Mixed Relay Placement for Quantum Key Distribution Chain Deployment over Optical Networks

Yuan Cao(1), Yongli Zhao(1), Jun Li(2), Rui Lin(2), Jie Zhang(1), Jiajia Chen(2)

(1) State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China, yonglizhao@bupt.edu.cn
(2) Department of Electrical Engineering, Chalmers University of Technology, 412 96 Gothenburg, Sweden, jiajiac@chalmers.se

Abstract *Four mixed trusted/untrusted relay placement strategies for quantum key distribution chain deployment over optical networks are proposed, which can improve a security level up to 119% relative to the conventional purely trusted relay placement.*

Introduction

Quantum key distribution (QKD) can offer future-proofed security to various applications, which is promising to be integrated with existing optical networks for massive deployment[1]. Recently, the feasibility of QKD coexisting with classical optical communications has been demonstrated in field trials[2],[3]. In practice, a large-scale QKD network usually consists of one or more QKD chains, where each QKD chain needs multiple relays between source and destination QKD backbone nodes (QBNs) for long reach. Proper relay placement ensures the success of QKD chain deployment. Conventionally, the trusted relay (TR) is adopted for QKD chain deployment over optical networks[3],[4]. By adding a number of TRs, a QKD chain can be extended to an arbitrary distance. However, the TRs are weak security points in a QKD network, since key information stops being in the quantum form and might be vulnerable to be eavesdropped at the TRs. In this regard, how to enhance the level of security for QKD chain deployment becomes a critical challenge.

Thanks to the invention of the measurement-device-independent QKD (MDI-QKD) scheme[5], the use of an untrusted relay (UR) to extend the reach of QKD becomes possible. An UR can close all loopholes on the measurement side, even if it is controlled by an eavesdropper. Thus, it has better security performance than the TR[6]. Nevertheless, using only the URs cannot extend QKD with arbitrary distance like the case using the TRs. The achievable distance by using the UR alone is limited to ~500 km with the state-of-the-art phase-encoding MDI-QKD protocol[7]. Therefore, the URs are expected to be placed together with the TRs for QKD chain deployment. To enhance the security level for QKD chain deployment over optical networks, we propose and evaluate four mixed TR/UR placement strategies. Simulations show their superiority over two conventional TR placement strategies.

Mixed relay placement problem

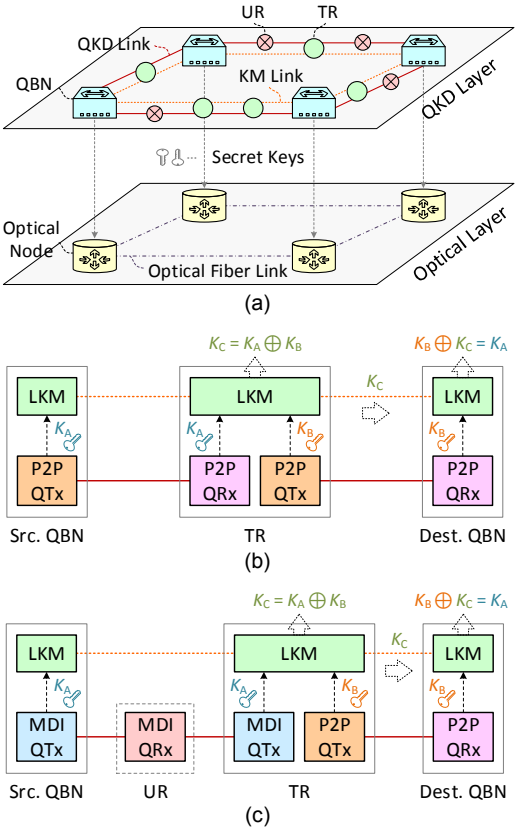

Fig. 1: (a) An architecture of QKD chain deployment over optical networks; (b) a QKD chain based on TRs; (c) a QKD chain based on mixed TRs/URs. [***QBN:*** *QKD backbone node;* ***TR:*** *trusted relay;* ***UR:*** *untrusted relay;* ***QTx:*** *QKD transmitter;* ***QRx:*** *QKD receiver;* ***LKM:*** *local key manager*]

An architecture of QKD chain deployment over optical networks is illustrated in Fig. 1(a), which is composed of QKD and optical layers. The optical layer is an existing optical network, which comprises multiple optical nodes interconnected via optical fiber links. The QKD layer consists of one or more QKD chains to be deployed over the optical layer, in which multiple QBNs are interconnected via QKD and key management (KM) links[8]. A QBN is co-located with an optical node to provide secret keys for optical layer security. A QKD link (including quantum and classical channels) connects QKD devices, i.e.,

QKD transmitter (QTx) and receiver (QRx), to generate the local secret keys (e.g., K_A and K_B in Fig. 1). The KM link via the classical channel connects local key managers (LKMs) to conduct key relay with the one-time pad method (i.e., perform a bitwise XOR operation) in a hop-by-hop fashion[8] for generating the global secret keys (e.g., K_A in Fig. 1) between the source and destination QBNs. To reduce the deployment complexity and cost, the QKD and KM links share the same fiber.

A conventional QKD chain is deployed based on multiple TRs, which is illustrated in Fig. 1(b). In the conventional TR placement, a TR contains a LKM and QKD devices that are based on point-to-point QKD (P2P-QKD) protocols such as BB84[2] and COW[3]. Thus, both QKD and KM links are required to connect the TRs.

A QKD chain based on mixed TRs/URs is shown in Fig. 1(c), which is deployed by placing and connecting multiple TRs and URs. In the mixed TR/UR placement, a TR can contain an LKM and different types of QKD devices that implement P2P-QKD or MDI-QKD protocols. P2P-QKD and MDI-QKD devices are compatible in a TR, since each segment used for key relay is independent. An UR only comprises QRxs based on the MDI-QKD protocol, since MDI-QKD generates the local secret keys between two connected QTxs with a QRx located in the middle[5]–[7]. Thus, only the QKD link is required to connect the UR. Notably, a TR can be placed at any point between two distant QBNs, while an UR can only be placed between the adjacent two TRs or a QBN and a TR under the distance limitation of the MDI-QKD.

Mixed relay placement strategies

The required number of relays for deploying a QKD chain is directly related to the distance between source and destination QBNs. During the deployment phase, the distance between any two adjacent relays (denoted by D) may be fixed or flexible. Two routing methods, *shortest-path* routing and *random-path* routing, are adopted. Based on the routing methods, the path for a QKD chain is selected, which passes through one or more physical links (note that a physical link connects two adjacent QBNs). To maximize the usage of the UR for high security level, all four proposed mixed TR/UR placement strategies have the UR and TR deployed in an interleaved manner. We also consider two ways to pass the intermediate QBNs, i.e., opaque and transparent. In the former one, both QKD and KM links are terminated in a TR located at the intermediate QBN; while in the later one, an optical switch instead of the TR facilitates bypassing the intermediate QBN. Our proposed four mixed

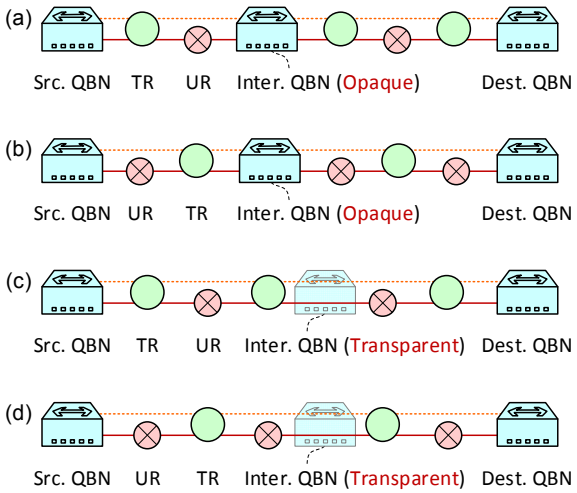

Fig. 2: (a) LTRF; (b) LURF; (c) PTRF; (d) PURF.

TR/UR placement strategies are depicted below.

- Link-based TR first (LTRF) in Fig. 2(a): The first relay is always a TR on each physical link and the intermediate QBNs have an opaque manner.
- Link-based UR first (LURF) in Fig. 2(b): The first relay is always an UR on each physical link and the intermediate QBNs have an opaque manner.
- Path-based TR first (PTRF) in Fig. 2(c): The first relay is always a TR on the selected path where the intermediate QBNs are transparent.
- Path-based UR first (PURF) in Fig. 2(d): The first relay is always an UR on the selected path where the intermediate QBNs are transparent.

Notably, the QBN must be a trusted node and it usually operates with the safeguard on duty, thus the TRs/URs at the source/destination or intermediate QBNs are not involved in the mixed TR/UR placement strategies. For a QKD chain with no intermediate QBN between its source and destination QBNs, the LTRF and LURF are the same as the PTRF and PURF, respectively. The set of multiple QKD chains to be deployed over an optical network is denoted by R. After performing the mixed TR/UR placement strategy for each QKD chain, the total required number of TRs (denoted by N_R) and URs can be computed. In particular, the security level of multiple QKD chains is defined as $|R|/N_R$.

Performance evaluation

The simulation uses a 14-node optical network topology (i.e., NSFNET with links of different lengths shown in [4]), over which multiple QKD chains will be deployed in an offline way. The source and destination QBNs of each QKD chain are randomly chosen from the 14 nodes in NSFNET. We assume that the wavelength resources are sufficient to accommodate the QKD and KM links of all QKD chains, such that each QKD chain can be successfully deployed.

Two conventional TR placement strategies are utilized for comparison, which are referred as link-based benchmark (LBM) and path-based benchmark (PBM) strategies. In the benchmark strategies, only TRs are placed for QKD chain deployment. Additionally, the simulation results are averaged with 100 times repetition.

Three cases are considered for performance evaluation: 1) *shortest-path* routing with a fixed value of *D*; 2) *random-path* routing with a fixed value of *D*; 3) *shortest-path* routing with a flexible value of *D*. In order to achieve a secret-key rate of kbps level and facilitate EDFA bypass, the relays can be placed approximately every 80 km (i.e., co-located with EDFAs in the optical network[4]) for a QKD chain. Thus, *D* = 80 km is used when a value of *D* is fixed. In addition, for the case with a flexible value of *D*, a typical span ranging from 80 to 100 km[2] is considered, in which the secret-key rate may be reduced compared to *D* = 80 km. The specific secret-key rate requirement of each QKD chain is not considered in this work. The number of TRs and security level versus the number of QKD chains in the three cases are plotted in Fig. 3.

As shown in Figs. 3(a)–3(c), the number of TRs shows approximately linear tendency as the number of QKD chains rises, which stems from the random chosen of source/destination QBNs for each QKD chain. From Figs. 3(d)–3(f) we can see that the security level basically keeps stable with the growing number of QKD chains, especially when the number of QKD chains is relatively large. This can be explainable based on the linear increase tendency shown in Figs. 3(a)–3(c). When using different routing methods, each relay placement strategy with the *shortest-path* routing shows lower number of TRs and higher security level than that with the *random-path* routing. It reflects that the randomness of routing sacrifices the security level. Besides, each relay placement strategy under *D* = 80 km shows larger number of TRs and lower security level than that under *D* ranging from 80 to 100 km. Thus, an increase in the secret-key rate leads to a decrease in the security level.

Moreover, it can be observed that the four mixed TR/UR placement strategies demonstrate similar relationships in the three cases. More specifically, the number of TRs for different strategies in a descending order is PTRF > LTRF > PURF > LURF. Correspondingly, the security level in a descending order is LURF > PURF > LTRF > PTRF. The LURF can show the highest security level among the four mixed TR/UR placement strategies. The link-based strategies slightly outperform the path-based strategies, because the opaque manner fully utilizes the secure TR resources at the intermediate QBNs. Moreover, the numbers of TRs (security levels) with the presented strategies are lower (higher) than that with the benchmark strategies. Notably, the security level enhancements of the presented strategies relative to the benchmark strategies are up to 118%, 114%, and 119% in the three cases, respectively.

Conclusions

This work devises four mixed TR/UR placement strategies aimed at enhancing the security level for QKD chain deployment over optical networks. Results show that the proposed strategies can achieve higher security level than the benchmark strategies (up to 119% security enhancement), where LURF shows the highest security level.

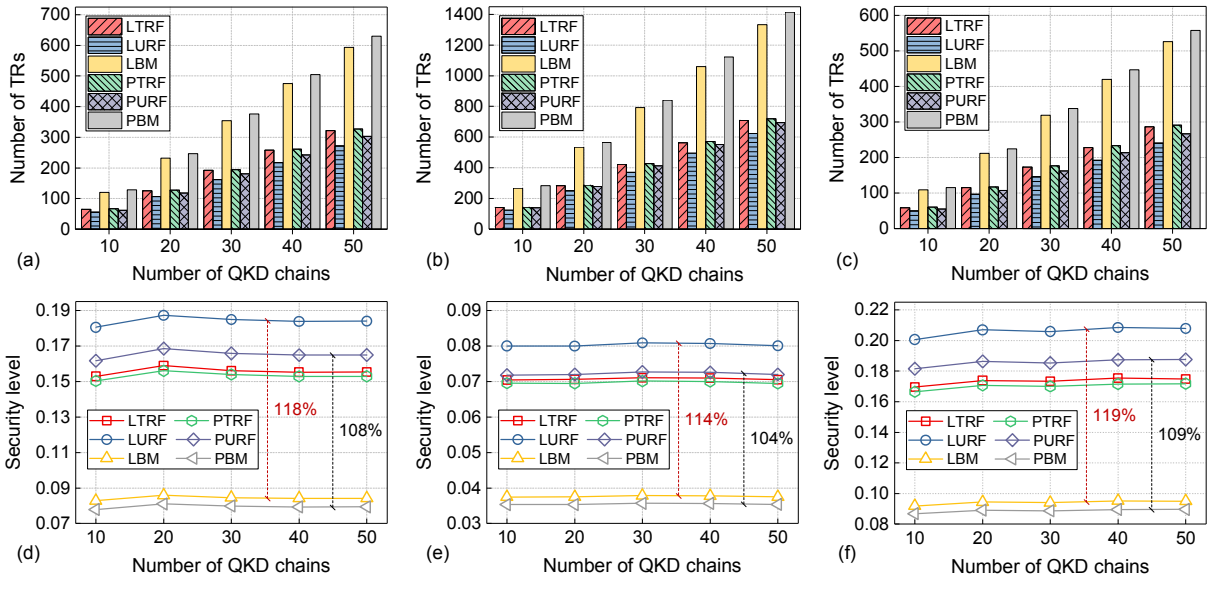

Fig. 3: Number of TRs and security level versus number of QKD chains: (a), (d) *shortest-path* routing with fixed *D* of 80 km; (b), (e) *random-path* routing with fixed *D* of 80 km; (c), (f) *shortest-path* routing with flexible *D* of 80–100 km.

Acknowledgements

National Key Research and Development Program of China (2019YFE020350), National Natural Science Foundation of China (61822105), Swedish Research Council, Swedish Foundation for Strategic Research, Swedish Foundation for International Collaboration in Research and Higher Education, and GENIE Project funded by the Chalmers University of Technology Foundation.

References

[1] Y. Cao *et al.*, "KaaS: Key as a service over quantum key distribution integrated optical networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 152–159, 2019.

[2] Y. Mao *et al.*, "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Express*, vol. 26, no. 5, pp. 6010–6020, 2018.

[3] A. Wonfor *et al.*, "Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5x100G DWDM transmission system," *Proc. ECOC*, Sept. 2019.

[4] Y. Cao *et al.*, "Cost-efficient quantum key distribution (QKD) over WDM networks," *J. Opt. Commun. Netw.*, vol. 11, no. 6, pp. 285–298, 2019.

[5] H.-K. Lo *et al.*, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, pp. 130503, 2012.

[6] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, no. 1, pp. 011024, 2016.

[7] X.-T. Fang *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," *Nature Photon.*, vol. 14, no. 7, pp. 422–425, 2020.

[8] "Overview on networks supporting quantum key distribution," Recommendation ITU-T Y.3800, Oct. 2019.