Wireless Communications and Mobile Computing

Quantum Communication Networks

Lead Guest Editor: Fabrizio Granelli
Guest Editors: Riccardo Bassoli, Frank H.P. Fitzek, Christian Deppe, and Holger Boche

Quantum Communication Networks

Wireless Communications and Mobile Computing

Quantum Communication Networks

Lead Guest Editor: Fabrizio Granelli
Guest Editors: Riccardo Bassoli, Frank H.P. Fitzek, Christian Deppe, and Holger Boche

Chief Editor

Associate Editors

Academic Editors

Contents

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3770994, 18 pages
https://doi.org/10.1155/2022/3770994

Research Article

A Novel Architecture for Future Classical-Quantum Communication Networks

Fabrizio Granelli,[1] **Riccardo Bassoli**,[2] **Janis Nötzel**,[3,4] **Frank H. P. Fitzek**,[2,5] **Holger Boche**,[3,4,6] **and Nelson L. S. da Fonseca**[7]

[1]*Department of Information Engineering and Computer Science (DISI), University of Trento, Trento, Italy*
[2]*Deutsche Telekom Chair of Communication Networks, Institute of Communication Technology, Faculty of Electrical and Computer Engineering, Technische Universität Dresden, Dresden, Germany*
[3]*Department of Electrical and Computer Engineering, Technische Universität München, München, Germany*
[4]*Munich Center for Quantum Science and Technology (MCQST), Schellingstr. 4, 80799 Munich, Germany*
[5]*Centre for Tactile Internet with Human-in-the-Loop (CeTI), Cluster of Excellence, Dresden, Germany*
[6]*Cyber Security in the Age of Large-Scale Adversaries (CASA)—Excellenzcluster, Ruhr Universität Bochum, Bochum, Germany*
[7]*Institute of Computing, State University of Campinas, Campinas 13083, Brazil*

Correspondence should be addressed to Fabrizio Granelli; fabrizio.granelli@unitn.it

Received 6 July 2021; Revised 18 February 2022; Accepted 12 March 2022; Published 25 April 2022

Academic Editor: Antonio Guerrieri

The standardisation of 5G is reaching its end, and the networks have started being deployed. Thus, 6G architecture is under study and design, to define the characteristics and the guidelines for its standardisation. In parallel, communications based on quantum-mechanical principles, named quantum communications, are under design and standardisation, leading to the so-called quantum internet. Nevertheless, these research and standardisation efforts are proceeding in parallel, without any significant interaction. Thus, it is essential to discuss an architecture and the possible protocol stack for classical-quantum communication networks, allowing for an effective integration between quantum and classical networks. The main scope of this paper is to provide a joint architecture for quantum-classical communication networks, considering the very recent advancements in the architectural design of 6G and the quantum internet, also defining guidelines and characteristics, which can be helpful for the ongoing standardisation efforts. For this purpose, the article discusses some of the existing main standardisation processes in classical communications and proposed protocol stacks for quantum communications. This aims at highlighting the potential points of connection and the differences that may imply future incompatible developments. The standardisation efforts on the quantum internet cannot overlook the experience gained and the existing standardisation, allowing the creation of frameworks in the classical communication context.

1. Introduction

The rise of new fundamental theories in physics always opens the door for subsequent advancement in practical physics and theoretical engineering. A fundamental theory of the last century is quantum mechanics. In the last decade, quantum phenomena have been applied to various fields such as photonics, computing, and cryptography. Moreover, quantum mechanics has become the primary enabler for a disruptive evolution in communication and computing systems, addressing existing open challenges not possible before.

The first worldwide telephone services required direct links between all communications entities. Next, the

communication paradigm became circuit switching, which provides a dedicated circuit between a source and a destination. Next, the communication networks evolved to packet switching. This paradigm allows information to be sent into a finite set of bits (messages), stored and forwarded by each router (switch) throughout the network, allowing communication among multiple heterogeneous entities in a scalable way. Packet switching was adopted as the transfer mode for the Internet, being its fundamental architectural choice for the design of a scalable network of networks. Another essential adoption to promote scalability was the employment of the tcp-ip protocol suite.

Access networks have played a vital role in expanding the Internet, allowing users to access the Internet with different devices. Especially, cellular networks have become one of the significant types of access after the advent of smartphones. 5G and 6G future networks bring a new approach to end-user communications. In fact, future networks will be an ecosystem (or pan infrastructure) capable of interconnecting highly heterogeneous networks, supporting demanding requirements and several different verticals. This will be possible via network virtualization, which is the software-based implementation of network functions, running on general purpose hardware. This breakthrough opened the way for a new approach, called compute-and-forward [1]. This term reveals the new role that computing assumes in the management and operations of communication networks.

Currently, 5G is under deployment and its standardisation is going to reach its end with release 18, in 2024. That is why, the research and the design of 6G started in 2021 to prepare the ground for the respective standardisation effort, together with its subsequent deployment starting from 2030. In the design of the next generation of networks, critical trade-offs arise. For example, some services offered by 6G networks will target very low latency (1 ms), very high throughput (up to 1 Tb/s), and very high energy efficiency (10-100 times the one of 5G) [2, 3]. Next, the load of unprecedented security level should also be added to these requirements. These high requirements have motivated a search for technical and theoretical tools to build and model 6G networks. Since ultimately every communication network is designed through application of knowledge about physical systems to the design process, an interest has arisen into using the most advanced theory as a key ingredient to the design process. The study, design, and standardisation of the quantum internet started from these premises. In the EU, the qia and the quantum flagship started their work in 2018, also leading the IETF qirg. In their perspective, communications based on quantum-mechanical principles could lead to a new Internet based on quantum communications.

Indeed, the ongoing IETF Internet-Draft of qirg [4] states

[...] we are at a stage where we can start to physically connect our devices and send data, but all sending, receiving, buffer management, connection synchronisation, and so on, must be managed by the application itself at a level below conventional assembly language, where no common interfaces yet exist. Furthermore, whilst physical mechanisms for transmitting quantum states exist, there are no robust protocols for managing such transmissions. [...]

Given the above premises, it is possible to see that not only the architectures of 6G and the quantum internet are still open research issues but also that the works are progressing independently, without any current clear integration. However, in order to solve the challenges stated by 6G and the quantum internet, a complete integration between the two communication networks is necessary. This implies it is now pivotal to discuss an architectural structure and the possible protocol stack for a future unique classical-quantum communication network. The design of this architecture is especially critical to allow for an effective and efficient integration between quantum and classical networks and to open the way for the study of possible protocols to manage the eventual "upper layers."

Thus, this paper aims at comparatively discussing in detail the status of the design and standardisation of classical and quantum communication networks. This aims at highlighting the potential points of connection and the differences that may imply future incompatible developments. Side by side, the article also describes the architectural and protocol stack's characteristics, focusing on key aspects like softwarization, layering, and synchronisation. Next, this work proposes an architectural design, with respective guidelines, in order to suggest an effective integration of 6G and quantum communication technologies, also beneficial for the future research on the quantum internet. We believe that since quantum communication networks will be built on top/next to the classical ones [2, 4], the discussions and standardisation efforts on the quantum internet cannot overlook the experience gained and the existing standardisation and realized frameworks in the classical communication context. In parallel, the current work on 6G must embrace the quantum communication technologies to go beyond its intrinsic limitations. The article starts with Section 2.1, which lists the main standardisation bodies in classical communications and introduces the research and design path towards 6G. Next, Section 2.2 summarises the characteristics of the classical Internet, especially focusing on the protocol stack and the layering problem. Section 2.3 explains the aspects of softwarization, focusing on its main architectural characteristics and standardisation effort. On the other hand, Section 3 shows the design and standardisation of the quantum internet, showing the layering aspects and the study of the protocol stack. Finally, Section 4 describes our new proposed architecture for future classical-quantum communications, taking advantage from the lessons learnt from classical and quantum communication technologies.

2. The Beginning of the Story: From the Internet and 1G to 5G

2.1. Main Standardisation of Classical Communication Networks. Major international standardisation bodies in

traditional telecommunications and networking include [1, Chapter 2].

2.1.1. International Organization for Standardisation. The International Organization for Standardisation was responsible for publishing the OSI model, which is a conceptual model that characterizes and standardizes the communication functions of a telecommunications or computing system without regard to its underlying internal structure and technology. The OSI model was defined in the document ISO/IEC 7498.

2.1.2. IEEE. The Institute of Electrical and Electronics Engineers published relevant standards such as IEEE 802.11 for WLAN, IEEE 802.3 (defining the physical layer and medium access characteristics of wired Ethernet), and IEEE 802.16 (for Wireless Wide Area Networks, so-called WiMAX).

2.1.3. 3rd Generation Partnership Project. The 3GPP covers cellular and mobile telecommunications technologies, including radio access, core network, and service capabilities. 3GPP is the main driver for the wireless 5G standardisation process with the current release 15/16/17.

2.1.4. ETSI. ETSI represents the recognized regional standard bodies dealing with telecommunications, broadcasting, and other electronic communications networks and services. ETSI partners with 3GPP to develop 4G and 5G mobile communication systems.

2.1.5. ITU-T. The mission of ITU-T is to ensure the efficient and timely production of standards covering all fields of telecommunications and ICT on a worldwide basis, as well as defining tariff and accounting principles for international telecommunication services.

2.1.6. Internet Engineering Task Force. The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. The IETF currently is the main driver for computing elements in communication networks through their standardisation activities on SDN and NFV.

2.1.7. Internet Research Task Force. The IRTF focuses on longer-term research issues related to the Internet while its parallel organization, the IETF, focuses on the shorter-term issues of engineering and standards development.

A primary aspect in all standarization efforts concern network synchronisation, which is a pillar to enable communication networks since it allows most of the protocols at every layer of the stack. Moreover, it is also fundamental for traffic engineering and assessment of most of the network performance metrics. Synchronisation can be performed in three possible domains [5]: time, phase, and frequency. Since the phase is also derived in the time, domain, time, and phase synchronisation are addressed concurrently.

A synchronisation scenario for 5G and beyond networks is depicted in Figure 1. Each network node usually has a clock (called slave clock measuring time $t_{s,i}$), which is synchronised with a so-called master clock time, t_m, equal to the reference time of the Global Navigation Satellite System (GNSS), obtained via a satellite link. The direct transmission of timing information from the gnss to each node of the network is impracticable because of technical limitations such as the coverage of indoor environments.

The ITU published its recommendation G.8271.1 in 2017, followed by an extension in 2020 [6]. These documents defined the maximum bounds on phase and time synchronisation error (see an extract in Table 1). Moreover, after the definition of the terminology to identify the devices involved in the synchronisation procedures, it stated the minimum accepted tolerance to phase and time synchronisation errors at the boundary of packet networks. Finally, this recommendation described the characteristics of the packet-based method for the distribution of time and phase synchronisation across a network.

Side by side, the Institute of Electrical and Electronics Engineers (IEEE) released the updated version of the standards IEEE 1588 [7], in 2019. In particular, this standard sets a packet-based synchronisation protocol called ptp. The main network architecture of ptp is depicted in Figure 2. The IEEE standard sets a network consisting of a k number of devices, where one represents the master clock with clock time t_m, which spread timing information to $k-1$ slave devices, owning clock time $t_{s,i}$, with $i = \{1, \cdots, k-1\}$. The reference time is sent to the prtc at the master clock from a gnss. Next, the time signal is passed to the Telecom Grandmaster (T-GM), which encapsulates timing information in the packets to be sent through the network.

The communication network between a master and its slaves consists of three kinds of devices: routers without support for packet-based synchronisation and routers with T-BC and T-TC. The T-BC has multiple ports and it can become a master or a slave as well. Nevertheless, it cannot be an end user (e.g., a sensor and an actuator). Another role is the termination and regeneration of timestamp messages. The T-BC devices can measure the residence time rt_i, which is the time a packet resides in the device from input to output ports. This calculation is separately performed for downstream (rt_i^{ms} from master to slave) and upstream (rt_i^{sm} from slave to master) communication. Side by side, the t-tc is fundamental to achieve a synchronisation accuracy in the order of microseconds or below. In fact, it can measure not only the residence time in a router/switch but can also measure processing and queuing delays. Next, T-TC devices can also be peer-to-peer, which implies the capability to also measure the link-propagation latency between similarly equipped ports at the opposite sides of the respective link.

The 3GPP has been active in the definition of the requirements, technologies, and protocols for aerial communications since 2017. The standardisation effort started analyzing the required additional characteristics to be added to LTE to provide optimal connectivity to UAV [8]. Next, in 2019, 3GPP started the work on integrating 5G upcoming networks with UAVs as base stations. This was published in the Release 17 [9]. Currently, the trend is to expand this preliminary approach to a full so-called three-dimensional

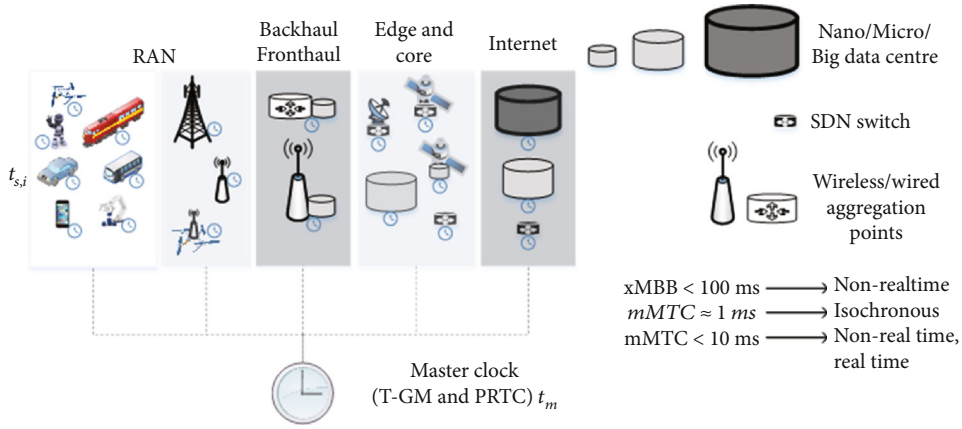

Figure 1: 5G and beyond communication network scenario with specification of master (time t_m) and slave clocks (time $t_{s,i}$).

Table 1: Synchronisation classes defined by the recommendation ITU G.8271.1, with the respective time/phase requirements [6].

Class	Error requirement	Possible application
Class 1	500 ms	Billing
Class 2	100 – 500 μs	IP delay monitoring
Class 3	5 μs	LTE TDD for large cells
Class 4	1.5μs	LTE TDD for small cells, NR TDD
Class 5	1μs	WiMAX TDD
Class 6	65 ns	LTE NR MIMO

networking in the context of future 6G architecture, where UAVs, haps, and satellites will seamlessly converge to a unique communication network architecture. This was clearly stated in the recently-published deliverable D5.1 of the EU flagship Hexa-X project [10], which focuses on the guidelines, enablers, and technologies for the future 6G architecture.

Figure 3 depicts the three 5G architectures using satellite and the 6G architectural vision of three-dimensional networking. The transparent 5G architecture allows ues to directly connect to satellites. Next, the traffic can also be routed to the terrestrial gNodeBs via the ntn gateways. On the other hand, the regenerative 5G architecture considers the placement of the gNodeB and its related computing tasks within the satellite-aerial platforms as well. Then, such a gNodeB can also communicate with the terrestrial core network and the Internet via the ntn gateways. The hybrid 5G architecture is the most flexible one since it also includes the softwarization and subsequent functional split of the gNodeB. In fact, the gNodeB is split into a du and cu, which can be placed somewhere between the aerial-satellite and the terrestrial platforms. This is the preliminary version of the 6G three-dimensional architecture that has been envisioning by now. The current architectural vision that will be standardised by 2030 will create a sort of "continuum," in which the softwarized network functionalities are dynamically placed. This so-called continuum is seamlessly either horizontal (two-dimensional) or vertical (three-dimensional). Especially, the latter can involve different kinds of terrestrial and aerial platforms, satellite, and haps.

2.2. Architectural Characteristics of Current Communication Networks. A reference model gives a conceptual framework to abstract network functionalities. In communication networks, most of these models adopt a hierarchical layering approach. Layering in networks is similar to the concept of objects in software engineering, furnishing services, and hiding their implementation. In the hierarchical layering approach, layers are stacked one on top of the other. Each layer offers service to the layer immediately above and receiving service from the layer immediately below. A layer interface defines how the services can be accessed and what restricts the information that can be retrieved from a layer. The ongoing trend to have network layers represented in software gives room for innovation, and at the same time, hides to some degree the physical representation of the layer from the network engineer.

Similar entities (process, agents) at the same layer in different network nodes can communicate with each other by obeying a set of rules, called a protocol. There is a protocol or set of protocols for the provisioning of communication services at each layer, realized by the exchange of pdu. Pdus are composed of a header, payload, and a trailer also called sdu. A pdu header contains information for processing the pdu at a receiving device, and a trailer delimits the end of the pdu. Trailers are less adopted in different protocol pdus since most of the headers contain a field defining the PDU size. Two endpoints do not exchange pdus directly, but a pdu is passed to the layer immediately below until reaching the physical mÃ©dium, where physical transmission effectively occurs. A layer-specific pdu is created at each layer by adding a header to the payload received from the layer above. The header is processed and removed at the corresponding layer at the receiving network node, and the resulting payload is passed to the layer immediately above.

Two standard reference models in communications networks are the OSI [11] and TCP/IP [12] reference models [13]. The Open System Interconnection, defined by the International Organization of Standardisation (ISO), is a de facto standard model commonly used to understand

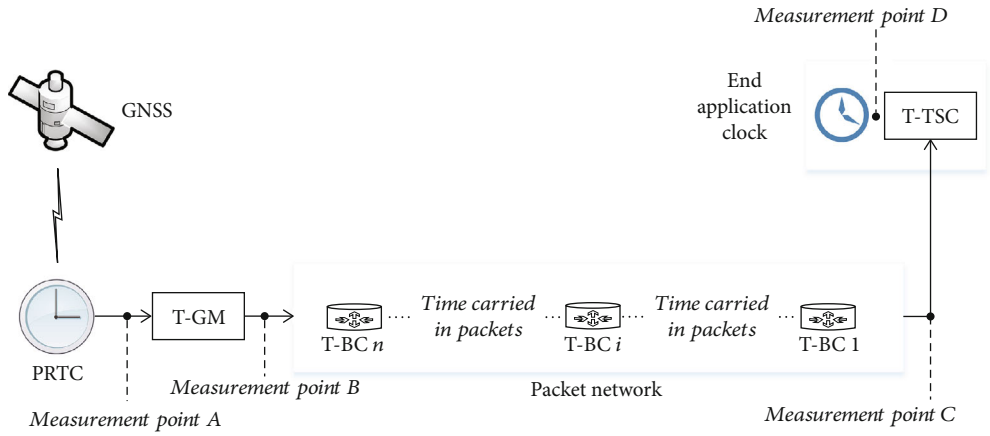

Figure 2: Time synchronisation model according to recommendation ITU G.8271.1 [6].

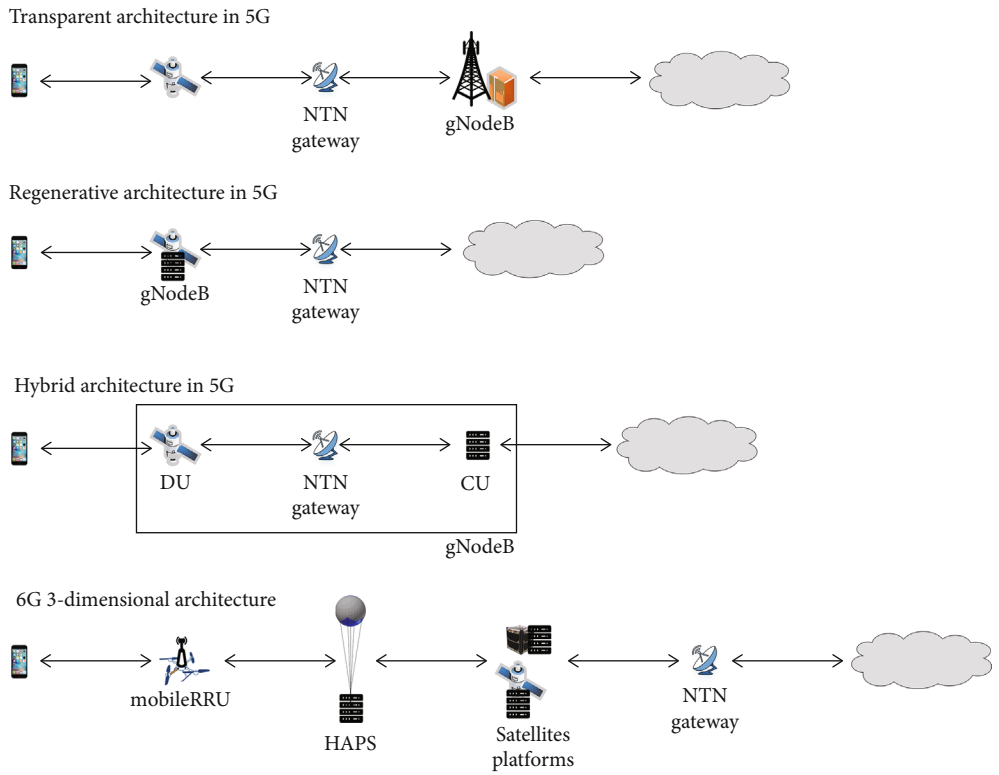

Figure 3: Satellite architectures proposed in 5G. The transparent payload acts as a relay since the gNodeB is on the earth surface. With the regenerative architecture, the base station functions are moved to the satellite. The hybrid architecture considers the potential softwarization and functional split of the functionalities of the base station. The last one is the 6G three-dimensional architecture, where softwarized functionalities of the base station can be activated dynamically at any aerial/satellite platform seamlessly.

new networking technologies and the relationship between different networking technologies [14, 15]. The OSI model defines seven layers: physical, data link, network, transport, session, presentation, and application layers, with functionalities described next.

In the physical layer, digital bits are transformed into electrical, radio, or optical signals, which are then transmitted on a physical communication channel. This layer's specifications include the definition of voltage levels and timing, data rates, maximum transmission distances, modulation scheme, and channel access schemes.

The data link layer gives the abstraction of a communication channel (link) for node-to-node data transfer. Error control and correction mechanisms support the creation of an error-free channel. Flow control, another common mechanism, attempts to avoid one node flooding another node with data. A multiple access control protocol needs to be defined in a broadcast type of link to avoid simultaneous

transmission of frames (data link pdus). Network nodes that realize connectivity and multiplexing of bits are called switches at the data link layer.

The network layer abstracts the subnet, that is, the set of routers and links. It provides the functionality of transferring packets from one node to another connected on the same network layer. Routing can be defined either as a predetermined fixed path or when the packet goes through a router (hop by hop). Since the network layer abstracts the subnet (network core), it is natural to place congestion control on this layer to avoid that the network enters a congestion state degrading the quality of the transport service substantially.

The transport layer abstracts the whole network between a pair of communicating processes in computers far apart. It is considered the first end-to-end layer connecting a data source and the destination. This layer defines the transport service seen by networked applications, which can be either connectionless or connection-oriented. A transport connection is a point-to-point reliable (error-free) channel that delivers pdus to the destination in the same order they were generated. The OSI model defines five classes of connections with distinct functionalities such as concatenation and separation, segmentation and reassembly of pdus, error recovery, reinitiation of connections, multiplexing/demultiplexing over a single fixed path, and flow control.

The session layer controls the dialogues between communicating endpoints and may include several transport connections. Session control also includes synchronisation (based on checkpoints) and token management (for access to critical regions).

The presentation layer is concerned with the syntax and semantics of the information transmitted. It makes possible communication between applications in computers with a different representation of information. It should define abstract data structures and the mapping of coded information to a standard abstract structure. The application layer contains the communication protocols used by applications. It hosts the various applications used by the end-users.

The OSI reference model provides a framework to compare and understand different network technologies. One example of such understanding remotes the launch of the Asynchronous Transfer Mode (ATM) networks which had four layers, and the first three correspond to the data link layer of ISO reference model with very few functionalities that could be considered functionalities typical of the network layer [16, 17]. The network layer also supports variable size packets (datagram) from the Internet Protocol (IP). This type of adaptation may be essential for adopting new physical and data link layers such as those in quantum communications.

Network architectures derived from a reference model may add planes to the layering models. These planes host specific functions composing a layer functionality. Typical planes are the data (user), control, and management plane. The data plane transports only packets generated by the end-user (forwarding function); the control plane transport control (signaling) packets which carry information for dynamic set up of the network; and the management plane, which coordinates the other two planes. A typical example is the transport of information by virtual circuits, fixed paths, or the transport of packets by the mpls [18]. The control plane is responsible for the setting and tears down of the virtual circuits (mpls paths), while the data plane is responsible for the forwarding of the packets generated by the users. Another example is the data and control plane of software-defined networks in which controllers residing on the control plane determine the routing of flows.

The TCP/IP reference model's development took a different path than that taken by the OSI model. The protocols were defined first, and then the reference model was specified. Indeed, the TCP/IP reference model resembles more a protocol suíte than a predefined architecture. The technical standards underlying the Internet Protocol suite are under the IETF. The TCP/IP reference model loosely defines four layers: link, internet, transport, and application layers.

The link layer is not a well-defined layer, and it specifies only an interface with links and devices on the same link layer. The link layer can be a single link or a whole network architecture. Indeed, anything below the internet layer is considered a link layer. Such definition reinforces the fact that the internet layer is independent of hardware implementations.

The internet layer solved the crucial issue of interconnecting incompatible networks by adding a layer on the top of all networks without needing translations and mappings between the connected networks. Connecting different networks, in other words, making different networks work together (internetworking), calls for the essential routing functionality, which defines the path packets (pdus) should take from a source to a destination node. Routing in the internet layer is carried out hop by hop, and decisions are made considering only the packet's destination address. Following the minimalist principle, the internet layer's delivery model is unreliable, which implies that packets can be dropped at network routers in case no space is available on router buffers to store them for later forwarding. Packets can also arrive out of order at the destination. Such type of service is known as best-effort service and is provided by the IP protocol, the only protocol employed to transport information on the Internet. Signaling on the Internet is in-band, contrary to other networks which have separated channels for data and signaling. Nonetheless, the forwarding of packets can be imagined belonging to a data plane while determining the next hop (routing) as residing in a control plane.

The transport layer offers two types of transport service for the applications: a connectionless one provided by the udp, which adds no functionality on the top of the internet layer, and a connection-oriented service provided by tcp. The application layer hosts all the communication protocols employed by the applications running on the Internet. These protocols use the transport layer protocols through the interface provided by sockets APIs. The application layer in the TCP/IP model is often compared to a combination of the session, presentation, and the application layers of the OSI model. Figure 4 compares the OSI and TCP/IP reference models [19].

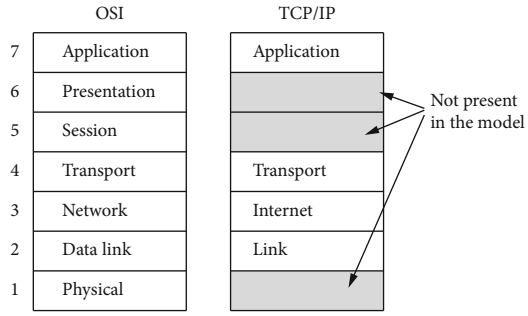

Figure 4: The TCP/IP reference model.

Although the layering principle is fundamental to network architectures and reference models, some functionalities are implemented in several layers and may require the interaction of mechanisms in different layers to realize the functionality needed effectively. An example of a cross-layer solution is error detection in tcp over wireless networks, where the link-layer hides and retransmits some lost packets to avoid unnecessary reduction of tcp window transmission. Such an approach is called cross-layer [20].

2.3. Future Softwarized Classical Networks. In Subsection 2.2, the protocol stack has been presented as a "monolithic" entity, consisting of layers interacting with each other via specific interfaces, the so-called sap. In such a structure, there is also the possibility of cross-layer solutions, but these are not as flexible as the software-based instances of network functions and operations previously described. In order to overcome this limitation, the concepts of pps and a wireless network operating system were proposed.

A programmable protocol stack is a software-based layered architecture, which can flexibly and adaptively manage protocols and network layers. The various entities in the virtualized protocol stack can reconfigure such as reassigning parameters, updating services, and replacing active functionalities, according to various conditions and requirements caused by users, network, and environment. This idea comes explicitly from the rise of applications for multimedia content distribution. Figure 5 depicts the logical structure of the two leading solutions proposed for pps, such as the Wireless Network Operating System and the Software-Defined Protocol.

First, the Wireless Network Operating System (WNOS) [21] exploits a network abstraction that targets a network control problem, given by the specific objectives of the hosted services. By characterising the network status via specific APIs, it is possible to adaptively optimise the KPIs like throughput and latency. In this scenario, the resources of the physical layer represent the available constraints. The PPS is included as a software-based pile, which adapts and configures according to the abstraction and the respective control problem to be addressed. The PPS also involves the physical layer since the adaptivity is possible via the deployment of reconfigurable radio technologies such as software-defined radios (SDRs).

Second, Software-Defined Protocol (SDP) system [22] consists of controllers and servers, which run specific blocks. The SDP blocks perform packets' routing. The SDP controller sets up the protocol stack's functionalities and characteristics to adapt layering, ensuring the required QoS. The SDP controller also configures flow tables in the switches and within the blocks in SDP servers.

Management and orchestration represent a crucial functionality to enable proper control on the softwarization of network functions. The reference in this field is represented by the ETSI-MANO architecture (see Figure 6). The key of the architecture is the availability of the network function virtualization infrastructure (NFVI), which enables to virtualize the available computational, storage, and networking resources. The NFVI is controlled by the Virtualized Infrastructure Manager (VIM). Management and orchestration are implemented by means of the NFV (Network Function Virtualization) orchestrator that oversees the operation of the NFV manager.

Even if it cannot be considered an official standardisation effort, the uonos project represents an effort to extend the capabilities and characteristics of ETSI-MANO architecture based on SDN and NFV. It is led by the open source community hosted by The Linux Foundation. uonos specifically aims at proposing a standard architecture for distributed control plane [23]. The main idea is the realization of a new generation of the SDN control plane based on ONOS. The objective is the splitting of SDN controller's functions into a set of subfunctions or microservices. These functionalities are deployed as virtual containers and managed by the Kubernetes orchestrator.

The μONOS protocol stack employs a new generation control protocol such as P4/P4runtime [24], which guarantees greater flexibility compared to the original OpenFlow protocol. The communication between functionalities is via Google's gRPC-based protocols, including network management interface and network command operations. Currently, the μONOS effort is leading the research on the decomposition of the SDN controller. Since this has just started, there is still no available implementation to test its performance. Moreover, the communication protocol is based on gRPC, and not on the rest API. This implies some specific limitations. First, μONOS has a limited isolation mechanism, which means the core functions and applications share the same resources or processes. Second, μ ONOS cannot have on-platform tenant-specific applications but only tenant-aware ones: tenant-specific apps must be off-platform, and it should use rest APIs. Third, the on-platform applications are limited to Java-based languages: applications developed using other languages have to be off-platform and need to use rest APIs. Next, the horizontal service scaling is difficult. Finally, it has limited integration with and support for NFV that do not adhere to either an OpenFlow abstraction of that of a legacy network element.

From the architectural perspective, given the capabilities opened by network softwarization, ai is going to play a key role in the management and orchestration of future communication networks. In fact, 6G is planning the realization of in-network intelligence, so that ai becomes not only a service but fully an element of the network architecture [25]. First,

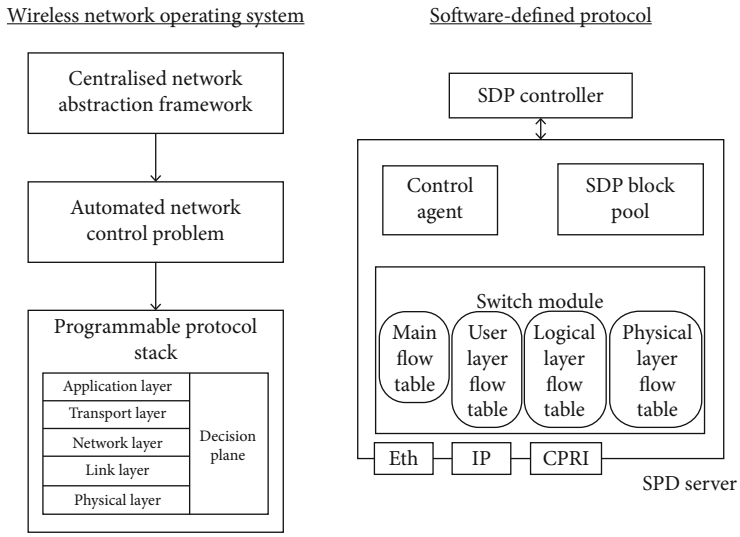

Figure 5: Logical structure of the Wireless Network Operating System and the Software-Defined Protocol.

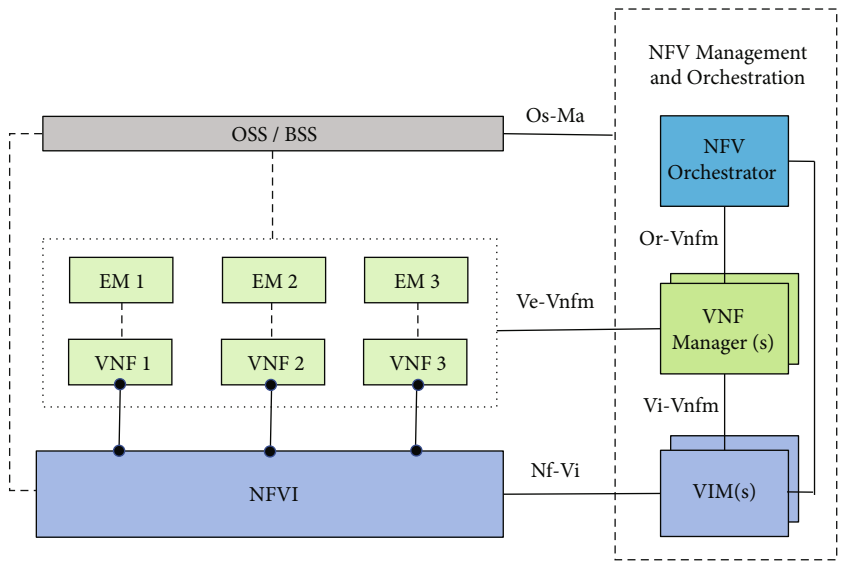

Figure 6: ETSI-MANO architecture.

the design of the AI-driven air interface of the ran will have a key role [25, 26]. In parallel, in-network learning methods will also be applied in the edge and core network for data, network, and users' management. As previously mentioned, in future 6G networks, each vnf will potentially be either a microservice or an intelligent agent. In the latter, intelligence will be integrated within several vnfs or sub-vnfs to realize multiagent systems, in which intelligent network entities collaborate to perform a specific network task [10].

Modern and upcoming communication networks are highly heterogeneous and complex ecosystems. Their stringent KPIs become necessary since the network design has been driven by new upcoming services such as the tactile internet, the industry X.0, and the internet-of-things. Moreover, future networks are going to fully employ network softwarization. This means that all the functions of the network, which are implemented in dedicated hardware, will run in virtual environments. This complex communication context will require a significant improvement of the existing network synchronisation procedures.

Network time synchronisation is fundamental for secure and tactile network operations, which require precise synchronisation among the nodes of the network. There are two main approaches to time-synchronisation in networks: the deployment of independently synchronised clocks at each network node packet-based synchronisation of distributed clocks. In the former, each network device is equipped with an atomic clock. This is an expensive and generally impracticable solution due to its high cost. Normally, each network node has a clock, which is driven by an internal oscillator. In a networked system, where different nodes can also have different types of clocks; clocks are powered

by nonidentical oscillators. Thus, these oscillators have inconsistent behaviour in different conditions, which result in timing errors and make datagram-based synchronisation necessary. The most important standard is the IEEE 1588, which aims at transferring timing messages from a master reference clock through the communication network in order to synchronise slave clocks. Moreover, the synchronisation of virtual environments of softwarized networks adds additional synchronisation errors. These aspects make datagram-based methods not able to satisfy the increasing precision and security required by the critical services of future communication networks.

3. The Advent of Quantum Communication Networks

Future networks call for an increase in current storage and computing capacities, which also implies augmenting energy usage (for computing) and consumption (for communications). Additionally, in-network intelligence will demand a large number of resources for communication during data mining and distributed decision-making. Prediction of future network states will also bring computational overhead. All these aspects will require ultraprecise reliable synchronisation protocols, which must satisfy the low-latency KPIs.

Moreover, the targeted KPIs of the existing 6G proposal may arise contradicting objectives. For example, energy saving contradicts the massive amount of computing needed by in-network intelligence. Next, anticipatory networking sets a trade-off between low-latency and reliability. Moreover, low latency will be critical for the amount of computing, data mining, and quite-high data rates. In fact, increasing data rates and link usage will raise transmission and scheduling latency. These are only some of the several trade-offs and contradictions within the design and realization of future classical networks.

In order to exceed the intrinsic limitations imposed by the abovementioned issues, quantum-mechanical communications and computing have been considered to support envisioned future networks. By employing distributed quantum computing instead of classical computing, the exploitation of entangled qubits within several interconnected devices can achieve an exponential speed-up of the network computational capabilities with just a linear increase in physical resources. Thus, the limitations imposed by classical paradigms and "softwarization" can be solved by exploiting quantum-physical parallelism based on the concepts of quantum superposition, entanglement, and quantum measurement [2]. Next, an overview of the current preliminary status of the architectural design and standardisation of quantum communication networks will be provided.

3.1. Current Standardisation Procedures for Quantum Communication Networks. The general prestandardisation focus group about quantum information technologies is the one belonging to ITU, called Focus Group on Quantum Information Technology for Networks (FG-QIT4N). This group was created in September 2019. The main objectives of the group are the study and definition of terminology and application for quantum information technologies, which can also open the way for a collaborative platform for designing future quantum communications with the contribution of industry, technical experts, scientists, and policy makers.

The vision of the quantum internet [27, 28] aims at designing and developing a quantum communication network, interconnecting quantum computers to target various quantum-enhanced network aspects such as security, synchronisation, and computing. The standardisation process of the quantum internet is going under the leadership of the IETF research group called qirg [4].

The standard starts with the definition of the atomic entity of information, the qubit, and subsequently the multiqubit systems. Entanglement between qubits is defined as the fundamental quantum resource for communication. However, quantum communications introduce some challenges such as those ones resulting from measurement, no-cloning theorem, and the fidelity. Furthermore, the document [4] states the inadequacy of direct transmission since it requires expensive quantum error correction mechanisms to keep quantum errors at the minimum. At this point, an important claim of the draft standard [4] is that

[...] quantum error correction is not expected to be used until later generations of quantum networks.[...]

Then, the most efficient way of distributing entanglement remains the use of Bell pairs, which is the fundamental pillar of the basic quantum protocols of dense coding and teleportation.

Entanglement can be generated in three main ways: at midpoint, at source, and at both end-points. The first involves a third party, which distributes the entangled qubits via quantum channels to the communicating nodes. The second and the third only involve one or both the communicating nodes in the entanglement generation and distribution. Since entanglement is very sensitive to time and interactions with the environment, entanglement swapping is the procedure, which can be used to ensure distribution for distances greater than 150 km.

When drafting the architecture of the quantum network, the document states

[...] In a quantum network, the entangled pairs of qubits are the basic unit of networking. These qubits themselves do not carry any headers. Therefore, quantum networks will have to send all control information via separate classical channels which the repeaters will have to correlate with the qubits stored in their memory. [...]

From this quotation, it is important to make some initial architectural considerations. First, entangled pairs are lower-layers entities, mainly upper-physical and lower-link layers. However, the kind of correlation created by these basic units of networking has an inherent cross-layer nature so that they can affect the network layer via the output information of the specific sap. This will be considered in the proposed new architecture in Section 4.

Next, the draft standard [4] makes a distinction between control and data plane. This network abstraction is defined as fundamental to set for example forwarding rules of qubits.

The control plane should be similar to its classical counterpart, and it does not handle quantum data in general. However, some quantum control protocols might be defined like the quantum ping. Additionally, the document defines so-called control information messages, which aims at managing single entangled pairs. Nevertheless, the characteristics of control plane also in relation with data plane are claimed to be out of the scope of [4]. Regarding the data plane, the draft standard states the existence of two concurrent planes, classical and quantum, with their respective operations and protocols. In the document, the authors say that the design of the specific network abstractions remains an important open challenge for the realization of interoperable quantum network protocols.

Finally, the draft standard [4] proposes a possible employment of mpls in quantum networks. Since the distribution and maintenance of entanglement among network nodes is a stateful process, the use of connection-oriented solution is the one suggested. This implies the connection via virtual communication circuits among network nodes for quantum entanglement distribution. Next, [4] mentions that signaling functions are needed for setting up virtual circuits so that protocols like resource reservation protocol (RSVP) or OpenFlow can be employed. Additionally, the generalized mpls (GMPLS) is suggested as a good potential protocol to handle separate channels for control and data plane flows.

Quantum key distribution (QKD) is a security protocol, which provides information-theoretic security against a third party such as an adversary or eavesdropper. The protocol distributes quantum keys to network entities. The security of these keys is not ensured by the limited capabilities of the adversaries. On the other hand, the physical characteristics of quantum mechanics make these keys inaccessible. In fact, the security mainly comes from the no cloning theorem and an underlying information gain/disturbance trade-off. If an eavesdropper interacts with a shared entangled state, it introduces an irreversible disturbance that is proportional to the information that has been gained. Then, the communication parties can detect and quantify the presence of noise and abort when it reaches levels that reveal the attack. It is important to notice that QKD protocols assume the existence of an authenticated classical channel among the parties that have to share the keys.

3.2. Currently Proposed Architectures for Quantum Communication Networks. The existing literature on quantum communication networks has focused on the design of network architectures and protocol stacks for quantum-only networks. This means that the combination between classical and quantum infrastructure has not been considered. The following overviews the main trends proposed for quantum communication network architectures and protocol stacks.

Figure 7 depicts the initially proposed protocol stack for quantum communications by [29]. In particular, it refers the physical and link layers. The main protocols, which have been proposed, are the MHP, the EGP, and the DCP.

The MHP is a control protocol, which was proposed for the upper-physical layer. This protocol should be implemented to comply with very stringent timing requirements because it is responsible for deciding the generation of entanglement. In that sense, it defines an MHP cycle, which granularity directly affects the communication performance (e.g., the throughput). The protocol uses time-division communication in which a timestamp and an ID set the detection window for each photon. The MHP was proposed based on two procedures: create-and-keep and create-and-measure. The former considers only quantum operations on photons (so-called quantum gates), while the latter allows for performing measurements. The results of these measurements are used by the EGP protocol.

The EGP is the core protocol of the architecture in [29]. The protocol exploits some assumed logical blocks such as a distributed queue, a qmm, a feu, and a scheduler. As mentioned above, the setup of entangled photons is helped by the MHP protocol. The EGP protocol maintains distributed queues, which schedule the requests of entangled particles. These queues can also employ different criteria of priority. The qmm logic block selects the specific photons that have to be entangled. A critical aspect is the "quality of the entanglement" or fidelity. The feu estimates the fidelity of the entangled photons, guaranteeing that this value is above the required minimum threshold. Next, the scheduler decides the serving policy of the queue.

The EGP protocol starts when a request for a number of entangled photons arrives from the above-two layers. At this point, the feu sets the specific requirements for fidelity and completion time of the process. Next, the request of entanglement is assigned to the distributed queue. The scheduler manages the status of the request so that finally, the qmm can successfully allocate the requested qubit. As mentioned above, the MHP allows the processing of the requests coming from the EGP. Each request in the queue has a unique identifier, which also helps the management of the respective qubits.

The DCP manages the distributed queue of requests of entanglement, coming from all network nodes. The protocol also stores the information about the requests, such as the creation time and the minimum time (that is introduced by the presence of a timeout cycle at the MHP).

In 2019, [30] provided a description of the protocol stack of quantum communication networks, from the physical to the network layer (see Figure 8). The physical layer has the same role and characteristics of its classical counterpart. In fact, it transmits/receives unstructured raw data via a physical transmission medium by converting the qubits into optical signals. Moreover, it converts the signals into different forms according to the transmission technology and frequency.

The second layer is a new layer between the physical and link layer, called connectivity layer. This layer is responsible for quantum error correction and setup of long-distance quantum communication links. In particular, the considered communications can be single-source unicast or multicast. The critical aspect of this layer is the distribution of

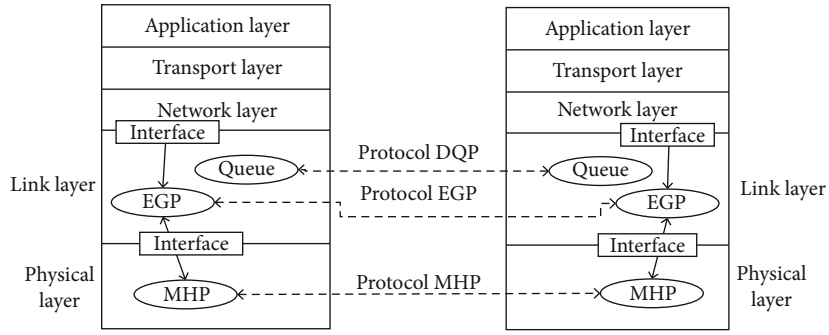

Figure 7: Initial protocol stack for quantum communications, proposed in [29].

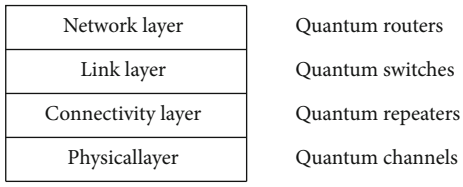

Figure 8: High-level protocol stack for quantum communications, proposed in [30].

entanglement—either Bell pairs or Greenberger–Horne–Zeilinger (GHZ) states—among distant nodes, which is the pillar of quantum communications. An important aspect is that the operations within this novel layer are independent of the above link layer's protocols. The main objective is the decoupling between pure link layer and connectivity operations in order to simplify maintenance and network upgrades.

Next, the link layer hosts the protocols to create the network quantum state of arbitrary topology. The aim is to generate and distribute the entanglement to the device of the required quantum entanglement topology. This layer also manages entanglement distillation in order to ensure the specified level of fidelity. Entanglement swapping and merging quantum states are also performed at the link layer.

Finally, the network layer is responsible for manipulating entanglement and allowing routing at a network level. The primary devices involved are the quantum routers. The authors in [30] have proposed some preliminary quantum protocols, which are comparable to their classical counterparts.

3.2.1. Open Systems Interconnection Conformal Quantum Networks. In [31, 32], the authors consider a different route to the development of classical-quantum communication networks, following an approach of subsequent minimal changes to the existing network architecture rather than a radical replacement of the existing one. The work is focused on entanglement-assisted data transmission only, resulting in relatively minor changes to the existing architecture in the sense that only the physical and link layers are affected. The authors describe the Generate Entanglement When Idle (GEWI) principle [32] as a sender-side mechanism that starts generating and distributing entanglement as soon as there is no data in the sender-side data buffer. A corresponding sliding window entanglement generation protocol is described in [31]. When there is data in the sender-side buffer but no entanglement stored between sender and receiver, the protocol transmits data without entanglement assistance. The recent development of entanglement-assisted communication techniques [33] makes the hybrid classical-quantum communication network structures an interesting proposal. Due to the need to distribute entanglement first, these proposals might suffer from the same problem that is inherent to quantum networks—namely, the dependence on a repeater architectures, where current achievements are promising but larger field trials have not yet been conducted. In addition, it is yet unclear in which data transmission scenario the entanglement-assisted communication schemes will bring the promised substantial benefits over nonassisted ones. While the focus on an end-to-end use of entanglement in networks is obvious from the literature, and current research has started to identify its potential [34] and use [33] for data transmission, the possibility of utilizing quantum technology in a localized fashion for the goal of faster data processing at lower energy consumption has been pointed out recently in [35]. The work [35] points out the potential of quantum signal processing where network functionalities are optimized using quantum techniques without any need to distribute entanglement over the network. Rather, the focus is on utilizing the enhanced sensitivity of quantum detectors and processing mechanisms. The research on the optimal data transmission methods has been pioneered in the fundamental works [36, 37]. A first concrete description for an implementation dates back to [38], follow-up works like [39, 40] described different variants and extensions of the proposed scheme. An excellent overview is given in [41].

3.3. Physical Layer Service Integration. Physical layer service integration (PLSI) is an approach that is emerging from a series of works analyzing communication tasks from an information-theoretic perspective, taking into account models going beyond the initial work by Shannon (sometimes these works are categorized as post-Shannon theory) in the sense of more accurate mathematical modelling of tasks, resources, and involved parties. PLSI identifies the principal resources available at the physical layer, the bottlenecks and vulnerabilities in typical communication scenarios, and the ability of the physical layer resources to solve

the identified problems. Plsi aims to rebalance the network architecture by adding critical functionalities to the physical layer, to accelerate their execution. Since the physical layer of every future communication network utilizing quantum technologies has to eventually address the question how to generate and distribute entangled states, plsi is important when thinking about quantum networks in general. Plsi can correct some of the drawbacks arising from softwarization by moving critical services towards the physical layer, thereby increasing its flexibility. While it is obvious that future networks will in addition to signal generation, transmission and detection also need to generate entanglement, a novel task which is being motivated in the post-Shannon context is also the generation and distribution of randomness. Fast random number generation can be used as an input to physical layer network coding [42]. The availability of entanglement and sometimes also shared randomness even allows the execution of novel security primitives such as oblivious transfer [43, 44], the origin and historical developments of which are well described in [45]. An oblivious transfer allows the secure computation of functions between network entities and reduces the need for a sharing of private data in such applications. With regards to the security assumptions, there are a variety of proposals. The information-theoretic perspective applied to the executions of oblivious transfer over single-hop classical network connections is described well in [46]. Recent work [47] claims a protocol for achieving positive oblivious transfer rates even in situations where the participating parties can be dishonest. Despite drawbacks, vulnerabilities, and the development of impossibility results [48], novel methods for the execution of oblivious transfer protocols have also been researched and proposed in quantum communication [49], such that the possibility of secure computation over communication networks remains.

Once the generation of distributed randomness (which can also be harvested from entanglement) is a physical layer service, the network nodes sharing this resource benefit from increased robustness against jamming and Denial of Service (DoS) attacks. These effects have been highlighted in the quantum information-theoretic literature on arbitrarily varying (quantum) channels [50–52] and motivated research on plsi. The increased resilience is vital for wireless links of critical infrastructures, such as in-campus networks. A crucial assumption in the aforementioned line of arbitrarily varying channel models is the existence of shared randomness which is unknown to a potential attacker (secret, for short). A possible way to satisfying such assumptions is to distribute entanglement through the network. The value of distributed shared (secret) randomness is best understood from the recent work [53]. In [53], the problem of detecting DoS attacks, for example, on wireless networks, has been formulated and analysed using the formalism of (classical) arbitrarily varying channels. As it turns out, deciding whether a DoS attack is possible on a given wireless link is not possible in general. Still, scenarios where a DoS attack is not possible can be detected. If shared secret randomness is available for a given system, its capacity can be computed using standard techniques. Thus, the question of how to assure the quality of secret shared randomness is vital for resilient communication.

Following from the work on OSI network conformal quantum networks as described in Subsection 3.2.1, physical layer service integration also encompasses efficient error correction in the transmission of classical data. To build on the concrete example given in [35] where quantum communication techniques were proven to reduce energy consumption in long-haul fiber transmission, an obvious and simple example of physical layer service integration is fully optical error correction in optical fiber transmission, where the task of error correction is handled by the physical layer. This approach ultimately allows building receivers attaining the data transmission capacity of any physical medium. Depending on the boundary conditions in terms of bandwidth, signal energy, or transmission range, quantum receivers can beat their classical counterparts by orders of magnitude.

In order to finally give a concrete historical example of successful plsi, we point to all-optical networks. In optical long-haul fiber transmission, a choice exists regarding the method of signal regeneration. In particular, a design choice can be made between opto-electronic conversion including error correction and feedback methods between nodes placed along a link connecting a sender end receiver, or fully optical amplification. The vision of all-optical networks [54], built on the latter approach, corrects the signal to noise ratio while leaving the signal in the optical domain and without applying error correction steps. In this sense, plsi is a design choice that with examples of successful application existing already today.

3.4. Spatial Structure of Current and Future Networks. A final important architectural aspect to be discussed is the highly-growing interest for aerial and satellite platforms' integration into the terrestrial quantum communication networks. This is mainly due to one of the major issues that are affecting the research on and the design of the quantum internet: the need for quantum repeaters. Quantum communications in fibres can reach a distance of about 100-150 km. Then, in order to maintain the fidelity of entanglement and to avoid decoherence, devices like quantum repeaters have to be employed. However, these devices are still under research, and they are highly complex and expensive. Around 2014, the research started to focus on qkd and entanglement distribution via satellites in order to achieve intercontinental communications more easily. A recent record was set when entangled photon pairs were distributed via two bidirectional downlinks from the Micius satellite to two ground observatories in Delingha and Nanshan in China [55]. In the last years, the scope has been moving to ensuring miniaturisation, lower costs, and lower orbits [56]. These advantages are necessary for a subsequent and seamless integration with the terrestrial network. However, the realization of entangled quantum systems and their distribution to any node on earth via nanosatellites (e.g., CubeSats) is still an open research challenge. Distributing entanglement via nanosatellites would significantly reduce the need and the cost of repeaters. That is why the three-

dimensional networking has a crucial role also in quantum communication networks.

3.5. Key Performance Indicators. In the following, we give a short overview over the most relevant Key Performance Indicators of quantum channels. As most systems are in a technically premature stage, we focus on those derived from information theory. In contrast to classical communication systems, where the Shannon capacity of a channel was the dominant metric over several decades, research on quantum communication systems identified three different capacities early on. In the context of post-Shannon literature, several additional KPIs were discovered both for quantum and for classical channels. The simplest KPI for a quantum channel is its message transmission capacity [36, 37]. A second KPI is the entanglement-assisted message transmission capacity which is based on the idea of dense coding [57]. For this type of data transmission, it is assumed that entanglement has been established between sender and receiver which is available to both of them at the time where the data needs to be transmitted. The third fundamental KPI of a quantum channel is its capacity for transmitting entanglement [58–60]. This latter capacity is also referred to as the quantum capacity of a quantum channel. It is an important open problem to derive exact formulas for the latter capacity, which is not even known for very simple transmission systems yet. In addition, the quantum capacities of quantum channels have been derived under the assumption of DoS attacks in [50] and under the assumption of incomplete information regarding critical system parameters in [61]. Channels with memory have been studied in [?], and the second-order behaviour which is relevant to the performance with finite blocklength in works such as [62, 63]. The effect of fading on quantum channels has been studied in [64, 65]. Finally, the identification capacity of a classical channel has been derived in [66], and formulas for several quantum communication systems have been proven [67, 68]. The identification capacity is a KPI from the domain of post-Shannon information theory, which describes the number of messages per channel use that can be achieved in situations where the receiver is only interested in the question whether or not the incoming message was intended for him. It should be noted that a direct technological comparison of the different techniques that are theoretically available from quantum technology development with those existing as a state-of-the-art is typically not available in a systematic fashion due to a lack of readily available components on the quantum technology side.

4. An Architecture for Future Classical-Quantum Communication Networks

In Section 3.2, the legacy quantum network architectures have been outlined. The question arises how to reconcile these architectures with current trends. Of particular importance is the decoupling between network functionalities and hardware through softwarization, which has opened the way to extensive employment of in-network intelligence, easier network management and upgrading, and to efficient and effective management of multitenancy.

The novel architecture this work proposes leverages the idea of network softwarization realized via SDN and NFV, in order to achieve a better integration of quantum communication networks with upcoming and future generation networks. Furthermore, it also inherit the pros of network softwarization that have been just mentioned, opening the way for a more flexible and advanced quantum-classical network management and operations. Figure 9 depicts the logic architecture that this work is going to propose. The network infrastructure consists of a hybrid quantum-classical network, combining 4G and 5G technologies, and the three-dimensional 6G communication networks with a quantum physical layer. As seen in the previous sections, the three-dimensionality is pivotal both for quantum and classical communication networks. Next, the end-to-end management and orchestration has to handle a hybrid three-dimensional infrastructure considering data and control planes with quantum capabilities as well.

As mentioned previously, the Internet is evolving towards a SDN approach, as modern networks are incrementally deploying SDN to facilitate configuration, operation, and automated management. In this framework, an interesting direction might be represented by introducing the detachment between control and data planes at the basis of the SDN paradigm and extend it to quantum communications. This integrated classical-quantum Internet architecture would enable the deployment of classical as well as quantum link level communication technologies and devices that will constitute the data plane of the converged infrastructure, while maintaining a "traditional" control plane functionality in the form of an evolved SDN controller—be that centralized or distributed. The relevant advantage of this solution, which in our considerations would be preferable, is the convergence of quantum-plus-traditional Internet as a single-integrated and single-managed entity that would enable faster integration of quantum technologies within modern networks.

Then, it is pivotal to maintain the current separation between data and control plane, envisioned by SDN. In this sense, the control plane will not only manage the classical protocol stack but also the quantum physical-link layer resources. This will also advance the hybrid quantum-classical protocol stack towards the idea of programmability, which means the capability of adapting the hybrid protocol stack according to network conditions with the possibility of slicing quantum communication resources as well. This will highly enforce the coexistence and the progressive introduction of quantum technologies within future communication networks. An important consideration refers to the design of the interfaces between the upper softwarized layers and the hybrid physical classical-quantum layer. Especially southbound, but also the northbound interface, will require programming that takes into account the different algorithmic implementations that quantum resources demand. Furthermore, the inherent cross-layer characteristics of entanglement, mentioned in Section 3.1, require a specific

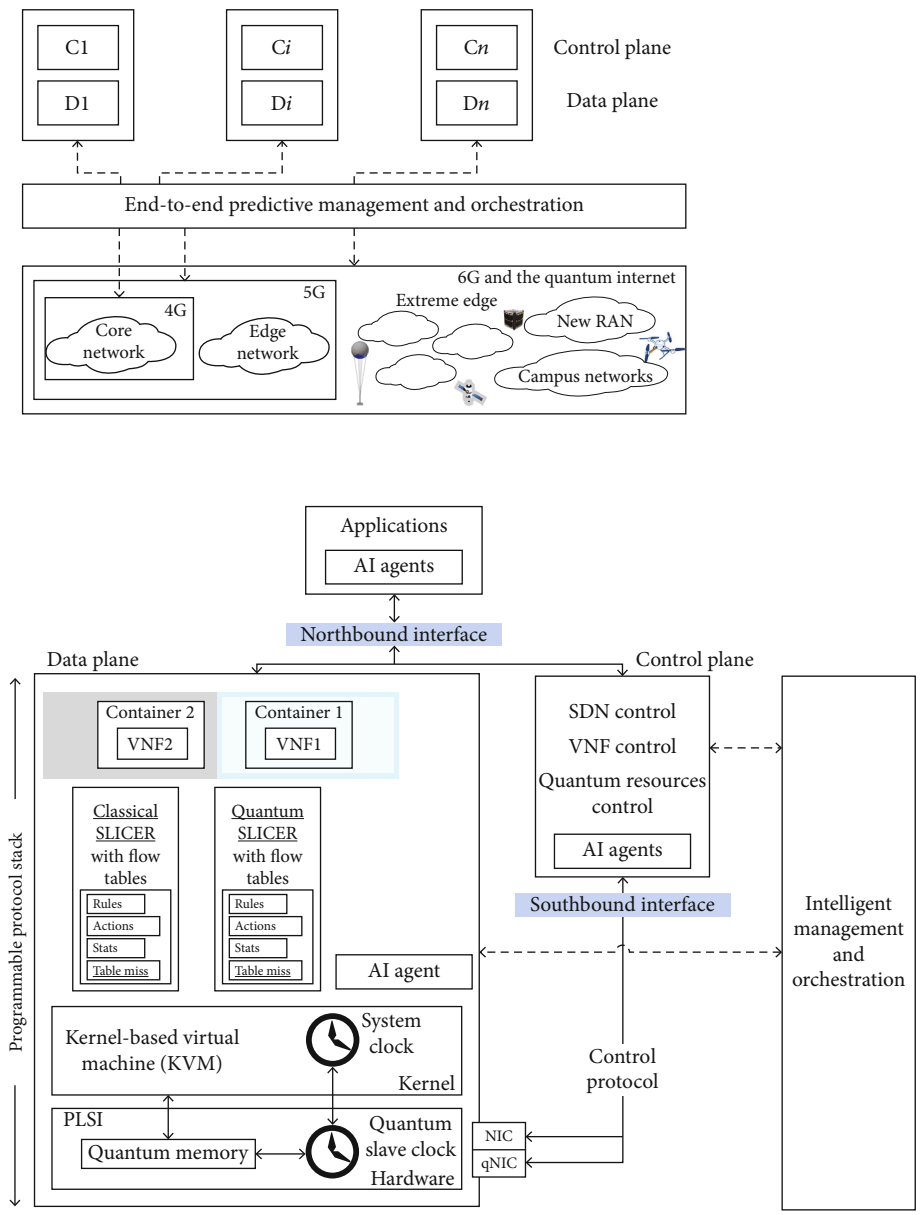

Figure 9: High-level schematic of the proposed quantum-classical network architecture, where control and data plane reside in all the devices. The network infrastructure is considered a continuum by the softwarized layers and by the management and orchestration, which can also employ intelligence (above). Logic architecture of quantum-classical communication network that has been proposed (below). The qNIC is the quantum network interface. The slave clock is the only one represented since the master clock can be either placed in another network node or in the controller according to the specific characteristics of the infrastructure.

design not only of link-layer but also of network-layer protocols and saps.

A distributed control plane can be preferable in respect of a centralized one since procedures like entanglement swapping for longer-distance entanglement distribution will imply significant communication control overhead. Then, controllers can be moved close to areas (for example geographically bounded campus networks or low latency verticals like the tactile internet) or routes where entanglement distribution is needed most. It should be taken into account that the controller will be a virtual function dynamically placed in data centers. Thus, in our proposed logic architecture, computing and the role of data centers is pivotal for quantum communications. Entanglement creates a physically distributed state among network nodes, and it is not a stateless operation [4]. This means that the architectural choice of a control plane, either centralized or distributed, can be very effective to manage these aspects and to keep spatial-temporal track of quantum network states.

Next, the control protocol and the interfaces between control and data plane have a key role. This can be a flow-oriented protocol and considering ports abstraction for

managing the quantum and classical data flows. This flow-management is possible by setting up the flow tables and their internal rules. These flow tables refer to both quantum and classical resources' assignment and allow for potential slicing and multitenancy. This novel proposed architectural element also has the capability of concurrently programming multiple network devices. Thus, in respect of other proposed architectures in the literature, this has a "network viewpoint," which can enable a more efficient and effective entanglement distribution and quality-assurance, in parallel to a more effective control of network resources and paths (also leveraging the programmability for future employment of intelligence).

The interfaces that come into our quantum-classical architectural view and that are missed in existing quantum network architectures are southbound, east/westbound, and northbound. First, the southbound control interface on quantum communication devices, which should integrate a proper interface to enable the control plane to issue commands and provide status information. Second, the update of the SDN southbound interface. The communication between the control and data plane is implemented using the southbound interface. In the most common cases, such interface might be provided by protocols such as OpenFlow or languages such as P4. Those technologies should be enhanced to support quantum-specific operation and to enable devices to advertise their quantum or traditional features.

Regarding the east/westbound interface, these are internal to the control plane, and they become pivotal when the control plane is distributed. In this latter case, it is necessary another protocol to manage the distributed control of quantum-classical resources and data plane in general. Finally, the northbound interface has to be included (and its classical version modified) so that classical software applications can leverage the quantum effects at the physical and link layers.

Backward compatibility could be enabled by introducing small modifications to the features' discovery process of SDN. Indeed, features' discovery represents a mandatory process to enable SDN controllers to learn the specific characteristics of the network devices. For example, in the case of OpenFlow, after the initial handshake implemented over TCP/SSH using the HELLO messages, the SDN controller will issue a FEATURES_REQUEST message in order to acquire the functionalities supported by the OpenFlow switch. To support quantum communications, the FEATURES_REQUEST and FEATURES_REPLY messages should be enhanced to support quantum-specific operation.

As it is possible to see from Section 3.1, the definition of an architecture and a protocol stack for quantum communication networks is currently neglecting a major aspect of future 6G networks: ai. However, some works have been underlining the importance of quantum communication networks for achieving efficiently in-network intelligence [69], together with the new potentials of opened by quantum machine learning for the management and orchestration of future hybrid quantum-classical communication networks [70]. Then, Figure 9 also tries to envision the placement of hybrid intelligence in the quantum-classical network architecture. The architectural integration of classical and quantum communication technologies implies the "hybrid" collaboration of classical and quantum intelligent agents. Since a great part of the control of the quantum networks will be performed classically, classical in-network intelligence will play a key role for management and orchestration. However, in this context, the decision-making and the prediction can also be based on potential new intelligent algorithms based on quantum machine learning, running in quantum data centers. Next, within the control plane and the data plane nodes, ai agents can perform specific tasks, exploiting either the classical or the quantum physical and link layers. This mainly depends on the technological advancements that will be achieved by quantum computing for communication nodes in the next ten to fifteen years. If the miniaturisation and costs of quantum computing will not reach reasonable thresholds, the role of quantum machine learning in 6G will be limited to centralized management and orchestration. Finally, intelligent agents can also be realized at the application layers, for paradigms like ai-as-a-service. In this context, the employment of "quantum" intelligent agents is going to take longer time since the maturity of "quantum" optimized software for fully-quantum hardware represents a long-term objective.

In legacy proposed architectures, a quantum link layer manages the mapping of entangled photons to entangled qubits, and it guarantees the overall quality of the communication. One possibility to achieve integration between quantum and traditional link layer technologies might be to consider quantum as another layer 1/layer 2 technology and to achieve loose integration by exploiting the interoperability provided by the Internet Protocol. Such a solution would require adapting TCP/IP lower layers to the needs of quantum communications. This mean introducing a proper version of the Address Resolution Protocol (ARP) as well as additional functionalities between IP and the quantum layers in order to support entanglement and channel setup functionalities.

An alternative might be to enable the integration of quantum-powered autonomous systems within the overall Internet topology by exploiting IP tunnelling functionalities. This alternative might represent a mature solution, considering the diffusion of tunnelling protocols for Virtual Private Networks (VPNs) and IPv6-IPv4 tunnelling. Quantum technologies would represent a specific physical-link layer technology operating under a network operator, connected to the rest of the Internet via tunnel end-points that would hide the specific characteristics of the quantum internals. Tighter integration might consider the possibility of enabling classical and quantum operation on the same physical link. This would require adaptation of classical mac protocols to this novel functionality or the introduction of an "upper" mac scheduler capable of facilitating the coexistence.

The advantage of both the above solutions would be to enable quantum communications to freely evolve as a separate standard providing methods for interoperating with other standards at the higher network layers without specific constraints from the rest of the public Internet while

incrementally enabling its implementation in parallel to innovations in Internet-related technologies.

In this new architecture, plsi as described in Subsection 3.2 can be used to meet specific demands in peak data rates, resilient low-latency communication, or secure network function computation.

Another service that can be considered as plsi is the network time synchronisation. Classically, this task is performed at layer 2 and layer 3 (as previously described). From synchronisation viewpoint, the architecture considers the presence of a quantum master clock, which transmits ultraprecise (in the order of picoseconds or below) timing information to its quantum slave clocks. The choice of master clocks and their placement is out of the scope of this work. However, it is important to notice that an example scenario may consider the placement of a master quantum clock for local area networks of slaves directly connected with the master.

Depending on the desired network hardware and structure, not all tasks can be considered in plsi. For example, the gains from entanglement-assisted data transmission depend both on entanglement storage times and the communication medium, while network time synchronisation is affected most by the topology and to some degree on storage times.

5. Conclusion

This article has provided a novel architecture for future quantum-classical networks, which leverages the trend of evolution of upcoming and future generation networks. While the legacy proposed architectures for quantum communications are limited to some perspectives, the one envisioned in this work considers the lessons learnt from in-network computing, network virtualization, and programmable stacks. Moreover, it considers the employment of quantum communications for network synchronisation operations, which are pillars of communications functionalities of the whole protocol stack. In order to justify our proposal and to compare it to the ones in the state-of-the-art, an introductory part on the important and related aspects of classical networks was provided. Next, the discussion also embraces research and standardisation status in order to show the differences between classical and quantum communications research and standardisation efforts. This is also important to show how our architecture brings together the different research trends and works by the different standardisation bodies.

From the explanation of the proposed architecture, it is possible to highlight important fields of research and standardisation, both in academia and industry. For example, the design, standardisation, and development of control protocols and architectural interfaces as have been done for SDN and NFV for classical networks. Next, the study and realization of quantum-classical network slicing and multitenancy. This will be fundamental in future scenarios with coexistence of heterogeneous services managed by multiple operators on the same network infrastructure.

An important role in such proposed architecture and in general in future quantum-classical networks will have data centers, both in the edge and in the cloud. Even the research of where and how to place the control of quantum network functions in data centers' network is still unknown. In particular, this will have to consider that in some cases (e.g., the tactile internet), entanglement generation and distribution will have to satisfy low latency, thus, being performed at the edge or access networks.

Next, the detailed design, analysis, and realization of centralized and distributed control planes are still in its infancy. This is also true for the various instances that may arise for the realization of quantum-classical pps, and, more generally, for quantum-classical network operating systems and software-defined protocols.

These are just few open fundamental challenges that our novel architecture opens to guarantee a seamless integration, operation, and management of future quantum-classical networks.

Data Availability

Data available on request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work has been partially funded by the German Research Foundation (DFG, Deutsche Forschungsgemeinschaft) as part of Germany's Excellence Strategy—EXC2050/1—Project ID 390696704—Cluster of Excellence "Centre for Tactile Internet with Human-in-the-Loop" (CeTI) of Technische Universität Dresden. The work of J. Nötzel was supported via the Emmy-Noether grant no. 1129/2-1 of the German Research Foundation DFG. The work of H. Boche was supported in part by the German Federal Ministry of Education and Research (BMBF) within the national initiative for Post Shannon Communication (NewCom) under Grant 16KIS1003K, and as well as in part by the German Research Foundation (DFG) within Germany's Excellence Strategy EXC-2092-390781972, EXC-2111-390814868 and within the Gottfried Wilhelm Leibniz Prize under Grant BO 1734/20-1. R. Bassoli, J. Nötzel, F. Fitzek, and H. Boche acknowledge the financial support by the Federal Ministry of Education and Research of Germany in the programme of "Souverän. Digital. Vernetzt." joint project 6G-life, project identification numbers: 16KISK001K (RB, FF) and 16KIS1003K (JN, HB).

References

[1] F. H. P. Fitzek, F. Granelli, and P. Seeling, *Computing in Communication Networks - From Theory to Practice*, vol. 1Elsevier, 1st ed., ser. 1 edition, 2020.

[2] R. Bassoli, H. Boche, C. Deppe et al., *Quantum Communication Networks*, Springer, 1st ed. edition, 2021.

[3] R. Bassoli, F. H. Fitzek, and E. Calvanese Strinati, "Why do we need 6G?," *ITU Journal on Future and Evolving Technologies*, vol. 2, no. 6, pp. 1–31, 2021.

[4] W. Kozlowski, S. Wehner, R. Van Meter et al., *IETF quantum internet research group (qirg): Architectural Principles for a Quantum Internet*, International Telecommunication Union, Geneva, 2020.

[5] M. Lévesque and D. Tipper, "A survey of clock synchronization over packet-switched networks," *IEEE Communication Surveys and Tutorials*, vol. 18, no. 4, pp. 2926–2947, 2016.

[6] ITU-T, "G.8271.1/Y.1366.1 – series G: transmission systems and media, digital systems and networks. Packet over transport aspects – synchronization, quality and availability targets," 2020, https://www.itu.int/rec/T-REC-G.8271.1/en.

[7] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," in *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)*, pp. 1–269, 2008.

[8] A. S. Abdalla and V. Marojevic, "Communications standards for unmanned aircraft systems: the 3GPP perspective and research drivers," *IEEE Communications Standards Magazine*, vol. 5, no. 1, pp. 70–77, 2021.

[9] 3GPP, "3GPP TR 22.829 – 3rd generation partnership project; technical specification group services and system aspects; enhancement for unmanned aerial vehicles; stage 1 (release 17)," 2019, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?speci_cationId=3557.

[10] Hexa-X, "D5.1 – initial 6G architectural components and enablers," 2021, https://hexa-x.eu/wp-content/uploads/2022/01/Hexa-X.

[11] H. Zimmermann, "OSI reference model–the ISO model of architecture for open systems interconnection," *IEEE Transactions on Communications*, vol. 28, no. 4, pp. 425–432, 1980.

[12] B. E. Carpenter, *Architectural Principles of the Internet*, vol. 1958 of Internet Requests for Comments, , RFC, 1996.

[13] D. Meyer and G. Zobrist, "TCP/IP versus OSI," *IEEE Potentials*, vol. 9, no. 1, pp. 16–19, 1990.

[14] J. D. Day and H. Zimmermann, "The OSI reference model," *Proceedings of the IEEE*, vol. 71, no. 12, pp. 1334–1340, 1983.

[15] F. M. Burg and N. Di Iorio, "Networking of networks: interworking according to OSI," *IEEE Journal on Selected Areas in Communications*, vol. 7, no. 7, pp. 1131–1142, 1989.

[16] M. P. Clark, "The ATM protocol reference model," in *ATM Networks*, Verlag, 1996.

[17] L. Staalhagen, "A comparison between the OSI reference model and the B-ISDN protocol reference model," *IEEE Network*, vol. 10, no. 1, pp. 24–33, 1996.

[18] A. Viswanathan, E. C. Rosen, and R. Callon, *Multiprotocol Label Switching Architecture*, RFC 3031, 2001.

[19] A. S. Tanenbaum and D. Wetherall, *Computer Networks*, Pearson, 5th Edition. edition, 2011, https://www.worldcat.org/oclc/698581231.

[20] D. Kliazovich, F. Granelli, and N. L. S. Fonseca, "Architectures and cross- layer design for cognitive networks," in *Handbook on Sensor Networks*, Y. Xiao and H. Chen, Eds., pp. 3–24, Idea, 2010.

[21] Z. Guan, L. Bertizzolo, E. Demirors, and T. Melodia, "WNOS: an optimization-based wireless network operating system," *CoRR*, vol. abs/1712.08667, 2017http://arxiv.org/abs/1712.08667.

[22] R. Wen, G. Feng, W. Tan, R. Ni, S. Qin, and G. Wang, "Protocol function block mapping of software defined protocol for 5G Mobile networks," *IEEE Transactions on Mobile Computing*, vol. 17, no. 7, pp. 1651–1665, 2018.

[23] ONOS, "Micro ONOS," 2020, December 2020, https://docs.onosproject.org/.

[24] P4, "P4 consortium," 2020, December 2020, https://p4.org/.

[25] Hexa-X, "D4.1 – AI-driven communication & computation co-design: gap analysis and blueprint," 2021, https://hexa-x.eu/wp-content/uploads/2021/09/Hexa-X-D4.1_v1.0.pdf.

[26] J. Wang, C. Jiang, H. Zhang, Y. Ren, K.-C. Chen, and L. Hanzo, "Thirty years of machine learning: the road to Pareto-optimal wireless networks," *IEEE Communication Surveys and Tutorials*, vol. 22, no. 3, pp. 1472–1514, 2020.

[27] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: a vision for the road ahead," *Science*, vol. 362, no. 6412, 2018https://science.sciencemag.org/content/362/6412/eaam9288.

[28] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum internet: networking challenges in distributed quantum computing," *IEEE Network*, vol. 34, no. 1, pp. 137–143, 2020.

[29] A. Dahlberg, M. Skrzypczyk, T. Coopmans et al., "A Link Layer Protocol for Quantum Networks," in *Proceedings of the ACM Special Interest Group on Data Communication, ser. SIGCOMM '19*, pp. 159–173, New York, NY, USA, 2019.

[30] A. Pirker and W. Dür, "A quantum network stack and protocols for reliable entanglement-based networks," *New Journal of Physics*, vol. 21, no. 3, article 033003, 2019.

[31] J. Nötzel and S. DiAdamo, "Entanglement-enhanced communication networks," in *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, pp. 242–248, Denver, CO, USA, 2020.

[32] J. Nötzel and S. DiAdamo, "Entanglement-assisted data transmission as an enabling technology: a link-layer perspective," in *2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1955–1960, Los Angeles, CA, USA, 2020.

[33] S. Guha, Q. Zhuang, and B. A. Bash, "Infinite-fold enhancement in communications capacity using pre-shared entanglement," in *2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1835–1839, Los Angeles, CA, USA, 2020.

[34] J. Nötzel, "Entanglement-enabled communication," *IEEE Journal on Selected Areas in Information Theory*, vol. 1, no. 2, pp. 401–415, 2020.

[35] J. Nötzel and M. Rosati, "Reducing energy consumption of fiber networks via quantum communication technology," 2022, https://arxiv.org/abs/2201.12397.

[36] A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," *Problems of Information Transmission*, vol. 9, no. 3, pp. 177–183, 1973, http://mi.mathnet.ru/ppi903.

[37] A. S. Holevo, "Coding theorems for quantum communication channels," in *Proceedings. 1998 IEEE International Symposium on Information Theory (Cat. No.98CH36252)*, p. 84, Cambridge, MA, USA, 1998.

[38] S. Guha, "Structured optical receivers to attain superadditive capacity and the Holevo limit," *Physical Review Letters*, vol. 106, no. 24, article 240502, 2011.

[39] M. Rosati, A. Mari, and V. Giovannetti, "Multiphase hadamard receivers for classical communication on lossy bosonic channels," *Physical Review A*, vol. 94, article 062325, 2016.

[40] K. Banaszek and M. Jachura, "Structured optical receivers for efficient deep-space communication," in *2017 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, pp. 34–37, Naha, Japan, 2017.

[41] K. Banaszek, L. Kunz, M. Jachura, and M. Jarzyna, "Quantum limits in optical communications," *Journal of Lightwave Technology*, vol. 38, no. 10, pp. 2741–2754, 2020.

[42] P. Chen, Z. Xie, Y. Fang, Z. Chen, S. Mumtaz, and J. J. P. C. Rodrigues, "Physical-layer network coding: an efficient technique for wireless communications," *IEEE Network*, vol. 34, no. 2, pp. 270–276, 2020.

[43] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[44] M. Rabin, *How to exchange secrets by oblivious transfer*, Harvard University Technical Report 81, 1981.

[45] A. Broadbent and C. Schaffner, "Quantum cryptography beyond quantum key distribution," *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 351–382, 2016.

[46] A. C. A. Nascimento and A. Winter, "On the oblivious-transfer capacity of noisy resources," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2572–2581, 2008.

[47] F. Oggier and G. Zémor, "Coding constructions for efficient oblivious transfer from noisy channels," *IEEE Transactions on Information Theory*, vol. 68, no. 4, pp. 2719–2734, 2022.

[48] H.-K. Lo, "Insecurity of quantum secure computations," *Physical Review A*, vol. 56, no. 2, pp. 1154–1162, 1997.

[49] Y.-H. Chou, G.-J. Zeng, and S.-Y. Kuo, "One-out-of-two quantum oblivious transfer based on nonorthogonal states," *Scientific Reports*, vol. 8, no. 1, p. 15927, 2018.

[50] R. Ahlswede, I. Bjelaković, H. Boche, and J. Nötzel, "Quantum capacity under adversarial quantum noise: arbitrarily varying quantum channels," *Communications in Mathematical Physics*, vol. 317, no. 1, pp. 103–156, 2013.

[51] H. Boche and J. Notzel, "Arbitrarily small amounts of correlation for arbitrarily varying quantum channels," *Journal of Mathematical Physics*, vol. 54, pp. 734–738, 2013.

[52] H. Boche, C. Deppe, J. Nötzel, and A. Winter, "Fully quantum arbitrarily varying channels: random coding capacity and capacity dichotomy," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 2012–2016, Vail, CO, USA, 2018.

[53] H. Boche, R. F. Schaefer, and H. V. Poor, "Denial-of-service attacks on communication systems: detectability and jammer knowledge," *IEEE Transactions on Signal Processing*, vol. 68, pp. 3754–3768, 2020.

[54] A. A. M. Saleh and J. M. Simmons, "All-optical networking—evolution, benefits, challenges, and future vision," *Proceedings of the IEEE*, vol. 100, no. 5, pp. 1105–1117, 2012.

[55] J. Yin, Y.-H. Li, S.-K. Liao et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.

[56] D. K. Oi, A. Ling, G. Vallone et al., "CubeSat quantum communications mission," *EPJ Quantum Technology*, vol. 4, no. 1, 2017.

[57] C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters*, vol. 69, no. 20, pp. 2881–2884, 1992.

[58] S. Lloyd, "Capacity of the noisy quantum channel," *Physical Review A*, vol. 55, no. 3, pp. 1613–1622, 1997.

[59] P. W. Shor, "The quantum channel capacity and coherent information," in *Lecture notes, MSRI Workshop on Quantum Computation*, Springer, 2002.

[60] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 44–55, 2005.

[61] I. Bjelaković, H. Boche, and J. Nötzel, "Entanglement transmission and generation under channel uncertainty: universal quantum channel coding," *Communications in Mathematical Physics*, vol. 292, no. 1, pp. 55–97, 2009.

[62] W. Matthews and S. Wehner, "Finite blocklength converse bounds for quantum channels," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 7317–7329, 2014.

[63] N. Datta, M. Tomamichel, and M. M. Wilde, "On the second-order asymptotics for entanglement-assisted communication," *Quantum Information Processing*, vol. 15, no. 6, pp. 2569–2591, 2016.

[64] D. Vasylyev, A. A. Semenov, W. Vogel et al., "Free-space quantum links under diverse weather conditions,," *Physical Review A*, vol. 96, article 043856, 2017.

[65] D. Dequal, L. T. Vidarte, V. R. Rodriguez, P. V. Giuseppe Vallone, A. Leverrier, and E. Diamanti, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Information*, vol. 7, no. 3, 2021.

[66] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Transactions on Information Theory*, vol. 35, no. 1, pp. 15–29, 1989.

[67] P. Löber, "Quantum channels and simultaneous ID coding," 1999, https://arxiv.org/abs/quant-ph/9907019.

[68] R. Ahlswede and A. Winter, "Strong converse for identification via quantum channels," *IEEE Transactions on Information Theory*, vol. 48, no. 3, pp. 569–579, 2002.

[69] R. Ferrara, R. Bassoli, C. Deppe, F. H. P. Fitzek, and H. Boche, "The computational and latency advantage of quantum communication networks," *IEEE Communications Magazine*, vol. 59, no. 6, pp. 132–137, 2021.

[70] S. J. Nawaz, S. K. Sharma, S. Wyne, M. N. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: state-of the-art and vision for the future," *IEEE Access*, vol. 7, pp. 46317–46350, 2019.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9927255, 15 pages
https://doi.org/10.1155/2022/9927255

Review Article

An Overview on Deployment Strategies for Global Quantum Key Distribution Networks

Jing Wang and Bernardo A. Huberman

Next-Generation Systems, CableLabs, 858 Coal Creek Circle, Louisville, CO 80027, USA

Correspondence should be addressed to Jing Wang; j.wang@cablelabs.com

Received 4 March 2021; Revised 28 December 2021; Accepted 2 April 2022; Published 25 April 2022

Academic Editor: Weizhi Meng

We present a comprehensive literature review and comparative study on the deployment strategies of quantum key distribution (QKD) networks for global coverage. The state-of-the-art deployment strategies, including terrestrial QKD via optical fibers, free-space QKD via ground-based fixed links and ground-to-air dynamic links, and satellite QKD, are reviewed and compared in terms of channel loss, interference, distance limit, connection topology, and deployment cost. Selection criteria and deployment strategies are developed to enable a global coverage of QKD networks from intercontinental, long-haul, metro, to access networks.

1. Introduction

Modern telecommunication relies on cryptography to protect the security of data traffic, where the confidentiality and integrity of keys become the bottlenecks of the whole system. Today's cryptographic systems can be divided into two categories, symmetric and asymmetric. The security of asymmetric cryptographic algorithms, i.e., public key algorithms, relies on the computational complexities of intractable mathematical problems, e.g., the integer factorization problem (RSA), the discrete logarithm problem (Diffie-Hellman), and the elliptic-curve discrete logarithm problem (ECC) [1]. Solving these problems requires tremendous amounts of computational resources. While not feasible for classical computers, these problems can be solved in polynomial time by a quantum computer running Shor's algorithm [1, 2]. To make things worse, increasing the key length does not help, since the required qubit number only scales linearly with the key length [1]. In 2019, Google claimed to have achieved quantum supremacy [3], whereas IBM argued that quantum computers will never reign supreme over, but rather work in concert with classical computers [4]. On the other hand, symmetric cryptographic algorithms, e.g., AES and SNOW 3G, are considered to be resistant against quantum computers. Although Grover's algorithm does speed up the attacks against symmetric ciphers, increasing the key length can effectively block these attacks [1, 5]. In modern communication, symmetric cryptography is only used for encryption and decryption. All other functions, such as signature, authentication, and key exchange, are carried out by asymmetric cryptography. Once sufficiently powerful quantum computers exist, classical cryptography will no longer be safe.

To address the challenges of quantum computing, two technological strategies were developed, postquantum cryptography (PQC) and quantum key distribution (QKD). PQC, also known as quantum-safe or quantum-proof cryptography, focuses on increasing the computational complexity by inventing new intractable problems [5]. Thanks to its software implementation and full compatibility with existing systems, PQC is considered a good candidate for postquantum eras. Three rounds of submissions have been organized by the National Institute of Standards and Technology (NIST) [6–8]. It is worth noting that, like the classical counterparts, PQC algorithms also rely on the assumptions of the computational power of attackers. They are only safe against quantum computers with a certain number of qubits but may lead to long-term issues due to the ever-growing computational power.

QKD, also known as quantum cryptography, relies on quantum mechanics, instead of mathematical assumptions, to guarantee the security of keys [9–12]. Instead of computational security, it offers information-theoretic security, i.e., the keys are deemed secure even if the adversary has unlimited computing power. From the first idea [13] to the first demonstration [14], various QKD protocols [10] and network topologies [11, 12] have been reported. It was found later, however, that the absolute security of QKD is only guaranteed for ideal devices, e.g., single-photon sources and single-photon detectors (SPDs) [15]. The lack of perfect single-photon sources and low detection efficiency of SPDs create security loopholes, which could be exploited by side-channel attacks.

In real systems, expensive single-photon sources are replaced by attenuated lasers to produce weak coherent pulses (WCP), whose photon number per pulse follows the Poisson distribution, so there are always pulses containing multiple photons. Multiphoton pulses could be the target of a photon-number-split (PNS) attack, where an eavesdropper blocks all single-photon pulses and divides multiphoton pulses, keeping half for herself and sending the rest to Bob. To eliminate this loophole, decoy-state protocols were invented to vary the photon number per pulse [16–18] so the blocking strategy of the eavesdropper will be revealed.

On the detector side, measurement-device-independent (MDI) protocols can close all detection loopholes and are immune to side-channel attacks on imperfect detectors [19, 20]. In conventional prepare-and-measure protocols, Alice prepares qubits and sends them to Bob; Bob makes measurements on the received qubits. In MDI protocols, both Alice and Bob prepare random qubits independently and send them to a third party, Charlie, for Bell state measurement (BSM). Charlie can only tell the results of BSM but cannot tell the two photons from Alice and Bob since they are indistinguishable; therefore, he does not know the qubits sent by Alice/Bob. Charlie announces the results of successful BSM events, based on which Alice and Bob infer each other's keys. Since Charlie serves as an untrusted relay, he can be controlled by an eavesdropper without information leakage. The postselection of successful BSM events entangles the qubits from Alice and Bob; that is why MDI-QKD is equivalent to a time-reversed entangled-photon-pair (EPR) protocol. In summary, MDI-QKD with decoy-state protocols eliminates the loopholes on both photon sources and detectors.

So far, QKD technologies have grown out of the laboratory and become ready to reach the market [21, 22]. Various demonstrations and field trials have been reported, including terrestrial QKD via optical fibers, free-space QKD on the ground and in the atmosphere, and satellite QKD between a satellite and a ground station. Meanwhile, quite a few different QKD protocols have also been studied. For terrestrial QKD networks in optical fibers, both discrete-variable protocols, e.g., polarization/phase-encoding BB84, E92, and coherent one way, and continuous-variable protocols have been investigated, and there is no decisive conclusion about the best choice. For free-space and satellite QKD, on the other hand, polarization-encoding BB84 protocol has been used extensively. Terrestrial QKD networks via optical fibers include the DARPA quantum network in Boston [23, 24], SwissQuantum network in Geneva [25, 26], SECOQC network in Vienna [27–30], metropolitan QKD networks in Tokyo [31] and Cambridge [32], and Beijing-Shanghai QKD backbone network in China [33]. QKD links in optical fibers are limited by short transmission distances, less than 600 km in the lab and ~100 km in the field. This is because the key rate scales linearly with channel transmittance, which decays exponentially with distance in optical fibers due to the photon absorption.

There are several strategies to extend QKD distance, including quantum repeater and trusted and untrusted relays. Despite recent advances, a quantum repeater remains infeasible because it requires high-quality quantum memory and complicated local entanglement distillation. Trusted relays can unlimitedly extend QKD distance with the penalty of key exposure since the key information ceases to be quantum at each intermediate node. Untrusted relays seem to be a promising candidate to extend QKD distance. Extensive research effort has been spent on MDI-QKD [34–40] and twin-filed QKD (TF-QKD) [41–48], where Alice and Bob independently prepare random qubits, and both send them to the relay node for measurement. Several field trials of time-bin phase-coding MDI-QKD have been reported in China [34–37], featuring a metropolitan scale of less than 200 km and a key rate of several bits per second [35]. A field trial demonstrated 15-30 km distances from users to the relay node with key rates of 16-38.8 bit/s [37]. More sophisticated three-intensity [38] and asymmetric four-intensity [39, 40] decoy-state protocols were proposed to further extend the distance and increase the key rate. The asymmetric four-intensity decoy-state protocol exploits three intensities (vacuum, weak, and signal states) in the X basis, and one intensity in the Z basis, and archives a distance record of 404 km using ultralow loss optical fibers (0.16 dB/km) with a key rate of only 1.16 bits per hour [40].

The key rates of prepare-and-measure and MDI-QKD protocols scale linearly with the channel transmittance η. Since the channel transmittance decays exponentially with distance in optical fibers, this linear bound severely limits the achievable distances and key rates [41]. Phase-matching QKD [41, 42] and twin-field QKD [43–48] can overcome this linear constraint by matching the phases of two coherent states and encoding key information on the common phase. It makes the key rates scale with the square root of the channel transmittance while keeping the same untrusted relay merit as MDI-QKD. Using a practical sending-or-not-sending (SNS) protocol [41], several milestone experiments have been demonstrated to set new distance records for terrestrial QKD, e.g., 509 km in the lab with ultralow loss fibers [45], 511 km [46] and 428 km [47] in field trials, and 605 km using dual-band stabilization technique for Rayleigh scattering noise reduction [48].

There is another category of QKD protocols, continuous-variable QKD, based on Gaussian modulation and coherent detection [49]. It features higher key rate for a short distance and improved compatibility with commercial coherent optical communication systems [50]. So far,

the distance records of CV-QKD are 200 km in the lab [51] and 50 km in the field [52], making it suitable for metropolitan networks.

The point-to-point (P2P) nature of quantum channels and its requirement of dedicated fibers hamper the wide deployment of terrestrial QKD networks. To enable the coexistence of quantum and classical channels in existing fiber infrastructures, wavelength division multiplexing (WDM) techniques have been investigated [53, 54]. Many works focus on the mitigation of interference caused by spontaneous Raman scattering (SRS) from classical channels [55–58]. So far, the coexistence of quantum and classical channels has been demonstrated in backbone [59, 60], metro [61–64], and access [65–71] networks.

Due to the low channel loss in space and negligible interference from classical channels, satellite QKD drew significant research interest and has been considered as a promising candidate to enable global coverage of QKD networks [72, 73]. The feasibility studies of satellite QKD started back in 2002 [74–76]. The first free-space QKD link on the ground was realized in 1996 [77] with a distance of 150 m (indoor) or 75 m (outdoor). After that, several ground-based fixed free-space QKD links were reported with distances up to 144 km [78–82]. The road toward satellite QKD was paved by the demonstration of dynamic free-space QKD links with airborne quantum transmitters [83, 84] or receivers [85–87]. Ground-based free-space QKD links were investigated as a preliminary step toward satellite QKD, but from the perspective of deployment, they are not quite practical due to the limit of line-of-sight (LoS) connections, geographical constraints (e.g., landscape and buildings), and adverse environmental influences (e.g., vibration, weather, and atmospheric turbulence). In real applications, ground-based free-space QKD links are only suitable for the last segment of access networks.

On the other hand, satellite QKD can achieve distances up to more than 1000 km thanks to the low channel loss in space [88–98]. Most reported works focused on low-earth-orbit (LEO) satellites, where a precise acquisition, pointing, and tracking system is required to follow the fast-moving satellite with high angular speed [88, 89]. The Micius satellite of China at ~500 km altitude realized downlink QKD from the satellite to ground over 1200 km [90]. As a trusted relay, it also enables intercontinental quantum-secured communication over 7600 km between China and Austria [91, 92]. Although the downlink QKD scheme from a satellite to the ground has the potential for higher detection efficiency and higher key rates, it requires more payload on the satellite and is not as flexible as the uplink scheme. An uplink scheme has higher channel loss and low detection efficiency but features a simple payload of quantum receivers on a spacecraft. Micius uses downlink channels for QKD and entanglement distribution and is also compatible with uplink schemes for quantum teleportation [89]. Canada's satellite plan (QEYSSat) employs an uplink scheme [93] and the feasibility of high channel loss [94–96], optical terminal design [97], and noise of SPDs in space [98] have been investigated. To further simplify the payload on satellite, a corner cube retroreflector with a modulator for polarization encoding is proposed [99]. Besides LEO satellites, QKD via medium earth orbit (MEO) [100] and geostationary orbit (GEO) [101, 102] satellites are also under investigation. Miniaturization and standardization of satellites have now become the trends of satellite QKD [103–107].

All aforementioned satellite QKD utilizes the satellite as a trusted relay. To eliminate the key leakage at the satellite, satellite-to-ground entanglement distribution has been demonstrated [108–111] with a distance record of 1200 km [110]. Before that, free-space entanglement distribution on the ground was studied [112–115] with distances of more than 100 km in the atmosphere [113, 115]. Moreover, free-space MDI-QKD was also demonstrated as an alternative to entanglement distribution [116].

Deployment strategies of QKD networks include terrestrial QKD via optical fibers, free-space QKD on the ground or from the ground to an airborne platform, and satellite QKD. Each method has its strengths and limitations and none of them can achieve global coverage alone. So far as we know, there is no comparative study of different deployment strategies. In this paper, we present a literature overview of existing deployment strategies of QKD networks and compare their pros and cons in terms of channel loss, interference, distance, connection topology, deployment cost, and use scenarios. Selection criteria and requirements for different network segments are developed to enable a global coverage of QKD networks, from intercontinental, long-haul, metro, to access networks.

Figure 1 shows a global telecommunication network, which can be divided into four segments, intercontinental (>5000 km), long-haul (1000-5000 km), metro (100-1000 km), and access (<100 km). Each segment features different connectivity topologies. Intercontinental and long-haul networks feature point-to-point (P2P) connectivities; metro networks utilize ring and mesh topologies; access networks have tree or star topologies.

2. Terrestrial QKD via Optical Fibers

Figure 2(a) shows the architecture of a terrestrial QKD link via optical fibers. Ideally, a quantum channel is deployed in a dedicated dark fiber to avoid the interference caused by SRS noise from classical channels. In case of fiber deficiency, it can also share the same fiber with classical channels using time/wavelength-division multiplexing (TDM/WDM) techniques. There are several techniques to reduce the interference from classical channels, such as spectral filtering before the quantum receiver, temporal filtering (i.e., gated SPDs), and power control of classical channels.

Figure 2(b) shows the setup of a prepare-and-measure QKD protocol. So far, several terrestrial QKD networks via optical fibers have been demonstrated, including the DARPA quantum network in Boston [23, 24], SwissQuantum network in Geneva [25, 26], SECOQC network in Vienna [27–30], metropolitan QKD networks in Tokyo [31] and Cambridge [32], and Beijing-Shanghai QKD backbone network in China [33]. Most of them are based on prepare-and-measure protocols with distance limits of hundred kilometers. In real deployments, the usable distance

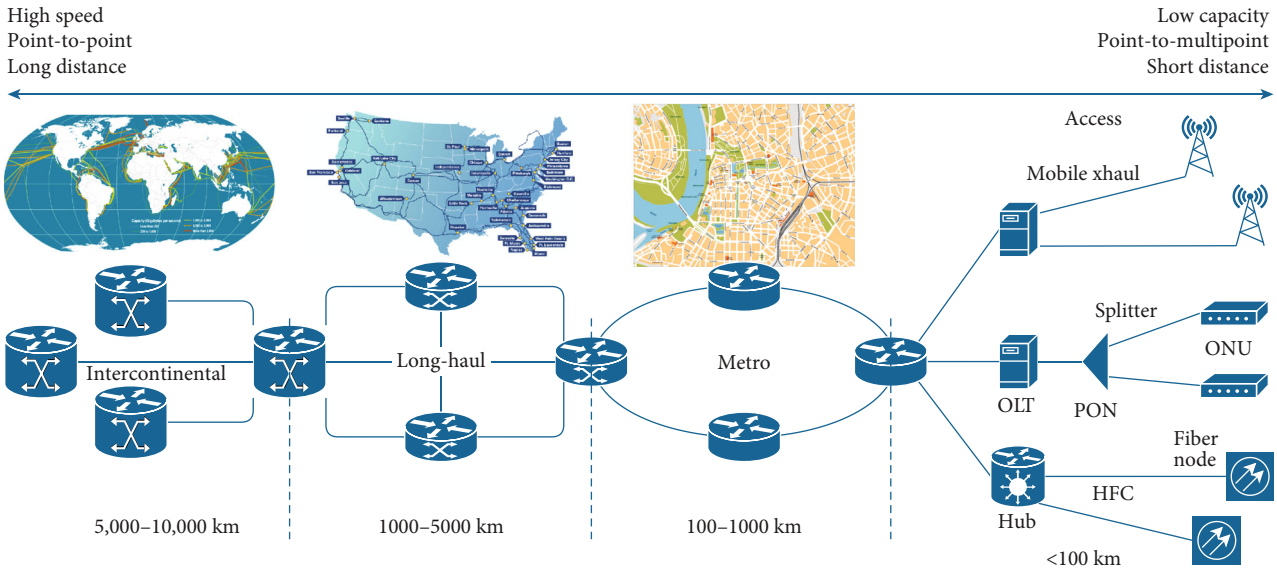

Figure 1: Global coverage of telecommunication networks, from the intercontinental, long-haul, metro, to access networks.

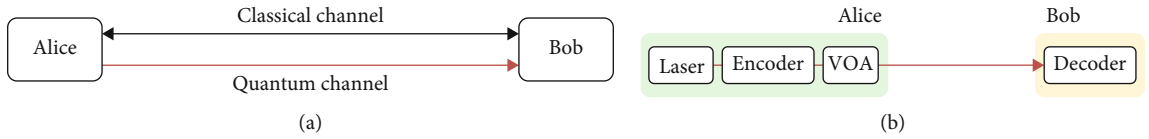

Figure 2: Terrestrial QKD via optical fibers. (a) To avoid interference from classical channels, the quantum channel is deployed in a dedicated fiber. (b) The setup of a prepare-and-measure protocol.

will be further reduced to ~100 km. This is because the achievable key rate scales linearly with channel transmittance, which decays exponentially with distance in optical fibers due to absorption. Therefore, terrestrial QKD via optical fibers is impractical for long-haul applications. For example, with a loss of 0.2 dB/km, a 1000 km fiber introduces a channel loss of 200 dB, which is so high that only 0.3 photons arrive at the receiver per century even if a 10 GHz single-photon source was used at the transmitter.

Relay technologies are essential to increase the distance and enhance the coverage area of terrestrial QKD networks. There are two categories of relaying technologies, trusted and untrusted, depending on whether the relay node has access to the keys. The operation principles of a trusted relay node are shown in Figure 3(a). It connects two neighboring nodes that are too far away from each other to establish a direct QKD link. The trusted relay node, Charlie, performs QKD with Alice and Bob, respectively, and obtains keys of K_A and K_B. He then makes a parity announcement of $K_C = K_A \oplus K_B$, which is a bitwise parity check of K_A and K_B. Since the original keys are independent bit strings, their bitwise parity is a uniformly random bit string, which does not reveal any information about the keys. With the help of K_C, both Alice and Bob can then infer the key of each other using the fact that $K_A \oplus (K_A \oplus K_B) = K_B$ and $K_B \oplus (K_A \oplus K_B) = K_A$. Trusted relay can extend the distance of secure communication unlimitedly, but with the penalty of key exposure at each relay node.

An interesting synergy is that classical fiber cables have repeaters every 100 km for the reamplification, reshaping, and retiming of classical pulses. Trusted relay nodes can be deployed at the same locations as classical repeaters. Since classical repeaters have fixed and public locations, relay nodes collocated with repeaters will be subject to constant surveillance and probing. For example, the Beijing-Shanghai backbone link in China uses 32 trusted relay nodes to divide the overall distance of more than 2000 km into many small segments, each less than 100 km. Moreover, a trusted relay node offers compatibility to the point-to-multipoint (P2MP) network topology, as shown in Figure 3(b).

On the other hand, an untrusted relay eliminates the key leakage at the relay node. It can be implemented by the distribution of entangled photon pairs or measurement-device-independent (MDI) QKD. In either case, the relay node has no information on the keys and could even be an eavesdropper itself. Figure 4(a) shows an entanglement distribution setup, where an entangled photon source at the relay node generates entangled photon pairs (EPR) using a nonlinear crystal or nonlinear fibers. The entangled photons are distributed to two users, who make independent measurements and get correlated results. The relay node is considered secure since the entangled photon source has no access to the exact states of two photons, but the measurement results of two users are always correlated. Figure 4(b) shows an MDI-QKD setup. Two users prepare random qubits

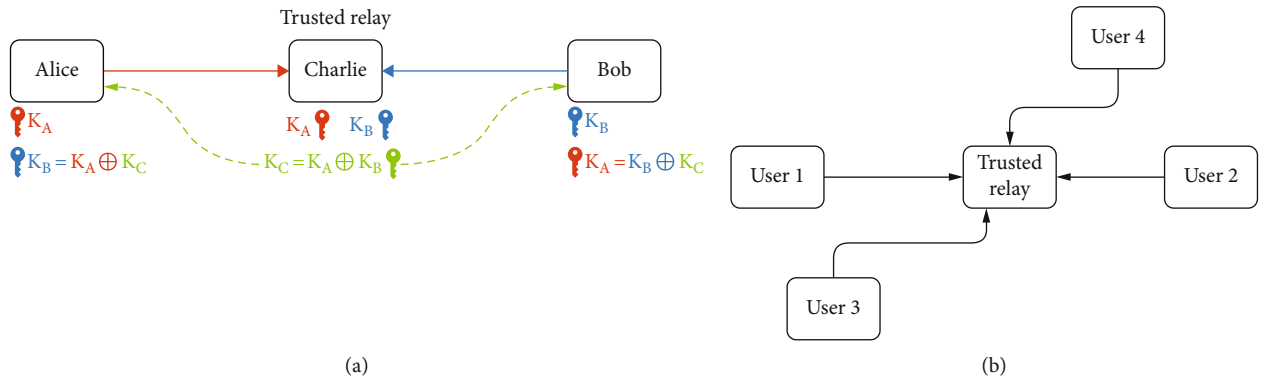

Figure 3: Trusted relay for terrestrial QKD networks. (a) The operation principles of a trusted relay. (b) A trusted relay node offers compatibility with point-to-multipoint networks.

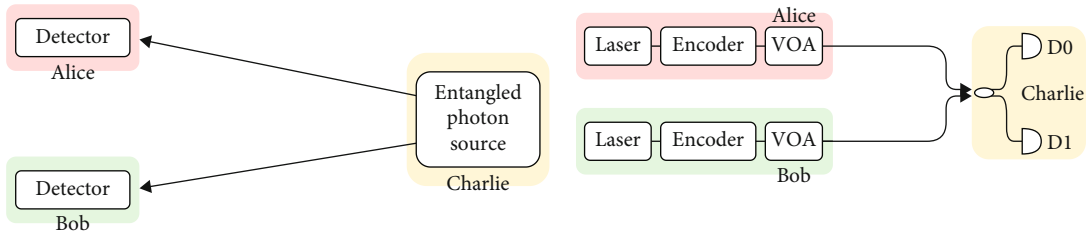

Figure 4: Untrusted relay for terrestrial QKD networks. (a) Distribution of entangled photon pairs. (b) Measurement-device-independent (MDI) QKD.

independently and send them to the relay node for Bell state measurements (BSM). Although the BSM cannot tell the exact states of two incoming photons, it can tell whether or not the two photons have entangled states. By postselecting entangled photons from the two users, MDI-QKD is equivalent to a time-reversed EPR protocol. So far, the distance record for MDI-QKD is 404 km using asymmetric four-intensity decoy-state protocol in ultralow loss optical fibers [40]. The key rate, however, is only 1.16 bit/s per hour, which is orders of magnitude lower than practical requirements.

The key rate of conventional QKD, including prepare-and-measure protocols, entanglement distribution, and MDI-QKD, has linear dependency on the channel transmittance η. Since the channel transmittance decays exponentially with distance in optical fibers, this linear bound severely limits the achievable key rate and distance of terrestrial QKD networks. Recently, a new QKD protocol, twin-field (TF) QKD, was proposed to overcome the linear key-rate constraint. Its setup is almost identical to a phase-encoding MDI-QKD and maintains the same merit of an untrusted relay, where pairs of phase-randomized optical fields are generated at two distant locations and combined at a central measuring station. Fields imparted with the same random phase are "twins" and can be used to distill a key. By matching the phases of two coherent states and encoding key information into the common phase, TF-QKD exhibits the same dependence on distance as quantum repeaters, i.e., its key rate scales with the square root of the channel transmittance. Several milestone experiments have been demonstrated to set new distance records of fiber-based terrestrial QKD links [45–48]. It should be noted that in MDI-QKD, the two photons from two users interfere at the relay station, where Charlie's receiver has two-photon interference and records coincidence detections. In TF-QKD, however, two optical fields are sent from two users to Charlie's receiver, where a single-photon interference is carried out followed by a single-photon detection event. TF-QKD retains the characteristics of MDI-QKD, whereas gaining extra distance thanks to the square-root dependence of key rate on the channel transmittance.

3. Free-Space QKD

Figure 5 shows the architectures of free-space QKD. Figure 5(a) shows ground-based free-space QKD links. Different from optical fibers, free-space QKD requires LoS connections, and the transmitters and receivers are usually deployed on top of buildings or mountains to avoid obstruction in the path. The associated classical channels could exploit wireless links, e.g., cellular, microwave, or rely on free-space optics as well. Since no fiber trenching is required, free-space QKD features low deployment cost and easy and fast installation and is an important reinforcement for fiber-based QKD networks owing to its configurational flexibility. The distance record for ground-based free-space QKD is 144 km [82]. Dynamic free-space QKD links to/from an aircraft were investigated as a preliminary step toward satellite QKD, and the feasibility of both downlink and

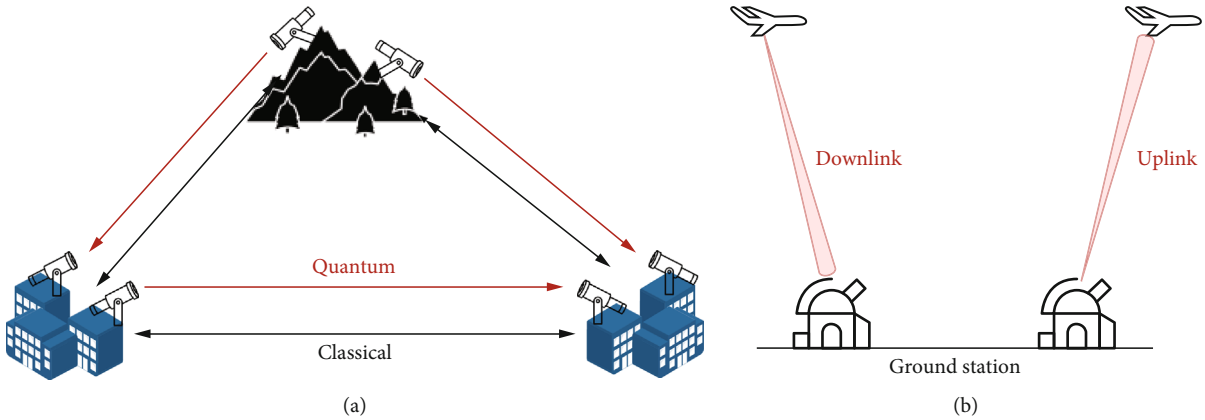

Figure 5: Free-space QKD. (a) Ground-based free-space QKD links. (b) Free-space QKD links to/from an aircraft.

uplink configurations has been verified, shown in Figure 5(b). A downlink scheme includes a flying transmitter on an airborne platform and a receiver on the ground [83, 84]; an uplink configuration uses a ground-based transmitter and places a quantum receiver on aircraft [86, 87]. The downlink scheme has higher detection efficiency, whereas the uplink scheme has a smaller payload on aircraft.

Since the quantum channel is not confined in the waveguide of optical fibers, free-space QKD is subject to environmental influence, such as vibration, adverse weather (fog, rain, and cloud), and atmospheric turbulence. Although the atmosphere has lower absorption than optical fibers, only 0.07 dB/km at 2400 m, the channel loss of free-space QKD is not dominated by absorption. Instead, it is determined by diffraction, weather, turbulence, and misalignment. Moreover, free-space quantum channels are subject to decoherence more than those in optical fibers, which further limits the link distance. On the other hand, there is no interference from classical channels in free space and the coexistence of quantum and classical channels is no longer an issue. Free-space QKD can easily support P2MP topologies, making it a promising candidate for interbuilding secure communication in the last few miles of access networks.

4. Satellite as a Trusted Relay

Thanks to the low channel loss in space, negligible interference from classical channels, and reduced environmental influences, satellite QKD can achieve distances more than 1000 km and is not limited by terrestrial conditions and can provide coverage for rural areas. Most reported work focused on LEO satellites with altitudes of less than 900 km, where a precise acquisition, pointing, and tracking system is required to follow the fast-moving satellite. The feasibility of MEO and GEO satellites is also under investigation. Miniaturization and standardization of satellites are also trends of satellite QKD. Figure 6 shows the operation principles of satellite QKD where the satellite is used as a trusted relay. An LEO satellite performs downlink QKD with two ground stations, Alice and Bob, respectively. It then makes a parity announcement so that Alice and Bob can infer each other's keys. The satellite needs LoS connections with Alice and Bob, but not necessarily at the same time. It can exchange keys with several ground stations one after another as it flies over them. As a trusted relay, any access to the satellite leaks the complete information about keys. The associated classical channels for satellite QKD can rely on terrestrial fibers, microwave, or free-space laser communication in space. For example, most Starlink satellites are currently operating in Ku and Ka bands and can be upgraded to laser communication in the future.

Since the effective thickness of the atmosphere is only ~10 km, the propagation of a quantum channel takes place mostly in vacuum space with negligible absorption and turbulence. Instead of absorption, the channel loss of satellite QKD is determined by beam diffraction and scales quadratically with distance. In comparison, the channel loss of terrestrial QKD is dominated by fiber absorption and scales exponentially with distance. Channels in space also have smaller decoherence than those in the atmosphere or optical fibers. For example, a 600 km optical fiber has a channel loss of 120 dB, whereas a link of the same length in space from satellite to the ground has a loss of only 50 dB given a reasonable aperture size is used at the receiver telescope. This is why satellite QKD can reach much longer distances. Intersatellite channels have even lower losses due to the absence of atmosphere.

Channel loss in space comes from two sources, beam diffraction and beam spreading beyond the effects of diffraction. Diffraction loss depends on the divergence of the transmitter telescope and the aperture size of the receiver telescope. Further beam spreading arises from wavefront aberrations caused by refractive index inhomogeneities due to atmospheric turbulence. There are two categories of turbulence. Small turbulence induces beam spreading, whereas large turbulent eddies with sizes larger than the beam spot cause beam wandering. A long-term beam spot is a superposition of moving short-term beam spots. The short-term beam size is determined by spreading and the instantaneous beam displacement from the unperturbed position caused by beam wandering. In real applications, the channel loss from a satellite to a ground station is dominated by diffraction, followed by beam spreading. Beam wandering and absorption have negligible contributions to the channel loss.

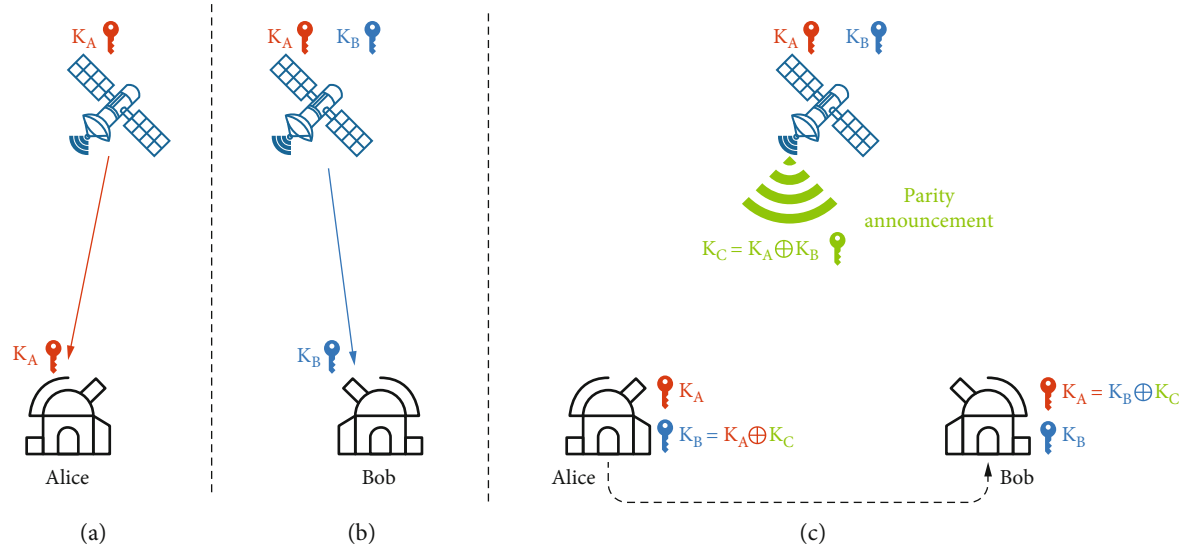

Figure 6: Satellite QKD using the satellite as trusted relays. The relay satellite first exchanges keys with ground stations, (a) Alice and (b) Bob, respectively. (c) The satellite makes a parity announcement so that Alice and Bob can infer each other's keys.

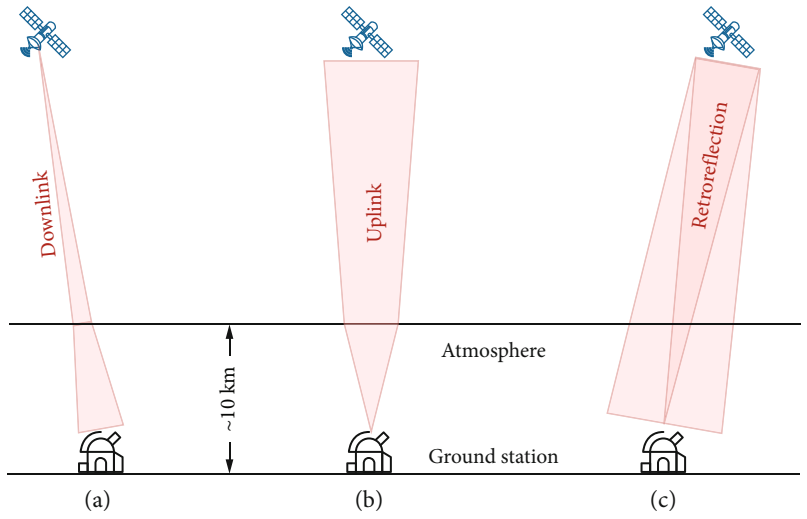

Figure 7: (a) Downlink and (b) uplink configurations of satellite QKD.

Satellite QKD has three different schemes, downlink, uplink, and retroreflection. In Figure 7(a), the downlink scheme has the quantum transmitter on a satellite and receiver on the ground. Since the effective thickness of the atmosphere is only ~10 km, the optical beam first propagates through vacuum space where the only channel loss is diffraction and then passes through the atmosphere in the final stage of the path. Due to the diffraction effect, when the beam arrives at the atmosphere, its size has been larger than most turbulent eddies. There is no beam wandering, and the beam size is spread slightly by wavefront aberrations caused by turbulence. For the downlink configuration, atmospheric turbulence has a limited impact on the channel loss and beam spreading. For example, the beam size after 1200 km downlink propagation expands to 12 m with diffraction loss of ~22 dB depending on the receiver telescope size [90]. Atmospheric turbulence introduces additional 3-8 dB attenuation, with an overall channel loss of less than 30 dB [90].

In Figure 7(b), an uplink channel first propagates through the atmosphere, where the wavefront aberration induced by turbulence causes significant beam spreading. At 500 km altitude, the beam size of an uplink channel can reach up to 50 m, much larger than any available spaceborne telescope aperture. Downlink channels can exploit large aperture receiver telescopes on the ground, but uplink channels have limited aperture size for receiver telescopes due to the weight and size limit on satellites. Thanks to the strong wavefront aberration, large beam spot, and small aperture size, uplink channels have higher losses than downlink ones. For example, a 500 km uplink channel has a loss up to 50 dB, whereas a downlink channel of the same length would have a loss less than 20 dB [94]. Most uplink channels cannot work without the help of the decoy-state technique [94].

Although the downlink scheme has higher detection efficiency and higher key rates, the transmitter setup requires more payload on the satellite and needs more adjustment during operation, which makes the downlink scheme not as flexible as an uplink configuration. The uplink scheme, on the other hand, only needs a simple payload of quantum receivers on the satellite, enabling an easier operation on the satellite. The downlink scheme leaves expensive and delicate SPDs on the ground for better protection, cooling, and maintenance, whereas the uplink scheme has to launch the sensitive SPDs into space, which have to go through launch vibration, shock in the flight, extreme temperature, and work under adverse conditions in space. Due to the sunlight, the satellite temperature varies by up to tens of degrees in one orbit, and there is limited electrical power on the satellite for cooling. The only way to dissipate heat is by radiation. To make things worse, most SPDs are avalanche photon detectors (APD), which are sensitive to dark counts caused by ionizing radiation in space. The feasibility of low-noise SPDs on a satellite is under investigation [98]. So far, downlink and uplink schemes are both considered important for future satellite QKD. For example, Micius uses downlink QKD and entanglement distribution, and it is also compatible with uplink for quantum teleportation [89]. Canada's satellite plan (QEYSSat) employs an uplink scheme [93], and many works have been done to verify the feasibility of high channel loss [94–96], optical terminal design [97], and noise of SPDs in space [98].

In a quantum channel, the qubits are carried by single photons and no amplification is allowed. The only way to increase the signal-to-noise ratio (SNR) is to reduce channel loss and background noise. Thanks to the low loss, downlink channels have larger SNR than uplink ones. In the daytime, the background noise from sunlight makes it difficult to establish a QKD link. One way to improve SNR in the daytime is to use the wavelengths at Fraunhofer lines, i.e., Sun absorption lines. At night, background noise is dominated by moonlight and scattered light from human activities, which depends on the location of the ground stations. SNR at night is orders of magnitude higher than that in the daytime, which is why most satellite QKD works were demonstrated at clear night by downlink channels. There are several techniques to improve the SNR of a free-space quantum link, e.g., reducing the beam size, reducing the field of view of the receiver telescope, narrowband spectral filtering before the receiver, and temporal filtering (gating window) of SPDs.

To further simplify the payload on satellites, a third configuration, retroreflection, was proposed [99, 100], as shown in Figure 7(c). It uses an orbiting corner cube retroreflector on a satellite with a modulator to encode polarizations. The single-photon transmitter is realized by corner cube retroreflectors mounted on a satellite. Only the reflected beam from the satellite to the ground is a quantum channel; the laser beam from the ground station to the satellite has bright classical pulses. This configuration features a compact and low-cost payload on satellite and can be used on not only LEO but also MEO and GEO satellites. The feasibility of single-photon exchange from an MEO satellite using a retroreflection scheme has been verified [100].

5. Satellite as an Untrusted Relay

When a satellite is used as a trusted relay, it has access to all the keys of all ground stations. To avoid the key leakage at the satellite, untrusted relaying is preferred since the eavesdropper gets no information even if it takes full control of the satellite. Figure 8 shows the architecture of satellite QKD with the satellite as an untrusted relay. Figure 8(a) shows entanglement distribution, where an entangled photon source on a satellite sends entangled photons down to two ground stations, Alice and Bob, respectively. Alice and Bob make independent measurements on the incoming photons and get correlated results. Since the entangled photon source has no control over the exact qubits carried by each photon, the satellite has no information of the key. For entanglement distribution, the loss of two downlink channels has to be combined since only photon pairs that both arrive at ground stations can be used for keys.

As an alternative, Figure 8(b) shows satellite MDI-QKD, where two ground stations independently prepare random qubits and send them via uplink channels to a satellite for BSM. Satellite MDI-QKD is equivalent to a time-reversed entanglement distribution protocol. The BSM can only tell whether or not the two photons are entangled, but it cannot tell the exact states of two incoming photons. The loss of two uplink channels has to be combined since only photon pairs that both arrive at the satellite can be used for keys. Due to the high loss of uplink channels, there is no demonstration of satellite MDI-QKD so far. But the feasibility study of free-space MDI-QKD has been reported on the ground over 19.2 km [116], well beyond the effective thickness of the atmosphere (~10 km).

Unlike trusted relaying, untrusted relaying requires simultaneous LoS connections from the satellite to both ground stations, which limits the separation distance between ground stations. For a given altitude of the satellite, wider separation between ground stations makes lower slant angles and longer propagation in the atmosphere, which leads to higher channel loss. The current distance record for entanglement distribution is ~1200 km, achieved by an LEO satellite Micius of China [110].

6. Deployment Strategies for Global Coverage of QKD Networks

Table 1 lists the pros and cons of different deployment strategies of QKD networks, including fiber-based terrestrial QKD, free-space QKD including ground-based and ground-to-air schemes, and satellite QKD with the satellite used as a trusted or untrusted relay. Terrestrial QKD via optical fibers suffers from high channel loss and short distance but offers compatibility with existing fiber infrastructure and P2MP topologies. Since the quantum channels are confined in fiber waveguides, terrestrial QKD networks can operate all day in adverse environments, such as background light, weather, and vibration. Without relays, a single span of fiber-based QKD can reach ~100 km in the field, only suitable for metro and access networks. Trusted relaying can unlimitedly extend the distance of fiber-based QKD with

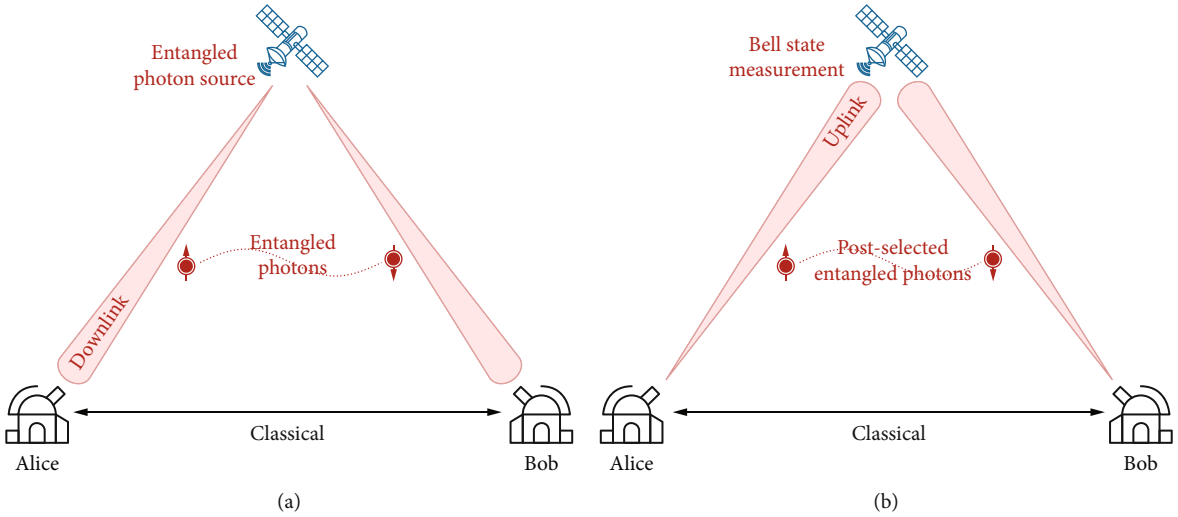

FIGURE 8: Satellite QKD with the satellite as an untrusted relay. (a) Entanglement distribution from a satellite. (b) Free-space MDI-QKD to a satellite.

the penalty of key leakage at each relay node. An interesting synergy is that classical fiber cables also have repeaters every 100 km. Trusted relay nodes can be deployed at the same locations as classical repeaters. Since classical repeaters have fixed and public locations, relay nodes collocated with repeaters will be subject to constant surveillance and probing. In contrast, satellite QKD using a satellite as a trusted relay is more secure because the satellite and quantum links are moving fast, making side-channel attacks difficult.

Ground-based free-space QKD requires LoS connections, and the transmitters and receivers are usually deployed on top of buildings or mountains to avoid obstruction in the path. It supports P2MP topology and can handle the coexistence of quantum and classical channels without interference. These features make it suitable for the last few miles of access networks among buildings. Although the atmosphere has lower absorption, the channel loss of free-space QKD is dominated by diffraction, adverse weather, and atmospheric turbulence. The distance record of ground-based free-space QKD is 144 km [78], but in real deployments, the usable distance will be less than 10 km for practical key rates. Since no fiber trenching is required, ground-based free-space QKD features low deployment cost and fast and easy installation and serves as an important reinforcement for fiber-based QKD networks. The ground-to-air free-space QKD shares the same pros and cons of ground-based counterparts plus the additional channel loss caused by misalignment and vibration due to the movement of the aircraft. We do not include the applications of airborne free-space QKD here, since it was mainly investigated as a preliminary step towards satellite QKD.

Compared with terrestrial and free-space QKD, satellite QKD features low channel loss and long distances. The downlink scheme from satellite to the ground has higher detection efficiency and higher key rates thanks to the lower loss and less turbulence-induced wavefront abbreviation. But it requires more payload on the satellite and needs more adjustment during operation. The uplink channels are more flexible, since it only needs a simple payload of quantum receivers on the satellite, enabling an easier operation on the satellite. On the other hand, the downlink scheme leaves expensive and delicate SPDs on the ground for the easiest maintenance, whereas the uplink scheme launches the sensitive SPDs into space, which have to go through the launch vibration, shock in the flight, extreme temperature, and work under adverse conditions in space.

Satellite QKD requires LoS connections between the satellite and ground stations and only works at night due to the background noise from sunlight during the daytime. To reduce the channel loss, LEO satellites are preferred, but low altitude leads to the fast movement of the satellite, a small coverage area, and a short flyover time window for each ground station. MEO satellites at higher orbit provide wider coverage and longer flyover time, but with the penalty of higher channel loss and lower key rate [100]. To choose an appropriate altitude, a trade-off must be made between the coverage area and time window versus channel loss and key rate. An extreme example is a geostationary orbit (GEO) satellite, which has an operational time window of the whole night but with a long path length of 35,786 km [101, 102]. There is a strong synergy between satellite QKD and classical satellite communication. For example, space communication also exploits LEO satellites at an altitude of 300-1000 km. Starlink plans to launch thousands of satellites at altitudes of 350-580 km. Although these satellites are using microwave communication in Ku and Ka bands, most of them are equipped with optical transceivers for future upgrades to laser communication. By adding quantum transmitters onboard, these satellites can be used as a trusted relay for QKD in space. Since quantum transmitters for most prepare-and-measure protocols only consist of commercial off-the-shelf devices, this upgrade will not significantly increase the satellite cost. The beam acquisition, tracking, and pointing systems designed for laser communication in space can also be reused by quantum channels. Satellite QKD covers long-haul networks, and by using the

Table 1: Pros and cons of terrestrial, free-space, and satellite QKD.

Deployment strategies	Terrestrial QKD via optical fibers	Free-space QKD on ground	Free-space QKD ground-to-air	Satellite QKD (trusted relay)	Satellite QKD (untrusted relay)
Attenuation	Fiber absorption	Diffraction Turbulence Weather Absorption	Same as ground-based QKD plus Misalignment Vibration	Diffraction Turbulence Weather	Diffraction Turbulence Weather
Interferences from classical channels	Spontaneous Raman scattering noise	No	No	No	No
Channel loss	High, scale exponentially with fiber length	High, scale exponentially with distance		Low Scale quadratically with distance	
Distance	~100 km in fields without relay Unlimited distance with trusted relay MDI-QKD: 404 km in the lab [40] 200 km in fields [35] TF-QKD: >500 km in lab [45, 46, 48] 428 km in fields [47]	144 km in experiments [82] <10 km in real fields	96 km in experiments [84]	Satellite to the ground distance over 1200 km [90] Unlimited distance between ground stations	1200 km between ground stations for a 500-km altitude LEO satellite Longer for MEO/GEO
Compatibility to P2MP topology	P2MP	P2MP	P2P at a time	P2P at a time	Satellite to two ground stations
Line of sight	No	Yes	Yes	Yes	Simultaneous LoS with both ground stations
Time window	Whole day	Only night Need special care for daytime operation		Short window in the clear night	
Deployment	Low cost Dedicated fiber or reuse existing ones	Low cost Simple and fast installation No fiber trenching		Expensive and slow Synergy with satellite laser communication in space	
Application scenarios	Metro, access	Last few miles of access networks		Long haul	

satellites as a trusted relay, its secure distance can be extended unlimitedly.

The scheme with a satellite as an untrusted relay shares the same pros and cons with trusted relays but eliminates the key leakage at satellites. It requires simultaneous LoS connections from the satellite to both ground stations, which limits the separation between two ground stations. The distance record of entanglement distribution from a satellite is 1200 km, which can be employed for long-haul networks, but not long enough for intercontinental connections. Figure 9 shows the deployment strategies for global coverage of QKD networks, from the intercontinental, long-haul, metro, to access networks.

It should be noted that not all user devices are equipped with optical terminals for fiber or free-space optics connections. Radio access has been and will continue to be used extensively in the last few miles of access networks. In these cases, keys have to be distributed wirelessly in a classical way to user devices. Figure 10 shows a hierarchical key delivery architecture. Several secure sites, e.g., bank buildings, business campuses, and government offices, are connected by satellite, fiber-based, or free-space QKD links, so the keys are delivered in an absolute secure way among these secure sites. Within each secure site, however, the keys are distributed wirelessly to mobile users using PQC algorithms. This is a trade-off between security and mobility because it is not feasible to connect all devices with optical fibers or free-space optics. We have to leverage the ubiquity and flexibility of radio access technologies in the last few miles. In this hierarchical architecture, two different levels of security-as-a-service (SaaS) are provided, i.e., absolute security over long-distance among secure sites and computational classical security over a short distance within each site. Once the mobile users

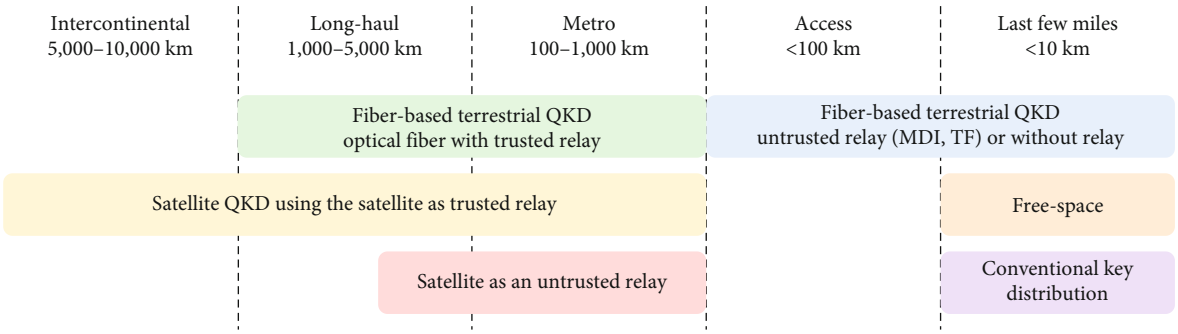

Figure 9: Deployment strategies for global coverage of QKD networks.

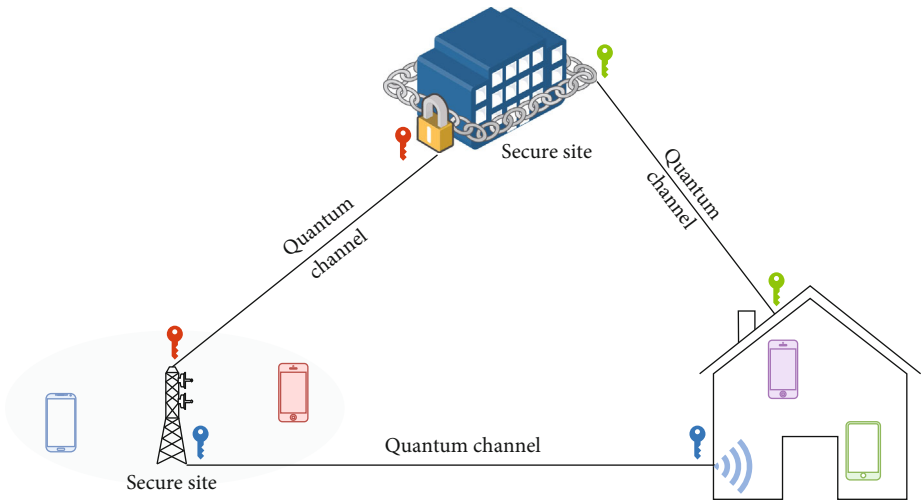

Figure 10: Hierarchical key delivery in the last few hundred meters.

get the keys, they can use these keys to encrypt their wireless communication. They can even roam away from the secure site and continue the secure communication as soon as they still possess the keys. Once they consume all the keys, they have to return to a secure site to fetch new keys. It should be noted that PQC and QKD do not necessarily compete with each other. Instead, they should work in an orchestrated way to complement each other. For example, PQC could exploit the keys delivered by QKD to enhance its security, while QKD can employ PQC for authentication, which cannot be handled by QKD itself.

7. Conclusions

To date, many deployment strategies of QKD networks have been demonstrated, but none of them provides global coverage of QKD networks. A comparative study on the pros and cons of various deployment strategies is still missing. In this paper, the state-of-the-art deployment technologies of QKD networks, including fiber-based terrestrial QKD, free-space QKD, and satellite QKD, are compared in terms of channel loss, interference, distance limit, connection topology, deployment cost, and application scenarios. Instead of competing with each other, these different deployment strategies will work in an orchestrated way to complement each other and enable a global coverage of QKD networks, from intercontinental, long-haul, metro, to access networks.

Given its compatibility with P2MP topology and ~100 km distance limit without relay, fiber-based terrestrial QKD is suitable for metro and access networks. With the help of a trusted relay, the QKD distance can be extended unlimitedly to cover long-haul networks, where the relay nodes are collocated with classical fiber repeaters. Ground-based free-space QKD is limited to 10 km due to diffraction, weather, and atmosphere turbulence and is suitable for the last few miles among buildings in access networks. Satellite QKD features low channel loss, high key rates, and long distances more than 1000 km. By utilizing satellites as trusted relays, the QKD distance can be extended infinitely and can be used for intercontinental, long-haul, and metro networks. Furthermore, satellite QKD is not restricted by terrain conditions and can reach rural underserved areas without difficulty. On the other hand, using a satellite as an untrusted relay requires simultaneous LoS connections from the satellite to both ground stations, where the separation between the ground stations is limited by the altitude of the satellite.

Data Availability

Data are not available.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[2] E. Grumbling and M. Horowitz, *Quantum Computing: Progress and Prospects*, The National Academies Press, Washington, 2019.

[3] F. Arute, K. Arya, R. Babbush et al., "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[4] IBM Research Blog, *On Quantum Supremacy*, vol. 22, 2019, Oct 2019.

[5] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds., Springer, Berlin, Heidelberg, 2009.

[6] L. Chen, S. Jordan, Y.-K. Liu et al., *Report on Post-Quantum Cryptography*, NISTIR 8105, 2016.

[7] G. Alagic, J. Alperin-Sheriff, D. Apon et al., *Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8240, 2019.

[8] G. Alagic, J. Alperin-Sheriff, D. Apon et al., *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8309, 2020.

[9] C. H. Bennett, "Quantum cryptography: uncertainty in the service of privacy," *Science*, vol. 257, no. 5071, pp. 752-753, 1992.

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, 2002.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, pp. 1301–1350, 2009.

[12] H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014.

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, Bangalore, India, December 1984.

[14] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[15] D. Gottesman, L. Hoi-Kwong, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Information & Computation*, vol. 4, no. 5, pp. 325–360, 2004.

[16] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, article 057901, 2003.

[17] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Physical Review Letters*, vol. 94, no. 23, article 230503, 2005.

[18] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, no. 23, article 230504, 2005.

[19] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, article 130503, 2012.

[20] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H. K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 112, no. 19, article 190503, 2014.

[21] J. Qiu, "Quantum communications leap out of the lab," *Nature*, vol. 508, no. 7497, pp. 441-442, 2014.

[22] M. Peev, "Why do I believe that quantum key distribution (QKD) is finally about to reach telecom markets and grow out of its present exotic standing?," in *Optical Fiber Communications Conference (OFC) 2019, paper W4D.3*, San Diego, CA, 2019.

[23] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Building the quantum network," *New Journal of Physics*, vol. 4, p. 46, 2002.

[24] C. Elliott, A. Colvin, D. Pearson et al., "Current status of the DARPA quantum network," *Quantum Information and Computation III*, vol. 5815, 2005.

[25] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New Journal of Physics*, vol. 12, article 063027, 2010.

[26] D. Stucki, M. Legré, F. Buntschu et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, article 123001, 2011.

[27] A. Poppe, M. Peev, and O. Maurhart, "Outline of the SECOQC quantum-key-distribution network in Vienna," *International Journal of Quantum Information*, vol. 6, no. 2, pp. 209–218, 2008.

[28] M. Peev, T. Länger, T. Lorünser et al., "The SECOQC quantum-key-distribution network in Vienna," in *Optical Fiber Communication Conference (OFC) 2009*, 2009, paper OThL2.

[29] M. Peev, A. Poppe, O. Maurhart, T. Lorünser, T. Langer, and C. Pacher, "The SECOQC Quantum Key Distribution Network in Vienna," in *35th European Conference on Optical Communication*, Vienna, Austria, 2009, paper 1.4.1.

[30] M. Peev, C. Pacher, R. Alléaume et al., "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics*, vol. 11, article 075001, 2009.

[31] M. Sasaki, M. Fujiwara, H. Ishizuka et al., "Field test of quantum key distribution in the Tokyo QKD network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[32] J. F. Dynes, A. Wonfor, W. S. Tam et al., "Cambridge quantum network," *Nature Partner Journals (NPJ) Quantum Information*, vol. 5, article 101, 2019.

[33] Q. Zhang, F. Xu, Y.-A. Chen, C. Z. Peng, and J. W. Pan, "Large scale quantum key distribution: challenges and solutions [invited]," *Optics Express*, vol. 26, no. 18, pp. 24260–24273, 2018.

[34] Y. Liu, T. Y. Chen, L. J. Wang et al., "Experimental measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 111, article 130502, 2013.

[35] Y. L. Tang, H. L. Yin, S. J. Chen et al., "Measurement-device-independent quantum key distribution over 200 km," *Physical Review Letters*, vol. 113, article 190501, 2014.

[36] Y. L. Tang, H. L. Yin, S. J. Chen et al., "Field test of measurement-device-independent quantum key distribution," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, article 6600407, pp. 116–122, 2015.

[37] Y. L. Tang, H. L. Yin, Q. Zhao et al., "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Physical Review X*, vol. 6, article 011024, 2016.

[38] X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," *Physical Review A*, vol. 87, no. 1, article 012320, 2013.

[39] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, "Making the decoy-state measurement-device-independent quantum key distribution practically useful," *Physical Review A*, vol. 93, article 042324, 2016.

[40] H.-L. Yin, T.-Y. Chen, Z.-W. Yu et al., "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, no. 19, article 190501, 2016.

[41] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, pp. 400–403, 2018.

[42] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Physical Review X*, vol. 8, article 031043, 2018.

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

[44] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Physical Review A*, vol. 98, no. 6, article 062323, 2018.

[45] J.-P. Chen, C. Zhang, Y. Liu et al., "Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km," *Physical Review Letters*, vol. 124, no. 7, article 070501, 2020.

[46] J. P. Chen, C. Zhang, Y. Liu et al., "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, pp. 570–575, 2021.

[47] H. Liu, C. Jiang, H. T. Zhu et al., "Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km," *Physical Review Letters*, vol. 126, article 250502, 2021.

[48] M. Pittaluga, M. Minder, M. Lucamarini et al., "600-km repeater-like quantum communications with dual-band stabilization," *Nature Photonics*, vol. 15, pp. 530–535, 2021.

[49] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters*, vol. 88, no. 5, article 057902, 2002.

[50] H. Guo, Z. Li, S. Yu, and Y. Zhang, "Toward practical quantum key distribution using telecom components," *Fundamental Research*, vol. 1, no. 1, pp. 96–98, 2021.

[51] Y. Zhang, Z. Chen, S. Pirandola et al., "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Physical Review Letters*, vol. 125, no. 1, article 010502, 2020.

[52] Y. Zhang, Z. Li, Z. Chen et al., "Continuous-variable QKD over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, no. 3, article 035006, 2019.

[53] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electronics Letters*, vol. 33, no. 3, pp. 188–190, 1997.

[54] B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," *New Journal of Physics*, vol. 12, article 103042, 2010.

[55] M. S. Goodman, P. Toliver, R. J. Runser et al., "Quantum cryptography for optical networks: a systems perspective," *The 16th Annual Meeting of the IEEE Lasers and Electro-Optics Society*, vol. 2, pp. 1040-1041, 2003, paper ThEE1.

[56] N. A. Peters, P. Toliver, T. E. Chapuran et al., "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New Journal of Physics*, vol. 11, article 045012, 2009.

[57] T. E. Chapuran, P. Toliver, N. A. Peters et al., "Optical networking for quantum key distribution and quantum communications," *New Journal of Physics*, vol. 11, no. 10, article 105001, 2009.

[58] N. A. Peters, P. Toliver, T. E. Chapuran et al., "Quantum communications in reconfigurable optical networks: DWDM QKD through a ROADM," in *Conference on Optical Fiber Communication (OFC) 2010, paper OTuK1*, San Diego, CA, 2010.

[59] L.-J. Wang, K.-H. Zou, W. Sun et al., "Long-distance copropagation of quantum key distribution and terabit classical optical data channels," *Physics Review A*, vol. 95, no. 1, article 012301, 2017.

[60] Y. Mao, B.-X. Wang, C. Zhao et al., "Integrating quantum key distribution with classical communications in backbone fiber network," *Optics Express*, vol. 26, no. 5, pp. 6010–6020, 2018.

[61] W. Chen, Z. F. Han, T. Zhang et al., "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photonics Technology Letters*, vol. 21, no. 9, pp. 575–577, 2009.

[62] S. Wang, W. Chen, Z. Yin et al., "Field test of wavelength-saving quantum key distribution network," *Optics Letters*, vol. 35, no. 14, pp. 2454–2456, 2010.

[63] S. Wang, W. Chen, Z. Yin et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express*, vol. 22, no. 18, pp. 21739–21756, 2014.

[64] T.-Y. Chen, J. Wang, H. Liang et al., "Metropolitan all-pass and inter-city quantum communication network," *Optics Express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[65] K. A. Patel, J. F. Dynes, I. Choi et al., "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," *Physical Review X*, vol. 2, no. 4, article 041010, 2012.

[66] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, "A quantum access network," *Nature*, vol. 501, pp. 69–72, 2013.

[67] K. A. Patel, J. F. Dynes, M. Lucamarini et al., "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Applied Physics Letters*, vol. 104, no. 5, article 051123, 2014.

[68] I. Choi, Y. Zhou, J. F. Dynes et al., "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Optics Express*, vol. 22, no. 19, pp. 23121–23128, 2014.

[69] B. Fröhlich, J. F. Dynes, M. Lucamarini et al., "Quantum secured gigabit optical access networks," *Scientific Reports*, vol. 5, article 18121, 2015.

[70] J. F. Dynes, W. W.-S. Tam, A. Plews et al., "Ultra-high bandwidth quantum secured data transmission," *Scientific Reports*, vol. 6, article 35149, 2016.

[71] L. J. Wang, L. K. Chen, L. Ju et al., "Experimental multiplexing of quantum key distribution with classical optical communication," *Applied Physics Letters*, vol. 106, no. 8, article 081108, 2015.

[72] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *Nature Partner Journals (NPJ) Quantum Information*, vol. 3, article 30, 2017.

[73] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, "Satellite-Based QKD," *Optics and Photonics News*, vol. 29, no. 2, pp. 26–33, 2018.

[74] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics*, vol. 4, pp. 82.1–82.21, 2002.

[75] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, "Feasibility of satellite quantum key distribution," *New Journal of Physics*, vol. 11, article 045017, 2009.

[76] A. Tomaello, A. Dall'Arche, G. Naletto, and P. Villoresi, "Intersatellite quantum communication feasibility study," in *Quantum Communications and Quantum Imaging IX, 816309*, vol. 8163 of *Proceedings of the SPIE*, San Diego, CA, USA, 2011.

[77] B. C. Jacobs and J. D. Franson, "Quantum cryptography in free space," *Optics Letters*, vol. 21, no. 22, pp. 1854–1856, 1996.

[78] W. T. Buttler, R. J. Hughes, P. G. Kwiat et al., "Free-space quantum key distribution," *Physical Review A*, vol. 57, no. 4, pp. 2379–2382, 1998.

[79] W. T. Buttler, R. J. Hughes, P. G. Kwiat et al., "Practical free-space quantum key distribution over 1 km," *Physical Review Letters*, vol. 81, no. 15, pp. 3283–3286, 1998.

[80] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics*, vol. 4, pp. 43.1–43.14, 2002.

[81] C. Kurtsiefer, P. Zarda, M. Halder et al., "A step towards global key distribution," *Nature*, vol. 419, p. 450, 2002.

[82] T. Schmitt-Manderbach, H. Weier, M. Fürst et al., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Physical Review Letters*, vol. 98, article 010504, 2007.

[83] S. Nauerth, F. Moll, M. Rau et al., "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, pp. 382–386, 2013.

[84] J. Y. Wang, B. Yang, S. K. Liao et al., "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, pp. 387–393, 2013.

[85] J.-P. Bourgoin, B. L. Higgins, N. Gigov et al., "Free-space quantum key distribution to a moving receiver," *Optics Express*, vol. 23, no. 26, pp. 33437–33447, 2015.

[86] C. J. Pugh, S. Kaiser, J. P. Bourgoin et al., "Airborne demonstration of a quantum key distribution receiver payload," in *2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC), paper EB_4_1*, Munich, 2017.

[87] C. J. Pugh, S. Kaiser, J. P. Bourgoin et al., "Airborne demonstration of a quantum key distribution receiver payload," *Quantum Science and Technology*, vol. 2, no. 2, article 024009, 2017.

[88] J. Yin, Y. Cao, S.-B. Liu et al., "Experimental quasi-single-photon transmission from satellite to earth," *Optics Express*, vol. 21, no. 17, pp. 20032–20040, 2013.

[89] J. Pan, "Quantum science satellite," *Chinese Journal of Space Science*, vol. 34, no. 5, pp. 547–549, 2014.

[90] S. K. Liao, W. Q. Cai, W. Y. Liu et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 2017.

[91] S. Liao, W. Cai, J. Handsteiner et al., "Satellite-relayed intercontinental quantum network," *Physical Review Letters*, vol. 120, no. 3, article 030501, 2018.

[92] T. Scheidl, J. Handsteiner, D. Rauch, and R. Ursin, "Space-to-ground quantum key distribution," in *International Conference on Space Optics (ICSO) 2018*, vol. 11180, Chania, Greece, 2018.

[93] T. Jennewein, J. P. Bourgoin, B. Higgins et al., "QEYSSAT: a mission proposal for a quantum receiver in space," in *Advances in Photonics of Quantum Computing, Memory, and Communication VII*, vol. 8997 of *Proceedings of the SPIE*, San Francisco, CA, USA, February 2014.

[94] E. Meyer-Scott, Z. Yan, A. MacDonald, J. P. Bourgoin, H. Hübel, and T. Jennewein, "How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss," *Physical Review A*, vol. 84, no. 6, article 062326, 2011.

[95] J. P. Bourgoin, E. Meyer-Scott, B. L. Higgins et al., "A comprehensive design and performance analysis of low earth orbit satellite quantum communication," *New Journal of Physics*, vol. 15, article 023006, 2013.

[96] J. P. Bourgoin, N. Gigov, B. L. Higgins et al., "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," *Physical Review A*, vol. 92, article 052339, 2015.

[97] H. Podmore, I. D'Souza, D. Hudson et al., "Optical terminal for Canada's quantum encryption and science satellite (QEYSSat)," *IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, 2019.

[98] M. Yang, F. Xu, J.-G. Ren et al., "Spaceborne, low-noise, single-photon detection for satellite-based quantum communications," *Optics Express*, vol. 27, no. 25, pp. 36114–36128, 2019.

[99] G. Vallone, D. Bacco, D. Dequal et al., "Experimental satellite quantum communications," *Physical Review Letters*, vol. 115, no. 4, article 040502, 2015.

[100] D. Dequal, G. Vallone, D. Bacco et al., "Experimental single-photon exchange along a space link of 7000 km," *Physical Review A*, vol. 93, article 010301, 2016.

[101] K. Günthner, I. Khan, D. Elser et al., "Quantum-limited measurements of optical signals from a geostationary satellite," *Optica*, vol. 4, no. 6, pp. 611–616, 2017.

[102] Y. A. Chen, Q. Zhang, T. Y. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, pp. 214–219, 2021.

[103] T. Jennewein, C. Grant, E. Choi et al., "The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite," in *Emerging Technologies in Security and Defence II; and Quantum-Physics-based Information Security III, 925402*, vol. 9254 of *Proceedings of the SPIE*, Amsterdam, Netherlands, October 2014.

[104] D. K. L. Oi, A. Ling, J. A. Grieve, T. Jennewein, A. N. Dinkelaker, and M. Krutzik, "Nanosatellites for quantum science and technology," *Contemporary Physics*, vol. 58, pp. 25–52, 2016.

[105] R. Bedington, X. Bai, E. Truong-Cao et al., "Nanosatellite experiments to enable future space-based QKD missions," *EPJ Quantum Technology*, vol. 3, article 12, 2016.

[106] D. K. Oi, A. Ling, G. Vallone et al., "CubeSat quantum communications mission," *EPJ Quantum Technology*, vol. 4, article 6, 2017.

[107] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photonics*, vol. 11, no. 8, pp. 502–508, 2017.

[108] K. Boone, J. P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon, "Entanglement over global distances via quantum repeaters with satellite links," *Physical Review A*, vol. 91, article 052325, 2015.

[109] Z. Tang, R. Chandrasekara, Y. C. Tan et al., "Generation and analysis of correlated pairs of photons aboard a nanosatellite," *Physical Review Applied*, vol. 5, no. 5, article 054022, 2016.

[110] J. Yin, Y. Cao, Y.-H. Li et al., "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[111] A. Villar, A. Lohrmann, X. Bai et al., "Entanglement demonstration on board a nano-satellite," *Optica*, vol. 7, no. 7, pp. 734–737, 2020.

[112] C.-Z. Peng, T. Yang, X.-H. Bao et al., "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," *Physical Review Letters*, vol. 94, no. 15, article 150501, 2005.

[113] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach et al., "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, 2007.

[114] X.-M. Jin, J.-G. Ren, B. Yang et al., "Experimental free-space quantum teleportation," *Nature Photonics*, vol. 4, no. 6, pp. 376–381, 2010.

[115] J. Yin, J.-G. Ren, H. Lu et al., "Quantum teleportation and entanglement distribution over 100-kilometre free- space channels," *Nature*, vol. 488, pp. 185–188, 2012.

[116] Y. Cao, Y. H. Li, K. X. Yang et al., "Long-distance free-space measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 125, article 260503, 2020.