added, if any QKD link has an available capacity of less than 5% of its maximum capacity, a parallel QKD fiber-pair is deployed on the bottleneck span. Therefore, the multi-fiber approach minimizes the probability of dropped SAE requests while increasing the number of QKD fiber-pairs and devices.

To improve confidence in our results, we run 100 random simulations for each comparison type. The evaluations have been performed on a machine equipped with 11th Gen Intel® Core™ i7-1185G7 @ 3.00GHz, 32 GB of RAM, running Windows 10. The time taken for each simulation run is in the order of milliseconds.

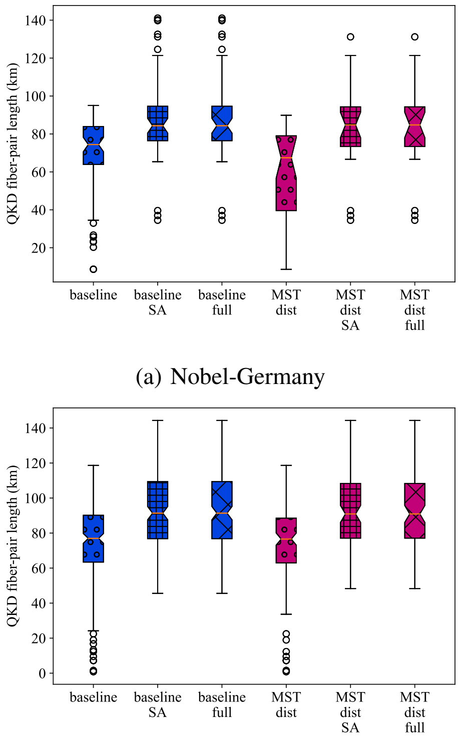
V. Results and Discussion

In this section we first compare 6 topological strategies in terms of the cumulative SKR for Nobel-Germany and Nobel-EU networks. Here we also show the effect of span aggregation algorithms for each of the networks across different topological strategies. Then, assuming that the proposed span aggregation algorithm is used on the *baseline* and *MST_dist* topologies, we compare a combination of 8 topological and technological strategies in terms of the number of QKD fiber pairs and the number of QKD devices in the network.

A. Topological Comparisons

Figs. 4a and 4b show the effect of span aggregation on each of the topological strategies. For Nobel-Germany, span aggregation leads to a mean increase of 15% and 18% in the length of fiber-pairs between TRNs as compared to the *baseline* and *MST_dist* strategy respectively. For Nobel-EU a similar increase in the fiber-pair lengths is observed.

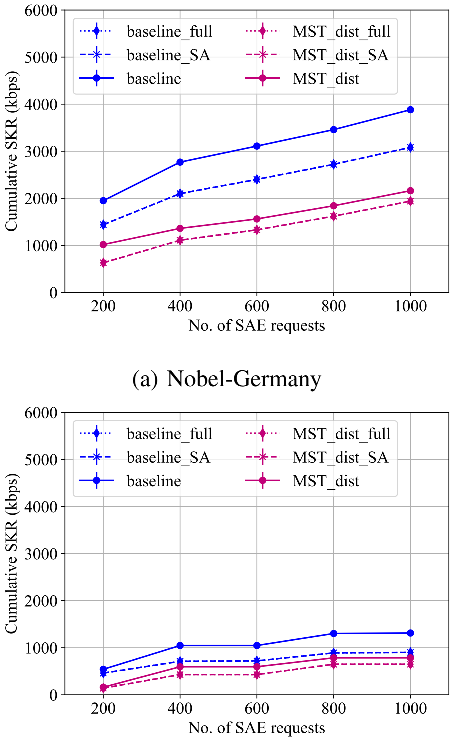
From the results, we see that although span aggregation techniques place lower SKR at higher SAE requests, the cumulative SKR is comparable to the non-aggregated topologies when SAE requests are lesser in the network. Therefore, a strategy of first deploying a span aggregation algorithm based solution and then adding additional TRNs can be planned, for example first deploying *baseline_SA* and then progressively moving towards *baseline* as SAE requests in the network increase. Moreover, comparing the span aggregation algorithm with the full-depth search, the results for both across all topologies and networks are similar. This is since the span lengths have a mean of 80 km, there are very few consecutive



(a) Nobel-Germany

(b) Nobel-EU

Fig. 4: Span length distribution for networks under to show the effect of span aggregation, fixing the technology strategy to HC1.



(a) Nobel-Germany

(b) Nobel-EU

Fig. 5: Cumulative SKR vs. number of SAE requests for single QKD fiber-pair per link deployment.

span lengths in the network which are aggregated, leading to negligible advantage of using a full-depth search for span aggregation.

Figs. 5a and 5b show the cumulative SKR carried by the Nobel-Germany and Nobel-EU network respectively, versus the number of SAE requests added into the network simulator. In this study, HC1 (transmission limit 140 km) is the choice of QKD device for all the simulations and only one QKD fiber-pair is available between every TRN location.

For both the networks under study, *baseline* strategy provides an upper-bound on the cumulative SKR. However, it is also the most expensive option since all the ILAs in the network are converted into trusted nodes. The *baseline_SA* and *baseline_full* as well as *MST_dist_SA* and *MST_dist_full* strategies have the same SKR because they have the same span lengths. As compared to *baseline*, *MST_dist* places almost 50% lesser SKR into the network. Since all the SAE requests in an MST topology can only be routed on their first shortest path, the link capacity saturates early, resulting in lower cumulative SKR. It is interesting to note that *baseline_SA* performs only slightly better than *MST_dist* in the case of Nobel-EU network. This is because span aggregation, while helpful in reducing the overall number of devices, can also reduce the SKR, despite having path diversity. For a given topology with span aggregation place on an average 20% lesser cumulative SKR at the maximum number of SAE requests.

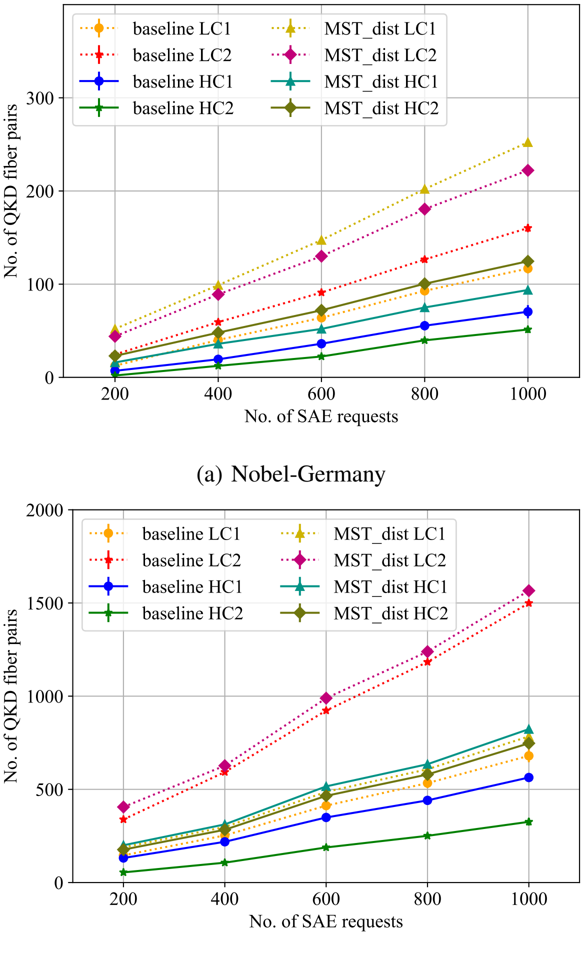
B. Technological Comparisons

After evaluating various topological strategies, we evaluate the effect of four different technologies (as introduced in Sec. III-B) on the networks under study. Since from Fig. 5 it is clear that the proposed span aggregation algorithm works identically to the full depth search on the given networks, we only consider the topologies with span aggregation in this study, namely, *baseline_SA* and *MST_dist_SA*. For brevity, we ignore the suffix "*SA*" for further discussions.

In order to evaluate the benefits of LC1, LC2, HC1, and HC2, we ensure minimum SAE request blocking by using the multiple fiber scenario (described in Sec. III-B). For all the 8 scenarios evaluated, the cumulative SKR, as well as the number of SAE requests placed are similar. Therefore, we compare the number of fiber pairs placed to draw inferences for deployment planning.

As seen in Figs. 6a and 6b, in terms of number of QKD fiber pairs placed, *baseline HC2* places the least number of fiber pairs. We also note that the minimum spanning tree-based topologies, namely *MST_dist LC1*, *MST_dist LC2*, *MST_dist HC1* and *MST_dist HC2*, consistently place more fiber pairs than their *baseline* counterparts using the same technology type in the Nobel-EU network.

From the technological analysis, for Nobel-Germany network, *baseline HC2* emerges as a clear choice for deployment. However, if the number of SAE requests stay relatively low, operators can also aim for an *MST_dist HC2* deployment thereby reducing the overall number of TRNs to be operated and maintained in the network.



(a) Nobel-Germany

(b) Nobel-EU

Fig. 6: QKD fiber pairs vs. number of SAE requests.

VI. Conclusions

In this work, we have analyzed several TRN deployment strategies, which enable Quantum Key Distribution in long-haul OTN. These strategies combine topological changes and a novel span aggregation algorithm to reduce the total number of TRNs in the network. The span aggregation algorithm allows for up to 20% higher QKD fiber-pairs for a fixed technology strategy. The proposed span aggregation algorithm, although sub-optimal, shows similar results as compared to an optimal full-depth search algorithm. Of the eight topological and technological strategies, a full network deployment of QKD, while using the span aggregation algorithm, and deploying the HC2 flavour of QKD devices (*baseline HC2* in Figs. 4 and 6) results in a saving of at least 3 times the number of fiber-pairs deployed as compared to the worst performing topological and technological combination (*MST_dist LC2*). We conclude by acknowledging that although QKD network deployment planning is a complex task with several degrees of freedom, comparative studies provide strategic insights to operators planning to deploy similar networks.

Future work will look into a mixed deployment and an upgrade strategy amongst the different topological and technological combinations. As the results are highly dependent on the network as well as the cost of devices and fiber pairs, a detailed cost model for a techno-economic analysis is also under development.

Acknowledgments

The authors would like to thank Dr. Helmut Griesser (ADVA Network Security), Dr. Matthias Gunkel, Dr. Felix Wissel and Daniel Giemsa (Deutsche Telekom AG) for their fruitful discussions.

References

[1] V. Bhatia and K. Ramkumar, “An efficient quantum computing technique for cracking rsa using shor’s algorithm,” in *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, 2020.

[2] “Quantum key distribution (qkd); qkd module security specification.” https://www.etsi.org/deliver/etsi_gs/qkd/001_099/008/01.01.01_60/gs_qkd008v010101p.pdf, Accessed: Jan 2023.

[3] “ID Quantique.” https://www.idquantique.com/quantum-safe-security/products/, Accessed: Jan 2023.

[4] M. Gunkel, F. Wissel, and A. Poppe, “Designing a quantum key distribution network - methodology and challenges,” in *Photonic Networks; 20th ITG-Symposium*, pp. 1–3, 2019.

[5] 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, no. 6, pp. 285–298, 2019.

[6] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, “The evolution of quantum key distribution networks: On the road to the qinternet,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 839–894, 2022.

[7] F. Pederzolli, F. Faticanti, and D. Siracusa, “Optimal design of practical quantum key distribution backbones for securing coretransport networks,” *Quantum Reports*, vol. 2, pp. 114–125, 01 2020.

[8] Q. Li, Y. Wang, H. Mao, J. Yao, and Q. Han, “Mathematical model and topology evaluation of quantum key distribution network,” *Opt. Express*, vol. 28, pp. 9419–9434, Mar 2020.

[9] B. Karanov, T. Xu, N. A. Shevchenko, D. Lavery, R. I. Killey, and P. Bayvel, “Span length and information rate optimisation in optical transmission systems using single-channel digital backpropagation,” *Opt. Express*, vol. 25, pp. 25353–25362, Oct 2017.

[10] “SNDLib Topologies.” https://sndlib.zib.de, Accessed: Jan 2023.

[11] “Phynwinfo.” https://github.com/SaiPatri/PhyNWInfo, Accessed: Jan 2023.

[12] E. Diamanti, *Security and implementation of differential phase shift quantum key distribution systems*. PhD thesis, Stanford University, 01 2006.

[13] “Toshiba quantum key distribution (qkd).” https://www.global.toshiba/ww/products-solutions/security-ict/qkd/products.html, publisher=ETSI, Accessed: 2023-01-17.

[14] C. H. Bennett and G. Brassard, “An update on quantum cryptography,” in *Workshop on the theory and application of cryptographic techniques*, pp. 475–480, Springer, 1985.