From Single-Protocol to Large-Scale Multi-Protocol Quantum Networks

Yuan Cao, Yongli Zhao, *Senior Member, IEEE,* Jie Zhang, Qin Wang, Dusit Niyato, *Fellow, IEEE,* and Lajos Hanzo, *Life Fellow, IEEE*

***Abstract*—In the initial stage of the quantum Internet, most of the practical quantum networks have been deployed relying on diverse individual quantum key distribution (QKD) protocols. However, this single-protocol paradigm cannot fulfill the heterogeneous requirements of the users, hence limiting the market-penetration of quantum networks. Given the recent advances in QKD protocols, the next generation quantum networks are expected to support both legacy and emerging QKD protocols. However, the evolution from single-protocol to multi-protocol quantum networks poses numerous challenging problems. As a remedy, we conceive a practical protocol translation framework for supporting this migration from single-protocol to large-scale multi-protocol quantum networks. Furthermore, we propose a programmable multi-functional relay node architecture for harmonizing the components of a suitable relay node. A pair of protocol translation policies are conceived for meeting the challenging security requirements of migration requests, which are compared to the single-protocol-based migration solutions both in terms of the translation success probability attained (i.e., the proportion of migration requests with successful protocol translation) and the average relaying risk probability encountered (i.e., the mean of the relaying risk probabilities of end-to-end key negotiation in a quantum network). Finally, we highlight a suite of open problems in both quantum secure direct communication and quantum teleportation for research into future multi-protocol quantum networks.**

I. Introduction

In the emerging quantum era, the rapid advances in quantum computing may render ubiquitous classical cryptographic algorithms, e.g., Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography, insecure in the near future. Hence, maintaining future-proof security is of utmost importance for the growing amount of sensitive information in a wide range of fields, such as government and finance. As an essential branch of quantum communications, quantum key distribution (QKD) [1] holds the promise of providing forward secrecy for users demanding long-term data security. In particular, QKD promises information-theoretic security based on the principles of quantum physics, which remains secure even in the face of quantum computers.

The compelling appeal of QKD is enabling symmetric secret key negotiation between a pair of legitimate users, which is typically implemented over a QKD link (e.g., an optical fiber or a free-space link) connecting the QKD transmitter (QTx) and the QKD receiver (QRx). Nevertheless, a single link can only support a few user pairs at the time of writing, thereby restricting the popularity of QKD. In order to guarantee security for network-wide users, a quantum network has to be constructed by numerous interconnecting QKD links. Over the past few years, an increasing number of quantum networks have been rolled out both in metropolitan and even long-haul scenarios [2]. In particular, an integrated space-to-ground quantum network has been reported in [3], covering fiber-based metropolitan and backbone quantum networks as well as satellite-ground QKD links. Hence, quantum networks have leaped out of the lab in support of practical applications by providing global secret keys for networked users, which may be considered as the initial stage for the development of the quantum Internet (Qinternet) [4].

To elaborate a little further, following the development of various QKD protocols (QKDPs), some practical quantum networks have been demonstrated. For example, the metropolitan quantum networks reported in [5] and [6] have been established based on the measurement-device-independent (MDI) and the Bennett-Brassard-Mermin-1992 (BBM92) protocols, respectively. Furthermore, the Cambridge-Ipswich [7] and the Beijing-Shanghai [3] intercity quantum networks can support the coherent-one-way (COW) and the Bennett-Brassard-1984 (BB84) protocols, respectively. In a nutshell, the existing field trials have demonstrated the feasibility of constructing quantum networks relying on diverse QKDPs, but they may not accommodate the wide range of requirements from different users, because each of these networks can only support a single QKDP.

Driven by the invention of various high-performance QKDPs, next generation quantum networks are expected to

This work was supported in part by National Key R&D Program of China (2020YFE0200600), NSFC (62150032, 62021005), Open Fund of State Key Laboratory of Advanced Optical Communication Systems and Networks (SJTU) (2022GZKF006), Open Fund of IPOC (BUPT), Natural Science Research Project of Jiangsu Higher Education Institutions (22KJB510007), and Natural Science Research Start-Up Foundation of Recruiting Talents of NUPT (NY221114). This research is supported in part by the National Research Foundation (NRF) and Infocomm Media Development Authority under the Future Communications Research & Development Programme (FCP) (FCP-NTU-RG-2021-014), under the AI Singapore Programme (AISG) (AISG2-RP-2020-019), and Singapore Ministry of Education (MOE) Tier 1 (RG16/20). L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/P034284/1 and EP/P003990/1 (COALESCE) as well as of the European Research Councils Advanced Fellow Grant QuantCom (789028).

Yuan Cao and Qin Wang are with the Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China (e-mail: yuancao@njupt.edu.cn; qinw@njupt.edu.cn).

Yongli Zhao and Jie Zhang are with the State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: yonglizhao@bupt.edu.cn; lgr24@bupt.edu.cn).

Dusit Niyato is with the School of Computer Science and Engineering, Nanyang Technological University, Singapore (e-mail: dniyato@ntu.edu.sg).

Lajos Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K. (e-mail: lh@ecs.soton.ac.uk).

QKD Family	Protocols	Features	Environments	Advantages	Limitations
SPM	BB84, GG02, DPS, SARG04, COW, etc.	QTx-QRx	Optical fiber Free space	High key rates High maturity	Relatively low security level Relatively low scalability
EB	E91, BBM92, etc.	QRx-QTx-QRx	Optical fiber Free space	High scalability High security level	Relatively low key rates Relatively low maturity
MDI	Original MDI, TF, etc.	QTx-QRx-QTx	Optical fiber Free space	Long distance High security level	Relatively low robustness Relatively low maturity

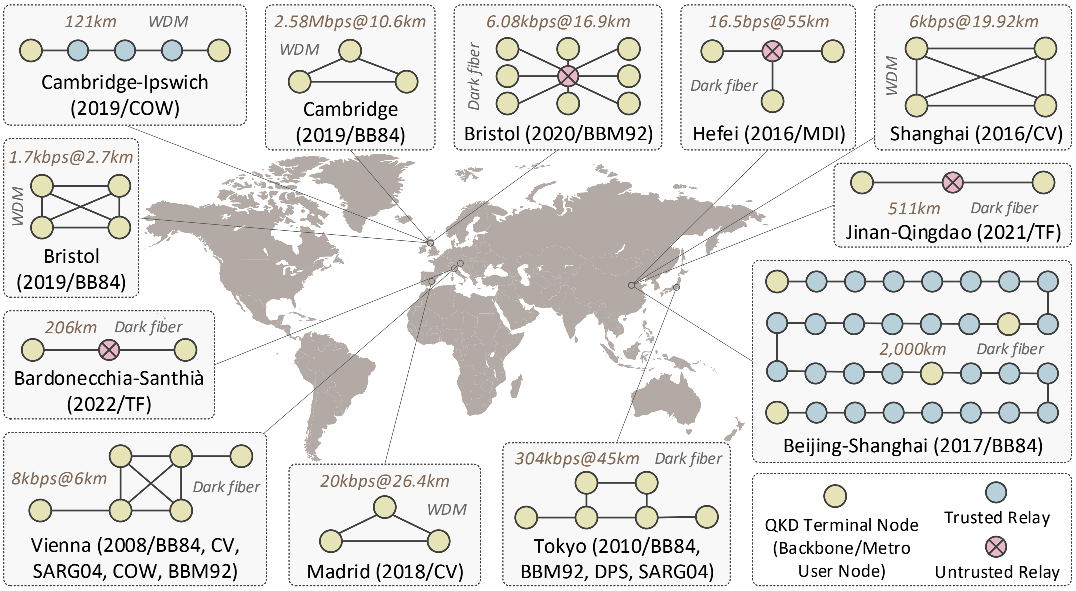

Fig. 1. **Diverse families of QKDPs and typical field trials of quantum networks around the world [2]. [SPM: Single-Prepare-and-Measure; EB: Entanglement-Based; MDI: Measurement-Device-Independent; QTx: QKD Transmitter; QRx: QKD Receiver; BB84: Bennett-Brassard-1984; GG02: Grosshans-Grangier-2002; DPS: Differential-Phase-Shift; SARG04: Scarani-Acín-Ribordy-Gisin-2004; COW: Coherent-One-Way; E91: Ekert-91; BBM92: Bennett-Brassard-Mermin-1992; CV: Continuous-Variable; TF: Twin-Field]**

cover a whole suite of both legacy and emerging QKDPs, aiming for operation in diverse network environments and secure application scenarios. Some preliminary studies have been performed for improving the system-level interoperability between different QKDPs, such as the conversion between the BB84 and MDI protocols [8], [9]. However, the design of multi-protocol quantum networks is still in its infancy. **At this early evolutionary stage, the migration from single-protocol to large-scale multi-protocol quantum networks is a critical open problem. To close this knowledge-gap, we propose a practical protocol translation framework, paving the way for the roll-out of large-scale quantum networks. The main contributions of this article are summarized below.**

1) **We propose both homogeneous and inhomogeneous protocol translation schemes to translate a single protocol into multiple protocols for long-haul QKD chains, where the network-layer interoperability of diverse QKDPs can be improved.**
2) **We present a programmable multi-functional relay node architecture for harmonizing the components of multi-protocol QKD chains, so that the protocol translation efficiency can be improved.**
3) We design a pair of protocol translation policies and compare them to the single-protocol-based solutions in the context of case studies.
4) We conclude with a range of open topics on incorporating protocols belonging to other branches of quantum communications into future large-scale multi-protocol quantum networks.

II. Typical QKD Protocols and Quantum Networks

A. QKD Protocols

A detailed review of QKDPs can be found in [1]. In 1984, Bennett and Brassard invented the first QKDP (known as the BB84 protocol), which has been widely employed in realistic QKD systems. Recently, a variety of sophisticated QKDPs have been proposed, one after another. Based on their physical characteristics, such as their encoding schemes, we can classify them into discrete-variable (DV) and continuous-variable (CV) QKDPs. In order to differentiate the QKD families in the network layer, we categorize them into single-prepare-and-measure (SPM), entanglement-based (EB), and MDI QKDPs, which are compared in Fig. 1.

To elaborate further, the SPM-QKDPs include but are not limited to the BB84, Grosshans-Grangier-2002 (GG02), and COW (2005) protocols. The local secret keys are generated between a pair of SPM-QTx and SPM-QRx. Furthermore, the family of MDI-QKDPs covers the original MDI protocol (2012) and the twin-field (TF) protocol (2018), where the local

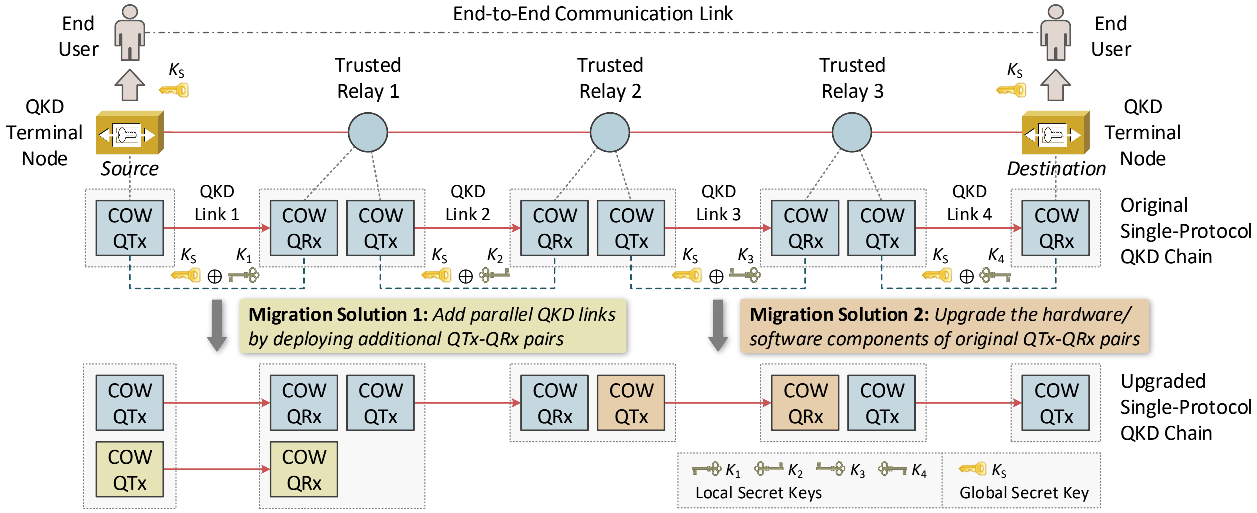
End-to-End Communication Link
End User
End User
K_S
K_S
QKD Terminal Node
Source
QKD Terminal Node
Destination
Trusted Relay 1
Trusted Relay 2
Trusted Relay 3
QKD Link 1
QKD Link 2
QKD Link 3
QKD Link 4
COW QTx
COW QRx
K_S ⊕ K_1
K_S ⊕ K_2
K_S ⊕ K_3
K_S ⊕ K_4
Original Single-Protocol QKD Chain
Migration Solution 1: Add parallel QKD links by deploying additional QTx-QRx pairs
Migration Solution 2: Upgrade the hardware/ software components of original QTx-QRx pairs
Upgraded Single-Protocol QKD Chain
K_1 K_2 K_3 K_4 Local Secret Keys
K_S Global Secret Key

Fig. 2. Illustration of the realistic single-protocol intercity quantum network [7] and single-protocol-based quantum network migration solutions.

secret keys are shared between a pair of MDI-QTxs associated with an MDI-QRx in the middle for performing interference measurement. By contrast, the class of EB-QKDPs comprises the Ekert-91 (E91) and the BBM92 protocols. The local secret keys are derived between a pair of EB-QRxs relying on an intermediate EB-QTx for distributing the entangled states (e.g., entangled photon pairs). Notably, the EB-QKDPs and MDI-QKDPs can eliminate attacks on the source and detector sides, respectively, hence they promise higher realistic security than the SPM-QKDPs.

In view of their different technical solutions and maturity, various QKDPs exhibit different performances. For example, the TF protocol has achieved a QKD distance record of 833.8 km in the lab at the time of writing [10]. In [11], a secret key rate of 13.72 Mb/s was realized over a 10 km standard fiber having an attenuation of 2 dB by relying on the BB84 protocol. In addition to the employment of a single protocol in a standalone system, the interoperability of different QKDPs in a system has attracted much attention. Roberts *et al.* [8] and Fan-Yuan *et al.* [9] implemented agile switching between the BB84 and MDI protocols. These efforts have confirmed the feasibility of combining multiple QKDPs to achieve high security levels, while satisfying different requirements.

In contrast to the family of software-based mailing service protocols (e.g., SMTP/POP3/IMAP), multiple QKDPs belong to the class of point-to-point protocols relying on a diverse variety of physical implementations, but their functions are the same, namely providing secret keys. The protocol translation schemes conceived for both mailing service protocols and QKDPs can be designed to address the associated multi-user requirements in diverse application scenarios, where the interoperability should be improved. However, the constraints imposed on the translation schemes of the mailing service protocols and QKDPs are rather different. In particular, the protocol translation schemes designed for QKDPs have to consider the constraints of the different connection features of QTx and QRx as well as both the advantages and limitations of the QKDPs, as illustrated in Fig. 1.

B. Quantum Networks

A comprehensive survey of quantum networks can be found in [2]. Since the first quantum access network demonstrated by the 1997 UK lab experiment, more and more quantum networks have been deployed and tested in the field. Figure 1 displays some typical field trials of quantum networks around the world. With respect to the preliminary tests of QKD systems using different protocols in metropolitan networks, six-node quantum networks were demonstrated in Vienna (2008) and Tokyo (2010), respectively. During that era, the MDI-QKDP (note that the first MDI protocol was invented in 2012) had not been proposed. The appeal of the early quantum networks was limited owing to the small network size and the immature QKDPs.

In recent years, more sophisticated QKDPs have been deployed in realistic metro networks, such as the MDI quantum network in Hefei (2016), the CV quantum networks in Shanghai (2016) and Madrid (2018), the BB84 quantum networks in Bristol (2019) and Cambridge (2019), as well as the BBM92 quantum network in Bristol (2020). Furthermore, the Beijing-Shanghai BB84 quantum network (2017), the Cambridge-Ipswich COW quantum network (2019), as well as the Jinan-Qingdao (2021) and **Bardonecchia-Santhià** (2022) TF quantum networks have been demonstrated in long-haul scenarios. Hence, the feasibility of deploying practical quantum networks relying on diverse protocols has indeed been confirmed, but most of the practical networks rely on a single QKDP at the time of writing.

As shown in Fig. 1, the operational QKDPs exhibit different features, advantages, and limitations, since they rely on diverse protocols exhibiting different performances. For example, although the BB84 protocol was invented about 40 years ago, it is still capable of attaining higher key rates than many of the more recent QKDPs [11]. By contrast, the MDI/BBM92 schemes exhibit higher security level.

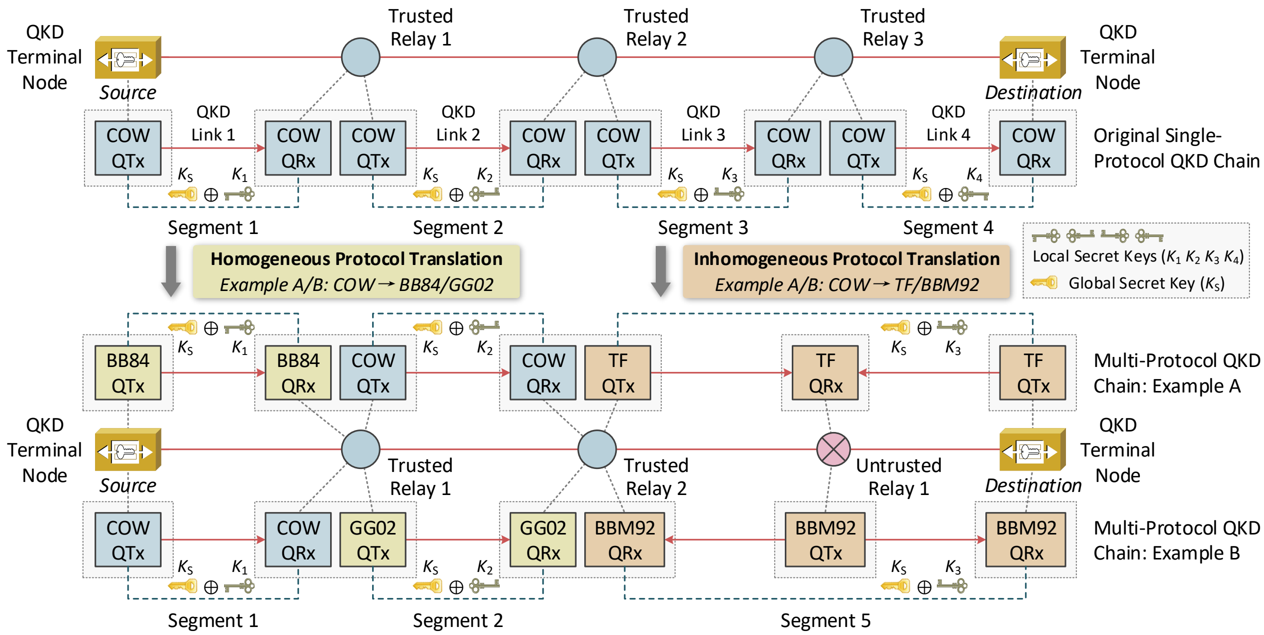

Fig. 3. Illustration of homogeneous and inhomogeneous protocol translation from single-protocol to multi-protocol QKD chains.

Clearly, developing a single QKDP standard for large-scale high-performance quantum networks is an extremely challenging task. In the interim, heterogeneous QKDPs can be interconnected to establish a large-scale multi-protocol quantum network for supporting end-to-end key negotiation between any pair of remote nodes. In this regard, ITU-T is developing standards for supporting the interworking of multiple quantum networks. Even though a few early studies have demonstrated the coexistence of different QKDPs in small-scale metropolitan quantum networks, the interoperability of multiple QKDPs in large-scale quantum networks is still a challenging problem at the time of writing.

III. Protocol Translation Framework

A. Single-Protocol-Based Quantum Network Migration

In a large-scale quantum network, one or more QKD chains can be established for end-to-end key negotiation for securing end-to-end communications. The so-called QKD chain is constituted by chaining the QTx and QRx along the path spanning from the source to destination nodes via the QKD links, as will be detailed hereinafter. The QKD terminal node is also referred to as the backbone/metro user node. We utilize the realistic single-protocol intercity quantum network of Fig. 2 for illustrating single-protocol-based quantum network migration solutions, located in Cambridge and Ipswich, respectively, with three trusted relays placed in between [7]. A pair of COW-QTx and COW-QRx are connected via a QKD link for point-to-point key negotiation. Typically, the QKD link contains the quantum channel for exchanging quantum signals, as well as the classical channel for carrying out several classical functions such as synchronization and key distillation [1], but these may be accommodated by the same fiber using WDM. The COW-QTx and COW-QRx along the path from source to destination are connected by QKD links to form a single-protocol QKD chain. In practice, a large-scale single-protocol quantum network may contain one or more single-protocol QKD chains.

In long-haul scenarios, the length of a single constituent QKD link is limited, since the quantum signals must not be amplified, otherwise the quantum signal collapses to the classical domain. Given that fully-fledged quantum repeaters [4] are still not available at the time of writing, trusted relays are used as a compromise for end-to-end key negotiation between the source and destination in the classical domain. The global secret keys generated may then be utilized for securing communications between end users who are in the same physical location as the associated QKD terminal nodes. Given that the COW protocol belongs to the SPM-QKD family, the local secret keys are derived between a pair of COW-QTx and COW-QRx, as exemplified in Fig. 2. A global secret key is forwarded from the source to destination by relying on hop-by-hop encryption/decryption, whose details can be found in ITU-T Y.3803. The global key relaying process is performed in the classical domain, where the encryption and decryption phases employ a so-called one-time pad algorithm for carrying out a bitwise exclusive OR operation between the global and local secret keys of the same string length, aiming for maintaining information-theoretic security of the secret keys. However, each trusted relay has knowledge of the global secret keys, hence the security of trusted relays relies on the assumption that the relay is fully trustworthy and it cannot be accessed by eavesdroppers.

As for the single-protocol-based quantum network migration solutions, the original QKDP is still adopted during the migration period, hence the upgraded QKD chain remains a single-protocol QKD chain. Typically, the goal of upgrading such a QKD chain is to satisfy higher secret key rate requirements.

As depicted in Fig. 2, the operator may find some QKD links in the QKD chain that cannot meet the growing secret key rate requirements. Hence they may select one of two optional solutions, namely adding parallel QKD links by deploying additional QTx-QRx pairs, or upgrading the hardware/software components of the original QTx-QRx pairs. The former solution requires more bandwidth for additional QKD links, while the latter solution has to rely on the maturity of the associated single-protocol QKD systems. Accordingly, the performance of each QKD chain is bound to a single QKDP, resulting in the challenge of satisfying different security requirements. In particular, each node/relay along the path of a long-haul QKD chain may support several metropolitan quantum networks. However, the single-protocol-based quantum network migration solutions may fail to accommodate different metro network requirements and environments.

B. *Homogeneous and Inhomogeneous Protocol Translation*

The single-protocol-based migration solutions constitute a beneficial evolutionary stepping-stone, but they fail to fully leverage the multi-fold advantages of different protocols. By contrast, invoking a combination of multiple QKDPs may provide complementary benefits. For example, each protocol belonging to the MDI/EB-QKD family may rely on an untrusted relay for improving security, but arranging for the seamless interworking of different QKD systems is quite a challenge. In order to operate multiple QKDPs based on the original single-protocol quantum network, sophisticated translation is required. Explicitly, the protocol translation is defined as translating the original QKDP used in one or more segments of a QKD chain into the target QKDP, aiming for improving the network-layer interoperability of diverse QKDPs.

Several examples of potential protocol translations are depicted in Fig. 3. **We differentiate the segments of a QKD chain based on the features of SPM, EB, and MDI QKD.** More concretely, recall that a segment corresponding to a QKD link connects a pair of SPM-QTx and SPM-QRx. For the MDI-QKDP, a segment connects a pair of MDI-QTxs with an MDI-QRx in between, which is associated with two QKD links. Additionally, a segment connects a pair of EB-QRxs with an EB-QTx in the middle, which also involves two QKD links. It can be observed that the quantum signal transmission direction and the number of QKD links required may be different for various segments. Hence, the protocol translation is performed in units of segments.

Based on the aforementioned segments, we propose a pair of protocol translation schemes, namely *a homogeneous and an inhomogeneous protocol translation*. The concept of homogeneous protocol translation is that the original and target QKDPs during the translation phase belong to the same QKD family. As depicted in Fig. 3, a COW segment can be translated into a BB84 segment or a GG02 segment in a multi-protocol QKD chain. This translation scheme also incorporates the above-mentioned single-protocol-based quantum network migration solutions. On the other hand, the concept of inhomogeneous protocol translation is that the original and target QKDPs during the translation phase belong to different QKD families. For instance, two COW segments can be translated into a TF segment or a BBM92 segment, as shown in Fig. 3.

In particular, the TF/BBM92 segment allows the employment of an untrusted relay, since the TF and BBM92 protocols belong to the class of MDI-QKD and EB-QKD, respectively. The untrusted relay does not rely on any security-related assumptions, whose security cannot be compromised even in the presence of an attacker, because it is secured by robust protocols exploiting the physical nature of MDI/EB-QKD. Hence, again, an untrusted relay exhibits better security than a trusted relay, and it is typically composed of the MDI-QRx or the EB-QTx. An MDI-QRx is utilized for the measurement (e.g., two-photon interference [1]) of quantum signals from a pair of MDI-QTxs, while an EB-QTx is employed for distributing the entangled states to a pair of EB-QRxs. The local secret keys are derived by negotiation between a pair of connected MDI-QTxs or EB-QRxs. **Further details concerning the family of untrusted relays in specific QKDPs can be found in [1], [2].**

The nature of MDI/EB-QKDPs does not permit the direct connection of a pair untrusted relays without any intermediate nodes. In long-haul scenarios, the achievable distance of a QKD chain relying on a single untrusted relay is limited. Such a specific QKD chain can be found both in the 511 km Jinan-Qingdao (2021) and in the 206 km **Bardonecchia-Santhià** (2022) TF quantum networks. Hence, an untrusted relay is expected to be combined with a trusted relay for extending the end-to-end key negotiation distance, as depicted in Fig. 3, where the untrusted relay does not have access to the real secret keys and the global key relaying process of a multi-protocol QKD chain is similar to that of a single-protocol QKD chain.

In practice, several benefits can be gleaned from protocol translation. For homogeneous protocol translation, the QKD transceivers relying on more suitable/advanced QKDPs can be utilized to meet the growing secret key rate demands. For example, a QKDP exhibiting relatively high secret key rates over long distances may in fact have lower secret key rates over short distances, than their specifically-designed short-range counterparts. Compared to the single-protocol-based migration solutions, homogeneous protocol translation may reduce the upgrading cost or difficulty. Furthermore, specific

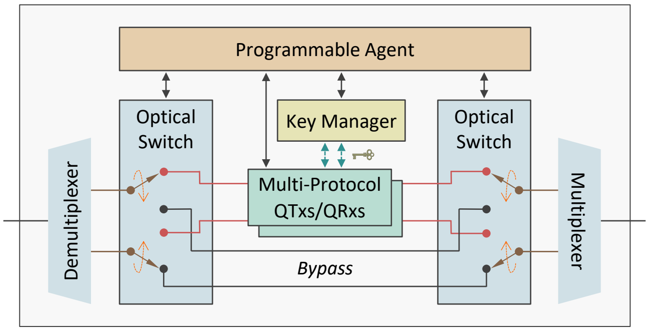

Fig. 4. Illustration of a programmable multi-functional relay node architecture.

benefits can be obtained for QKD chains by performing inhomogeneous protocol translation, such as improving the security level and reducing the relaying risk probability of end-to-end key negotiation by relying on MDI/EB-QKD-based untrusted relays.

C. Multi-Functional Relay Node Architecture

In a large-scale quantum network, a relay node might be shared by one or more QKD chains, since the QTxs/QRxs along the intersections of different QKD chains may be enclosed in the same physical location. Furthermore, after protocol translation, QTxs/QRxs based on the original protocol can be retained in the relay node to cope with the future requirements of other QKD chains, or combined with the target protocol-based QTxs/QRxs for enhancing the performance of the associated multi-protocol QKD chain. Hence, a relay node may assume multiple roles for different QKD chains. To harmonize the diverse components of such a relay node as well as facilitate the homogeneous and inhomogeneous protocol translation, Figure 4 illustrates a programmable multi-functional relay node architecture, which consists of the programmable agent, the key manager, multi-protocol QTxs/QRxs, optical switches, and multiplexers/demultiplexers.

The multi-protocol QTxs/QRxs identify whether the relay node acts as an untrusted or a trusted relay dedicated to a QKD chain. For example, a relay node formed by the MDI-QRx or EB-QTx acts as an untrusted relay, while the SPM-QTx/QRx, MDI-QTx, or EB-QRx harnesses the relay node as a trusted relay. Additionally, the relay node between a pair of connected nodes within a relatively short distance can be bypassed, which is implemented by the optical switch. More concretely, the optical switch enables the on-demand bypassing of its relay node, and facilitates the flexible switching of quantum channels, as well as the dynamic interconnection of QTxs/QRxs between adjacent nodes. The key manager stores and manages the secret keys derived from multi-protocol QTxs/QRxs (covering the SPM-QTx, SPM-QRx, MDI-QTx, and EB-QRx), as well as supports key relaying, when the relay node functions as a trusted relay. The MDI-QRx or EB-QTx is not connected to the key manager, since it does not access the real secret keys. The multiplexers/demultiplexers are employed to bundle/separate multiple quantum and classical channels.

Finally, the above components are controlled and configured by a programmable agent. This agent is capable of communicating with each component, instructing it through a control interface, as well as achieving the dynamic adjustment of these components to fulfill the specific requirements of multi-protocol QKD chains. In conclusion, the protocol translation efficiency can be improved with the aid of the programmable agent.

IV. Protocol Translation Policies

A. Policy Description

In real-world applications, different protocol translation objectives may be considered for a QKD chain to fulfill the requirements of diverse users, such as increasing the global secret key rate and improving the security level of global secret keys. Here, we focus on two types of security requirements, namely providing global secret keys having different security levels and reducing the relaying risk probability of global secret keys. The former is influenced by the realistic security level of the entire QKD system, while the latter is subject to the trustworthiness of relays. To satisfy these security requirements, we design a chain-based and a segment-based protocol translation policy, which are shown in Fig. 5. **Both protocol translation policies can be applied by a centralized software-defined network controller [2].** The migration requests of the original single-protocol QKD chains are handled one by one. Given that the connection of QTxs/QRxs is fixed for establishing the original QKD chain, the path spanning from the source to destination is identified. It is important to note that different original QKD chains may share the same paths and relay nodes, but their QTxs/QRxs are independent. **To strike a compelling trade-off between the price of and the demand for QKD devices, we can aim for the on-demand deployment of target protocol-based QTxs/QRxs while retaining the QTxs/QRxs relying on their original protocol. This trade-off also has to be further imroved in support of large-scale multi-protocol quantum networks. Meanwhile, chip-based multi-protocol QTxs/QRxs can be further developed to reduce the associated costs [2].**

In the chain-based protocol translation policy, the original and target security levels are identified based on the associated security requirements. For example, the global secret keys

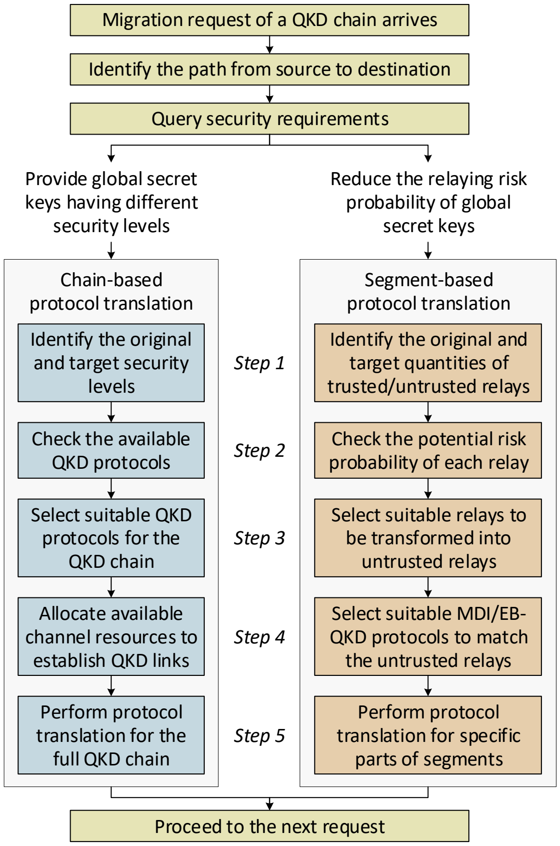
Migration request of a QKD chain arrives
Identify the path from source to destination
Query security requirements
Provide global secret keys having different security levels
Reduce the relaying risk probability of global secret keys
Chain-based protocol translation
Segment-based protocol translation
Identify the original and target security levels
Step 1
Identify the original and target quantities of trusted/untrusted relays
Check the available QKD protocols
Step 2
Check the potential risk probability of each relay
Select suitable QKD protocols for the QKD chain
Step 3
Select suitable relays to be transformed into untrusted relays
Allocate available channel resources to establish QKD links
Step 4
Select suitable MDI/EB-QKD protocols to match the untrusted relays
Perform protocol translation for the full QKD chain
Step 5
Perform protocol translation for specific parts of segments
Proceed to the next request

Fig. 5. Two protocol translation policies for different security requirements.

derived from the single-protocol QKD chain illustrated in Fig. 3 only have the original security level of SPM. The target security levels may incorporate the security levels of MDI and EB having improved realistic security. The secret keys having different security levels can be utilized for securing both data and control channels. After checking the available QKDPs, the most suitable QKDPs are selected for the QKD chain. If the original QKDP is retained, the QTxs and QRxs based on the target QKDP have to be connected through additional QKD links. Hence the available channel resources are allocated for establishing the associated QKD links relying on a so-called first-fit algorithm defined in [2]. The chain-based protocol translation is performed for all segments in the full QKD chain.

In the segment-based protocol translation policy, the original and target quantities of trusted/untrusted relays are identified according to the specifically queried security requirements. The original single-protocol QKD chain typically consists of purely trusted relays. In practice, the potential risk probability of a relay varies from 0 to 1, but it is 0 for an untrusted relay, because the untrusted relay is always secure against any attacks. Notably, the methods for obtaining this probability for each trusted relay and ensuring its accuracy have to be further explored. The potential risk probability of each relay in the original QKD chain is checked, based on which the suitable relays are selected to be transformed into untrusted relays, where the relay transformation should obey that untrusted relays must not be directly connected. Furthermore, suitable QKDPs belonging to the MDI/EB-QKD class are selected to match the untrusted relays. For example, the most suitable relay for transformation may have a relatively high potential risk probability, while the most suitable protocol may exhibit high key rates or low costs. The segment-based protocol translation is performed for specific parts of segments in the QKD chain.

B. Case Studies

Simulations were conducted for evaluating the policies designed. The Beijing-Shanghai BB84 quantum network topology [3] was adopted, which comprises four QKD terminal nodes and 28 trusted relays, as shown in Fig. 1. We assume that 12 BB84-QKD chains have been randomly established between the QKD terminal nodes for satisfying the secret key demands of legacy and future users. Then we set the number of migration requests to the interval [1, 12]. The channel resources available for establishing additional QKD links are fixed to 12, while the channel requirements per QKD link are set to 2 (i.e., one for quantum signal exchange and one for synchronization, the other classical functions are implemented over public classical networks). Each QKD terminal node has to be fully trustworthy, and the potential risk probability of each trusted relay is assumed to be 1%. As illustrated in Fig. 6, four cases are defined based on the above two security requirements, where the global secret key rate requirements are not considered. **The translation success probability is defined as the ratio of the number of successful and the total number of translation requests. The average relaying risk probability is obtained by averaging the relaying risk probability (depending on the number of trusted relays and the potential risk probability of each trusted relay) of the QKD chains after protocol translation.** The average value each point is obtained from 1000 simulation repetitions.

Cases	Policies	Parameters
Case I	Chain-based	Two security levels: SPM, MDI (or EB)
Case II	Chain-based	Three security levels: SPM, MDI, EB
Case III	Segment-based	Trusted relay reduction: [1, 25% of the total in a chain]
Case IV	Segment-based	Trusted relay reduction: [1, 50% of the total in a chain]

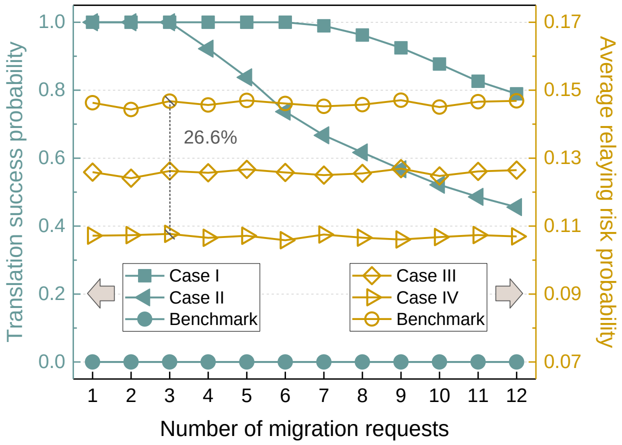

Fig. 6. **Translation success probability and average relaying risk probability versus the number of migration requests for QKD chains in four cases. (The number "1" in Cases III and IV indicates the reduction by one trusted relay; The single-protocol-based migration solutions are utilized as the benchmarkers)**

Figure 6 plots the translation success probability and average relaying risk probability versus the number of migration requests. The translation success probability is unity for <=**3** migration requests, but then decreases with the growing number of migration requests. This is because the proliferating migration requests associated with different security levels cannot be fully accommodated by the limited channel resources. Furthermore, the translation success probability in Case II is lower than that in Case I, since the total security levels are increased from 2 to 3. The translation success probability for the benchmark is 0, reflecting that the single-protocol-based migration solutions fail to satisfy the associated security requirements. For the segment-based protocol translation policy, it can be observed that the average relaying risk probability basically remains unaffected by the number of migration requests, since all the migration requests are successfully accommodated. This is supported by performing protocol translation based on the original QKD links. The average relaying risk probability of Case IV in Fig. 6 is lower than that of Case III, which stems from the relatively large proportion of trusted relay reduction required in Case IV. Specifically, the average relaying risk probability reduction of the segment-based policy can reach 26.6% relative to the benchmark, validating the benefits of translating a single BB84 protocol into different MDI/EB-QKDPs. Hence, our chain- and segment-based protocol translation policies are eminently suitable for fulfilling the security requirements of migration requests defined for the QKD chains.

V. Multi-Protocol Quantum Networks Beyond QKD: Open Issues and Challenges

This article intends to facilitate the migration from single-protocol to multi-protocol quantum networks through protocol translation. Apart from our basic policies mentioned above, a suite of more sophisticated policies can also be conceived for satisfying diverse requirements. On the road to the Qinternet [2], [4], [12]–[14], QKD has become a commercial reality. **Guided by the roadmap of [14] - including an OSI-alike layering model and cluster-based structure - the emergence of a large-scale wide-area Qinternet can be foreseen. However, the most suitable protocol designs have to be further studied.** Beyond QKD, large-scale multi-protocol quantum networks may incorporate other quantum-domain protocols, as discussed below.

Quantum Secure Direct Communication (QSDC) enables direct information transfer via the quantum channel, whose information-theoretic security is promised without any prior secret key negotiation. Furthermore, QSDC is promising for constructing a secure repeater network [13], which creates an evolutionary path for the Qinternet. Numerous promising QSDC protocols have been proposed, paving the way for their ultimate incorporation into multi-protocol quantum networks, where their collaboration with QKDPs requires further investigations.

Quantum Teleportation achieves the secure transfer of quantum information between distant sites based on the action of quantum entanglement [12], which can provide end-to-end information-theoretic security relying on fully-fledged quantum repeaters. **Given the inevitable decoherence and volatile storage of entangled pairs, the protocol design of long-distance entanglement distribution plays a pivotal role in quantum networks. In [15], a connection-oriented protocol design was proposed for facilitating the development of quantum teleportation, where the associated real-time resource allocation and the provision of end-to-end rate guarantees were addressed.** From a global perspective, quantum teleportation requires substantial further research before the pervasice roll-out of multi-protocol quantum networks.

In reality, different branches of quantum communications have different pros and cons in the heterogeneous application scenarios and evolutionary stages of the Qinternet. **They are expected to cooperate with each other in the construction of ultimately secure large-scale multi-protocol quantum networks. However, harmonized standardization efforts are required for ensuring the compatibility of components based on heterogeneous protocols.**

VI. Conclusions

Protocol translation supports migration from single-protocol to large-scale multi-protocol quantum networks. We proposed both homogeneous and inhomogeneous protocol translation schemes for long-haul QKD chains for translating a single protocol into multiple protocols in units of segments. We described a programmable multi-functional relay node architecture for harmonizing diverse components in a relay node for multi-protocol QKD chains. To deliver global secret keys having different security levels and reduce the relaying risk probability of global secret keys, we designed the chain- and segment-based protocol translation policies, respectively. Our case studies demonstrated the superiority of the policies designed over the single-protocol-based migration solutions. Beyond QKD, QSDC and quantum teleportation have to be further developed into secure practical applications, and their quantum-domain protocols are expected to be incorporated in future large-scale multi-protocol quantum networks to pave the way for the Qinternet. **Do join this frontier-research based community effort valued Colleague, where there is substantial 'head-room' for high-impact research into what might assume the fond connotation of 'Communications V 2.0'.**

References

[1] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, no. 4, pp. 1012–1236, Dec. 2020.

[2] Y. Cao *et al.*, "The evolution of quantum key distribution networks: On the road to the Qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart. 2022.

[3] Y.-A. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, Jan. 2021.

[4] S. Wehner *et al.*, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, Oct. 2018, Art. no. eaam9288.

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

[6] S. K. Joshi *et al.*, "A trusted node-free eight-user metropolitan quantum communication network," *Sci. Adv.*, vol. 6, no. 36, Sept. 2020, Art. no. eaba0959.

[7] A. Wonfor *et al.*, "Field trial of multi-node, coherent-one-way quantum key distribution with encrypted 5x100G DWDM transmission system," in *Proc. Eur. Conf. Opt. Commun.*, Dublin, Ireland, Sept. 2019.

[8] G. L. Roberts *et al.*, "Experimental measurement-device-independent quantum digital signatures," *Nature Commun.*, vol. 8, Oct. 2017, Art. no. 1098.

[9] G.-J. Fan-Yuan *et al.*, "Measurement-device-independent quantum key distribution for nonstandalone networks," *Photonics Res.*, vol. 9, no. 10, pp. 1881–1891, Oct. 2021.

[10] S. Wang *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature Photon.*, vol. 16, no. 2, pp. 154–161, Feb. 2022.

[11] Z. Yuan *et al.*, "10-Mb/s quantum key distribution," *J. Lightwave Technol.*, vol. 36, no. 16, pp. 3427–3433, Aug. 2018.

[12] A. S. Cacciapuoti *et al.*, "When entanglement meets classical communications: Quantum teleportation for the quantum Internet," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3808–3833, June 2020.

[13] G.-L. Long *et al.*, "An evolutionary pathway for the quantum Internet relying on secure classical repeaters," arXiv: 2202.03619, 2022.

[14] Z. Li *et al.*, "Building a large-scale and wide-area quantum Internet based on an OSI-alike model," *China Commun.*, vol. 18, no. 10, pp. 1–14, Oct. 2021.

[15] J. Li *et al.*, "A connection-oriented entanglement distribution design in quantum networks," *IEEE Trans. Quantum Engineering*, vol. 3, June 2022, Art. no. 4100513.

Yuan Cao received the Ph.D. degree from Beijing University of Posts and Telecommunications (BUPT) in 2021. During June-August 2018 and June-August 2019, he was an Academic Visitor with the KTH and University of Southampton, respectively. He is currently a Lecturer with Nanjing University of Posts and Telecommunications (NUPT). His research focuses on quantum communications and networking.

Yongli Zhao [SM'15] received the Ph.D. degree from BUPT in 2010. From January 2016 to January 2017, he was a Visiting Associate Professor with the University of California, Davis. He is currently a Professor with BUPT and a Fellow of the IET. His research focuses on quantum networks, optical networks and machine learning.

Jie Zhang received the Ph.D. degree from BUPT in 1998. He is currently a Professor and the Dean of the School of Electronic Engineering, BUPT. His research focuses on optical networks and quantum networks.

Qin Wang received the Ph.D. degree from the University of Science and Technology of China in 2006. From October 2006 to July 2012, she was a Post-Doctoral Researcher with the KTH, DTU, and University of Copenhagen. She is currently a Professor with NUPT. Her research interests include quantum networks and quantum optics.

Dusit Niyato [M'09-SM'15-F'17] is a professor in the School of Computer Science and Engineering, at Nanyang Technological University, Singapore. He received B.Eng. from King Mongkuts Institute of Technology Ladkrabang (KMITL), Thailand in 1999 and Ph.D. in Electrical and Computer Engineering from the University of Manitoba, Canada in 2008. His research interests are in the areas of Internet of Things (IoT), machine learning, and incentive mechanism design.

Lajos Hanzo [F'04] (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo), received Honorary Doctorates from the Technical University of Budapest and Edinburgh University. He is a Foreign Member of the Hungarian Science-Academy, Fellow of the Royal Academy of Engineering (FREng), of the IET, of EURASIP and holds the Eric Sumner Field Award.