Optimized Deployment and Routing Strategies for QKD and DWDM Networks

Mario Wenning*†, Sai Kireet Patri†‡, Tobias Fehenberger* and Carmen Mas-Machuca†
* Adva Network Security, Berlin, Germany
Email: {mario.wenning, tobias.fehenberger}@advasecurity.com
† Chair of Communication Networks, School of Computation, Information and Technology,
Technical University of Munich (TUM), Germany
Email: cmas@tum.de
‡ ADVA, Martinsried/Munich, Germany
Email: spatri@adva.com

***Abstract*—Quantum key distribution (QKD) is an emerging technique for encrypting dense wavelength-division multiplexing networks (DWDMNs). The network-wide utilization of QKD raises challenges for deploying a QKD network (QKDN) and operating it via the key management network (KMN). These challenges include the optimized placement of QKD devices and the utilization of the QKDN. The goal of our QKDN deployment strategies is to maximize the reuse of infrastructure of the DWDMN, and the routing algorithms focus on the most efficient use of the deployed QKDN. We evaluate the multi-layer network consisting of a QKDN, a KMN, and a DWDMN and jointly optimize operation and deployment. Our analysis comprises different routing algorithms for key relaying within the KMN. Furthermore, we compare different deployment strategies for QKDNs and investigate the joint impact of both network layers, the QKDN, and the key management layer. For the two analyzed scenarios of uniformly distributed demands and the multi-year planning scenario, we can reduce the number of required QKD devices by approx. 11 % to 18 % without any performance penalty through optimized utilization of the deployed QKDN as compared to suboptimal operation. Finally, we show the combination of deployment and key relay algorithms that can cope with a multi-period traffic demand forecast. In the analysis of the multi-year planning scenario, we demonstrate deployment strategies that scale with the increasing demands of the DWDMN in the future, maintain optimized utilization, and, hence, allow efficient future-proof quantum-safe communication.**

***Index Terms*—Quantum Key Distribution, Network Planning, Multi-Layer Networks**

I. Introduction

As the security of communication becomes more important and the requirements for secure communications increase, current encryption and decryption schemes do not fulfill future security requirements due to the threat imposed by powerful quantum computers [1]. Quantum key distribution (QKD) recently gained attention due to advancements in its maturity, maximum reach, and achievable secure key rates (SKRs). In addition to the advancements, QKD guarantees the information-theoretic security of the key exchange through physical properties [2]. This allows utilizing QKD for securing optical dense wavelength-division multiplexing Networks (DWDMNs) and making them future-proof. However, QKD only covers the key exchange and is used in conjunction with symmetric encryption schemes to secure data. The prerequisite for the symmetric encryption scheme is the same key at the transmitter and the receiver. We investigate the network-wide usage of QKD in DWDMNs for encrypting all traffic data. Therefore we consider the deployment and operation of an QKD network (QKDN) and a key management network (KMN) in addition to the DWDMN [3]–[5]. Figure 1 illustrates the simplified multi-layer network [3]. The DWDMN is responsible for secure data transmission. Here, transmitters A and D symmetrically encrypt and decrypt bidirectional communication of traffic data. The key management layer performs the key relay to share keys between arbitrary nodes via intermediate trusted nodes. Therefore, the key distribution to meet the key demands in DWDMNs depends jointly on the QKDN and the KMN. In our work, we investigate the joint impact of the KMN and QKDN on the key distribution for the DWDMN. On the one hand, we analyze routing algorithms for the KMN to determine the optimal route of the key relay. On the other hand, we investigate trusted node deployment algorithms to maximize reuse of DWDMN infrastructure and provide sufficient SKRs.

Applying QKD to secure DWDMNs has two benefits. Firstly, the infrastructure of the DWDMN can be reused for deploying the QKDN, e.g., dark fiber and amplifier huts. Secondly, the configuration of the DWDMN is assumed to be static for the period of a year since the planned capacity can cope with the peak traffic in the given period [6]. The latter relaxes time constraints for the processes within the KMN because the request for keys can be forecasted, and keys can be proactively distributed via both lower layers. The forecast is given by optical network planning as described in [7], and serves as an input for this work. Our contribution is twofold:

- Joint evaluation of different deployment algorithms for the QKDN and operation algorithms for the KMN
- Multi-year planning scenario for optimizing the utilization of the deployed QKDN

QKD has recently been subject to various optimization

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

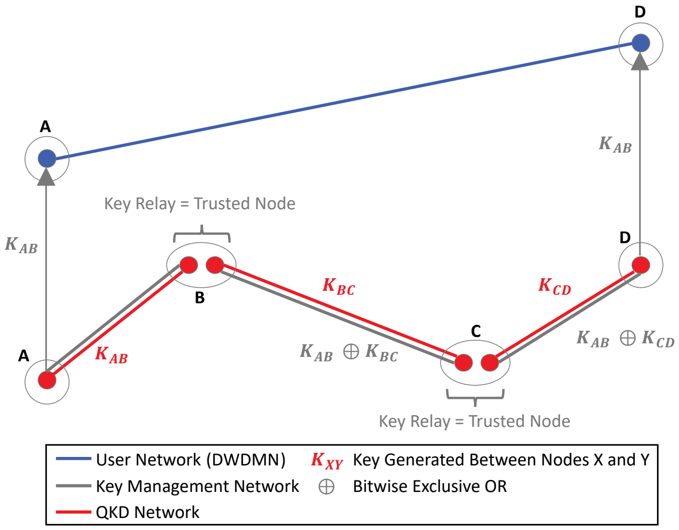

Fig. 1. Schematic multi-layer network [3]. The user network (DWDMN) represents the data transmission. QKD and KMN ensure the key distribution which is the prerequisite for secure data transmission.

studies, due to its maturity and advancements. However, the focus was on either the QKDN or the KMN. Savva et al. assessed the optimal placement of QKD devices and management nodes within the network such that the minimum and average SKR over all links is maximized [8]. The optimization shows that the location of nodes and the number of QKD devices significantly influence the SKRs between the nodes. However, they restricted their analysis to one specific route per communication path and do not optimize the routing of the key relay path. Other works analyze parameters based on the network's topology and aim for an optimized extension of the topology for deploying a QKDN [9]. They propose a quality measure of the topology based on the generic maximum flow problem. Hence, they extend the topology by additional nodes and links and evaluate the gain in the quality measure. The quality parameter of the topology, however, does not provide information on the routing scheme. Utilizing the topology's quality through the routing scheme remains an open task.

In comparison, the authors in [10] propose an optimized routing algorithm selecting out of candidate paths based on the Dijkstra algorithm. For the evaluation, they propose a dynamic simulation of the QKDN and a greedy algorithm for minimizing the cost of a path. The cost is exponentially proportional to the residual local key. However, they fix the deployment of the QKDN in the assumptions. To the best of our knowledge, there is no joint evaluation of the multi-layer network design strategy for this problem.

II. QKD Secured DWDMNs

This section describes the mapping of secured DWDMNs utilizing QKD to the generic standardized multi-layer network [3]. Therefore, we begin with the DWDMN and specify the encryption scheme. After that, we describe the routing algorithms of the KMN, and the deployment strategies and modelling of the QKDN.

A. Encryption Scheme and Key Usage for DWDMN

We determine DWDMN demands by a source and destination node as well as a requested data rate. Depending on the data rate, one or more lightpaths (LPs) are needed to cope with the traffic data [7]. While QKDNs have dynamic performance changes within minutes, the configuration of LPs is assumed to be static within one year [11]. Hence, the required key for updating the symmetric encryption scheme, i.e., the key request, in a given time range is also static. Firstly, we assume uniformly distributed demands between any pair of nodes. Secondly, we use a traffic model based on the number of data centers and internet exchange points in each node to derive demands. Using these demands, a network planning algorithm calculates the required LPs and their configuration of different years [7]. In a given planning period of one year, we assume static LP configurations. The encryption scheme defines the relation between the DWDMN and the QKDN. Depending on the encryption scheme, the key size and the frequency of key requests might differ for the same setting of the DWDMN. In our work, we assume the utilization of the advanced encryption standard (AES) with a key size of 256 bits (AES-256). AES is standardized by the National Institute of Standards and Technology (NIST) [12]. In [13], AES is also considered secure in the presence of quantum computing resources. We assume the largest key size of 256 bits for maximizing security via encryption. One key can securely encrypt 0.3887 terabytes of traffic data [14]. Hence, an LP carrying 100 Gbps encrypted traffic would require a new key of 256 bits every 31.12 seconds. In our analysis, we limit the granularity of the data rate to integer multiples of 100 Gbps. We refer to the key usage in a given time frame as the *key consumption rate*. The operation of the KMN, i.e., the key relay, must guarantee the same key at the source and destination node for each encrypted LP.

B. Routing within the KMN

In the first step, solely neighboring nodes of the QKDN have shared keys in common. By utilizing key relays, the KMN enables end-to-end encryption for the DWDMN. Figure 1 depicts the key relay for the simplified network to ensure that nodes A and D have the same shared key K_{AB}. The One Time Pad (OTP) is the preferred option for key relaying because it maintains information theoretical security [15]. The implementation of the OTP for key relaying is the bitwise exclusive OR (XOR) operation for combining two keys and sending the result via the KMN. However, the application of the OTP implies that relayed keys have the same size. Hence, the minimum SKR of all links shown in the QKDN in Figure 1 limits the resulting SKR for encrypting communication between nodes A and D. The topology of the KMN is the same as the QKDN and might differ from the DWDMN topology. Furthermore, we assume a buffer at every node for every edge. Those buffers allow key storage and compensate for quantum links' fluctuations. We consider key requests every 31.12 seconds, hence the key size equals integer multiples of 256 bits according to the data rate of the LP. Generally, the path of the LP within the DWDMN can differ from the key relaying path within the KMN. In our previous work [11], we developed three routing algorithms and applied them to simplified dynamic QKDNs. These algorithms provide the bases for the routing in the KMN. For all routing algorithms, we consider the k-shortest paths and set $k = 5$. We compare three different routing algorithms performing the path decision based on the k-shortest paths. Firstly, we evaluate a load-balancing heuristic as described in [16]. The algorithm tries to distribute the demands equally by monitoring the load per edge. Secondly, we assess a routing scheme based on machine learning (ML). The algorithm chooses one of the k-shortest paths depending on the number of hops, least filled buffer, shortest-path betweenness centrality for the nodes, and average SKRs [11]. Finally, we consider an optimal routing algorithm utilizing integer linear programming (ILP) to maximize the least filled buffer within the KMN [11]. In general, the decision of the routing algorithm is based on information on the QKDN and the DWDMN. The ILP-based algorithm needs data on all demands and key buffers simultaneously. Compared to the ILP-based algorithm, the heuristic- and ML-based algorithms need limited information on the k-shortest paths. Furthermore, the latter two algorithms route the demands separately and optimize the decision for a single demand.

C. QKD Networks

After the description of both upper layers, we describe the QKDN starting with the model of quantum links. In addition to the key consumption rate, key size, and data rates, we need to estimate the SKR of the QKDN. We assume the BB84 protocol for the QKDN [17]. Furthermore, we estimate the SKR by using the modeling from [18]. We use the following parameters: attenuation = 0.2 dB/km, margin loss = 1 dB, quantum efficiency = 10 %, repetition rate = 1.25 GHz [19], system error rate = 0.01, dark count rate = 1000 Hz, time window = 1 ns. The maximum reach of commercial QKD devices is between 90 and 150 km [19]. For our analysis, we fix the maximum reach to 100 km. To stay within the maximum reach, the deployment of trusted nodes guarantees the split up of every link into spans shorter or equal to the maximum reach. The minimum SKR of its spans limits the SKR of a link.

Figure 2 shows the SKR depending on the reach. Different attenuation and repetition rates are displayed to show the sensitivity of the SKR to those parameters. Figure 2 clearly shows the exponential dependency of the SKR on the reach and emphasizes the influence of the span's length on the performance of the QKDN. We model time-dependent fluctuations of the SKR as Gaussian noise with a standard deviation of 9 % of the SKR [11]. The SKR is assumed to be stable for time periods of approx. 30 seconds. The time-dependent performance of quantum link has been shown to approximately match measurements of a live QKDN [11]. Besides the model of the quantum link, we derive the QKDN from optical core networks focusing on the deployment of trusted nodes. Furthermore, we maximize the reuse of infrastructure, i.e., by using amplifier huts for trusted nodes. For the initial span distribution of optical core networks, we refer to [20]. There are two degrees of freedom for deploying QKDNs: choosing the topology and choosing the locations of trusted nodes. Firstly, we want to describe the topology selection. For enabling secret communication between any pair of nodes, every node must be included in the QKDN, but not necessarily every link. We evaluate the minimum spanning tree with the shortest total length for the minimum deployment and refer to this topology as *minimum spanning tree topology* [21]. In addition to the minimum spanning tree topology, we assess the deployment over the entire topology. Hence, every link of the DWDMN is also a link of the QKDN. We refer to the topology of full deployment as *baseline topology*.

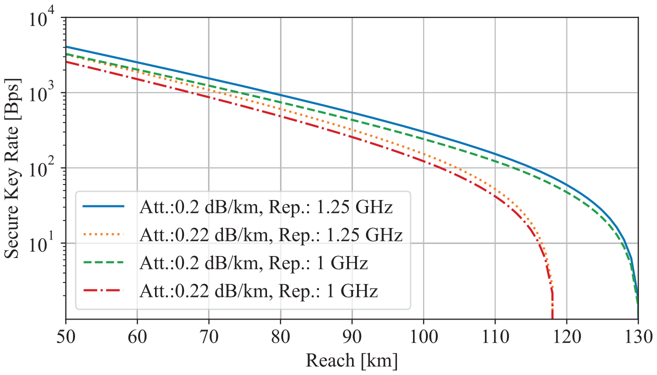

Fig. 2. Estimated SKR depending on the the reach.

Besides the choice of the topology, we compare two trusted node deployment strategies. The requirements for the location of a trusted node as defined in Figure 1 are high because it is potentially a point of attack. During the key relay, both keys are accessible, requiring adherence to security standards and access to an electrical power supply [22]. Therefore, the deployment strategy is to install the minimum number of required trusted nodes by reusing the infrastructure of the DWDMN. We consider a maximum reach of 100 km implying for the QKDN that within every link, the distance between neighboring trusted nodes is not allowed to exceed 100 km [19]. We consider two different deployment strategies. Firstly, we assume a trusted node at the location of every in-line amplifier (ILA). We refer to this deployment as *baseline deployment*. Secondly, we analyze the deployment strategy that minimizes the number of trusted nodes by performing a brute-force search. The brute-force search takes the ILAs of a link as candidate trusted nodes. The result of the brute-force search is the selection of trusted nodes out of the candidate positions that minimizes the number of trusted nodes while fulfilling the maximum reach requirement. Within this solution set, we select the result that minimizes the maximum span length within a link [21]. We refer to this deployment as *minimal deployment*. Potentially, there is the option to add more trusted nodes than present ILAs. The exploitation of new trusted nodes is more expensive than reusing existing amplifier huts. Hence, it is advantageous to upgrade from the minimum spanning tree topology to the baseline topology instead of exploiting more trusted nodes for the minimum spanning tree topology. The combination of the topology and the trusted node placements leads to four different QKDNs with a different number of QKD devices as depicted in Figure 3. In the following section, we jointly compare the different QKDNs and routing algorithms.

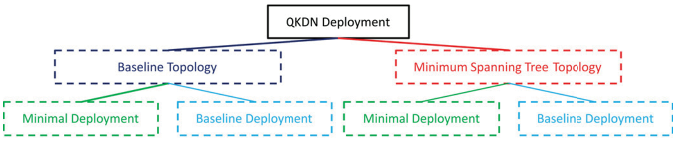

Fig. 3. Deployment Strategies for the QKDN.

III. Results

We split the results into two subsections to gain insights into the inter-dependencies between demands, routing algorithms, and trusted node deployments. The first subsection sheds light on the impact of routing algorithms and trusted node deployments. We assume in this subsection uniformly distributed demands between any pair of nodes. Secondly, we consider demands derived from the DWDMN planning. The latter analyzes the impact from the highest layer. Finally, we combine the results of previous subsections for examining multi-year planning. We evaluate the Nobel-Germany (Nobel-DE) network [23].

A. Uniformly Distributed Demands between Any Pair of Nodes

Firstly, we assess the capabilities of the minimum spanning tree topology. The results compare the baseline with the minimal deployment of trusted nodes for the Nobel-DE topology and 4 hours of operation. For both deployments, the maximum number of LPs between any pair of nodes equals one. The corresponding overall bidirectional throughput equals 13.6 Tbps. Figure 4 shows the buffer loads. All buffers are initialized with a load of 50 %.

The results show similar evolution of the buffer loads for both deployments. The filling of every buffer is above 90 % within the first hour of operation. Both deployments cope with the key consumption rate without draining buffers. However, choosing two LPs would empty the buffer over time, as neither deployment strategy can deliver a sufficient high SKR. The baseline and minimal deployment need 66 and 56 QKD devices, respectively. Due to the integer increase of 256 bits, there is no gain in deploying more than 56 QKD devices. Routing schemes can not increase the performance because the minimum spanning tree topology determines the route.

Next, we analyze the baseline topology, where every edge of the DWDMN is also part of the QKDN. The ILP-based algorithm is used for estimating the maximum key consumption rate. We consider the same key consumption rate for the heuristic-based and ML-based routing algorithms. Figure 5 shows the results for the operation of 4 hours.

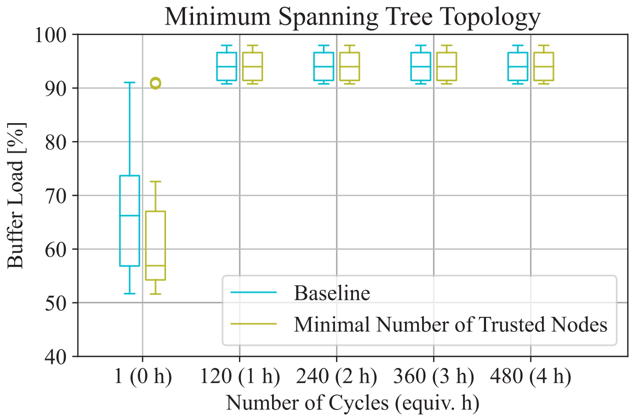

Fig. 4. Illustration of the buffer loads for the baseline and minimal deployment of trusted nodes. The key consumption rate allows one encrypted LP of 100 Gbps between any pair of nodes.

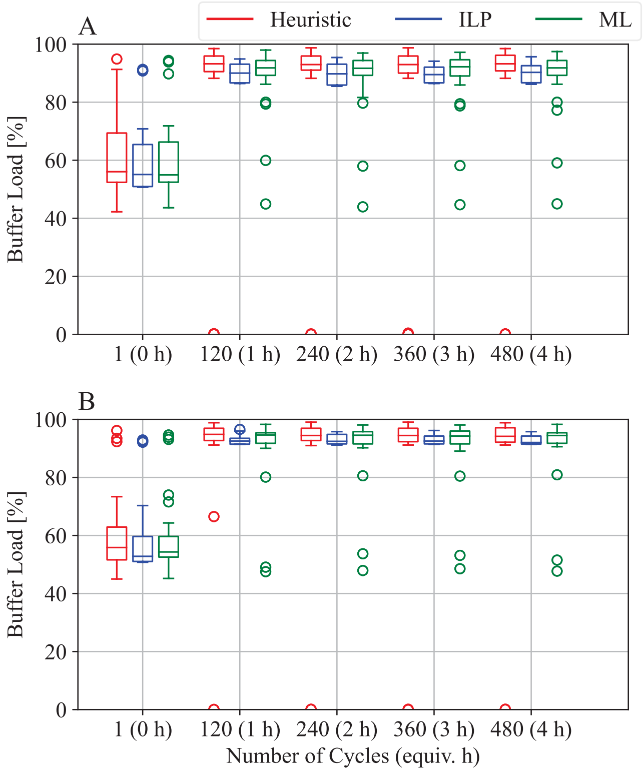

Fig. 5. A depicts the distribution of buffer loads for all three routing algorithms, baseline topology, and baseline deployment. B illustrates the distributions for the baseline topology, but the minimal deployment. In both graphs, the key consumption rate allows three encrypted LPs of 100 Gbps between any pair of nodes.

Both graphs show the distribution of the buffer load for the same key consumption rate of three LPs with a data rate of 100 Gbps, i.e., the overall bidirectional throughput equals 40.8 Tbps. There is no measurable gain in the baseline deployment of trusted nodes due to the increment's size of the key consumption rate. The minimal deployment of trusted nodes saves 14 QKD devices. Furthermore, the results show that the routing algorithms mainly differ in the least filled buffer's load. For all routing algorithms, most buffers have a load higher than 90 %. The least filled buffer has a load in the range of 0 %, 80 %, and 40 % for the heuristic- , ILP- , and ML- based algorithms, respectively. Only the latter two support the key consumption rate with the given deployment. The heuristic-based routing algorithm allows only one LP for both deployments. The analysis shows that a few edges are the driving factor for limiting the key consumption rate. Furthermore, the results indicate the importance of the optimal operation of the key management layer.

B. Heterogeneously Distributed Demands in a Multi-year Planning Scenario

After considering the same key consumption rate between any pair of nodes, we evaluate a more realistic demand distribution [7]. The overall bidirectional throughput in the initial year equals 14.21 Tbps. Regarding the QKDN deployment, we solely investigate the baseline topology because the minimum spanning tree topology can not cope with the derived key consumption rates. In the first step, we investigate the minimal deployment of trusted nodes for three consecutive years with an average traffic increase of 25 %. Figure 6 shows the distribution of the least filled buffer load for the first hour of operation. The first hour suffices to achieve a steady state.

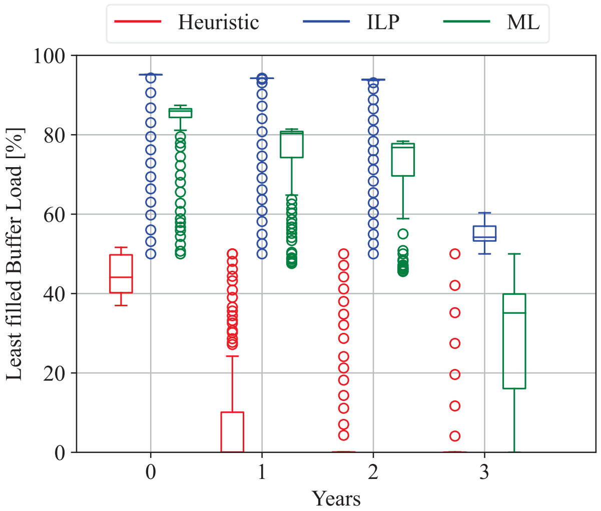

Fig. 6. Illustration of the least filled buffer load for the baseline topology and minimum deployment of trusted nodes in a multi-year planning scenario. The traffic increase leads to an increased key consumption rate and a reduced buffer load.

The results from Figure 6 underline the influence of the routing algorithm. Although the number of QKD devices and the demands are the same, only the ILP-based routing algorithm can support the key consumption rate within the first three years. Furthermore, Figure 6 indicates the increased performance of the ML-based routing algorithm compared to the heuristic-based one. The ML-based algorithm is suitable for the first two years without draining any buffer. The heuristic-based algorithm can only cope with the initial year. Considering the ILP- and ML-based algorithms, the first two years indicate an underutilized QKDN. For comparing the minimum with the baseline deployment of trusted nodes, the following Figure 7 shows the results for the first four years.

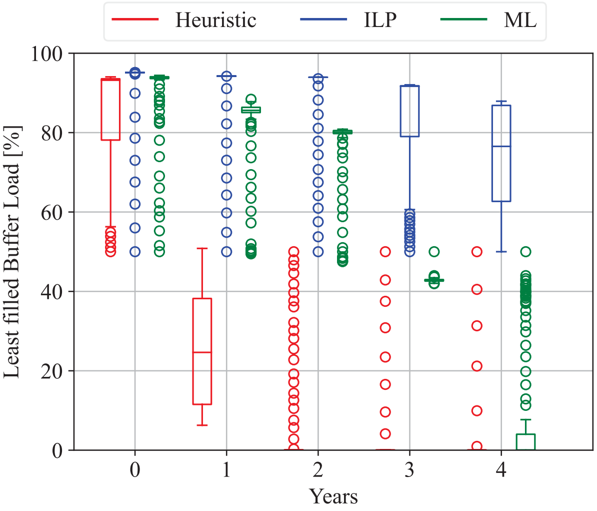

Fig. 7. Illustration of the least filled buffer load for the baseline topology and baseline deployment of trusted nodes in a multi-year planning scenario.

Figure 7 verifies the results of the previous analysis. Compared with the baseline deployment, the minimal deployment of trusted nodes can save up to 14 QKD devices without performance penalties within the first three years. The comparison shows the increased median of the least filled buffer load using the ILP-based routing algorithm. Median values above 90 % do not improve performance compared to median values higher than 50 %. The latter scenario is preferable due to the higher utilization of the QKDN. Assuming an optimal utilization of the QKDN by the KMN, the deployment of trusted nodes could be minimal for the first three years and, after that, extended by 14 QKD devices for the fourth year. However, none of the described deployments of trusted nodes satisfies the key consumption rates from the fifth year onward.

IV. Discussion

We have analyzed the multi-layer network design for applying QKD to optical DWDMNs. AES-256 was assumed for the encryption scheme. For key relaying, we assumed the OTP to combine the keys per span, corresponding to a bitwise XOR operation. Our study compared three different routing algorithms for KMN and two different trusted node deployment strategies. The optimal utilization of the QKDN by the key management layer, i.e., the ILP-based routing algorithm, can save up to 10 QKD devices for the analyzed topology. Additionally, it allows one further year of increased traffic served with keys from QKD. The findings indicate the importance of the optimal operation of such a multi-layer network. Furthermore, it shows the benefits of diverse routes compared to the minimum spanning tree deployment.

However, the optimization of the minimal trusted node deployment is small compared to the gain of the routing algorithm. As indicated by the multi-year scenario, the highest number of deployed QKD devices suffices at the most for the next four years. Hence, applying QKD to long-haul optical data transmission raises the question of how to extend the minimal deployment and be future-ready. The optimal extension of the QKDN to encrypt increased overall throughput is part of our future work.

References

[1] V. Hassija et al., “Present landscape of quantum computing,” IET Quantum Communication, vol. 1, no. 2, pp. 42–48, Dec. 2020, doi: 10.1049/iet-qtc.2020.0027.

[2] D. Ribezzo et al., “Deploying an Inter-European Quantum Network,” Adv Quantum Tech, p. 2200061, Dec. 2022, doi: 10.1002/qute.202200061.

[3] ITU-T Y.3800, Overview on networks supporting quantum key distribution, Dec. 2022.

[4] ITU-T Y.3803, Quantum key distribution networks - Key management, Dec. 2022.

[5] ITU-T Y.3807, Quantum key distribution networks - Quality of service paramters, Dec. 2022.

[6] ”DE CIX”, DE CIX Management, [Online], Available: https://www.decix.net/de/standorte/frankfurt/statistiken, [Accessed: 14-JAN-2023]

[7] S.K. Patri et al., ”Multi-Band Transparent Optical Network Planning Strategies for 6G-Ready European Networks,” Journal of Optical Fiber Technology, 2023.

[8] G. Savva et al., ”Quantum Key Distribution: An Optimization Approach for the Management Plane,” ICC 2022 - IEEE International Conference on Communications, pp. 5737–5743, May 2022, doi: 10.1109/ICC45855.2022.9838813.

[9] Q. Li et al., ”Mathematical model and topology evaluation of quantum key distribution network,” Optics Express, 28(7), p. 9419, 2020, doi: 10.1364/OE.387697.

[10] C. Yang et al., ”Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying”, China Communications, 15(2), pp. 33–45, Feb. 2018, doi: 10.1109/CC.2018.8300270.

[11] M. Wenning et al., ”Towards Optimized Demand Routing in QKD Networks,” Optical Fiber Communication Conference, Optica Publishing Group, 2023.

[12] National Institute of Standards and Technology, “Advanced encryption standard (AES),” National Institute of Standards and Technology, Gaithersburg, MD, NIST FIPS 197, Nov. 2001. doi: 10.6028/NIST.FIPS.197.

[13] X. Bonnetain et al., “Quantum Security Analysis of AES,” ToSC, pp. 55–93, Jun. 2019, doi: 10.46586/tosc.v2019.i2.55-93.

[14] A. Luykx et al., “Limits on authenticated encryption use in TLS,” Aug. 2017.

[15] C. E. Shannon, “Communication Theory of Secrecy Systems*,” Bell System Technical Journal, vol. 28, no. 4, pp. 656–715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[16] M. A. Ojewale et al., “Routing heuristics for load-balanced transmission in TSN-based networks,” SIGBED Rev., vol. 16, no. 4, pp. 20–25, Jan. 2020, doi: 10.1145/3378408.3378411.

[17] C. H. Bennett et al., “Quantum cryptography: Public key distribution and coin tossing,” 2020, doi: 10.48550/ARXIV.2003.06557.

[18] E. Diamanti, ”Security and implementation of differential phase shift quantum key distribution systems”, 2006.

[19] ”ID Quantique”, ID Quantique Products, [Online], Available: https://www.idquantique.com/quantum-safe-security/products/, [Accessed: 14-JAN-2023]

[20] ”PhyNWInfo”, Physical Network Information, [Online], Available: www.github.com/SaiPatri/PhyNWInfo, [Accessed: 14-JAN-2023]

[21] S. Krannig et al., ”How to design an optimized set of fibre-trees for filterless optical networks - The elegance of a multi-goal evolutionary Pareto optimization versus,” Photonic Networks, 17. ITG-Symposium, pp. 1-8, 2016.

[22] D. Stucki et al., “Long-term performance of the SwissQuantum quantum key distribution network in a field environment,” New J. Phys., vol. 13, no. 12, p. 123001, Dec. 2011, doi: 10.1088/1367-2630/13/12/123001.

[23] “SNDlib”, Zuse-Institute Berlin, [Online], Available: https://sndlib.zib.de, [Accessed: 14-JAN-2023].