Foundations in
Signal Processing, Communications and Networking 23
Series Editors: Wolfgang Utschick · Holger Boche · Rudolf Mathar

Riccardo Bassoli · Holger Boche
Christian Deppe · Roberto Ferrara
Frank H. P. Fitzek · Gisbert Janssen
Sajad Saeedinaeeni

Quantum Communication Networks

Springer

Foundations in Signal Processing, Communications and Networking

Volume 23

This book series presents monographs about fundamental topics and trends in signal processing, communications and networking in the field of information technology. The main focus of the series is to contribute on mathematical foundations and methodologies for the understanding, modeling and optimization of technical systems driven by information technology. Besides classical topics of signal processing, communications and networking the scope of this series includes many topics which are comparably related to information technology, network theory, and control. All monographs will share a rigorous mathematical approach to the addressed topics and an information technology related context.

** Indexing: The books of this series are indexed in Scopus and zbMATH **

More information about this series at http://www.springer.com/series/7603

Riccardo Bassoli • Holger Boche • Christian Deppe
Roberto Ferrara • Frank H. P. Fitzek
Gisbert Janssen • Sajad Saeedinaeeni

Quantum Communication Networks

Springer

Riccardo Bassoli
Technical University Dresden
Dresden, Germany

Christian Deppe
Technical University of Munich
Munich, Bayern, Germany

Frank H. P. Fitzek
TU Dresden
Dresden, Germany

Sajad Saeedinaeeni
Technical University Munich
Munich, Germany

Holger Boche
Technical University of Munich
Munich Center for Quantum
Science and Technology
Munich, Germany

CASA – Cyber Security in the
Age of Large-Scale Adversarie
Bochum, Germany

Roberto Ferrara
Technical University Munich
Munich, Germany

Gisbert Janssen
Technical University Munich
Munich, Germany

ISSN 1863-8538 ISSN 1863-8546 (electronic)
Foundations in Signal Processing, Communications and Networking
ISBN 978-3-030-62937-3 ISBN 978-3-030-62938-0 (eBook)
https://doi.org/10.1007/978-3-030-62938-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Taking a quick look at this book, a reader might think: *Oh, here comes another book on quantum computing, quantum information theory, and quantum communications!* This may be partially true. Quantum mechanics was born at the beginning of the last century and, over the decades, has obtained huge popularity in mathematics and physics. Additionally, quantum mechanics has been applied to computing and information theory for the past 40–50 years. Recently, it has been also applied to communications.

Thus, by exploring the available scientific literature, it is possible to find plenty of books on quantum mechanics, quantum computing, and quantum information theory and some on quantum communications. So, the question is: *Is this book needed in the panorama of scientific literature?* The answer is yes, and there are some important reasons to support this.

First, many of the books are not very recent (especially from a communication perspective), so they miss some important recent updates. Furthermore, most of them are monographs, which focus on specific areas of research in quantum theory and its applications.

Second, to the best of the authors' knowledge, no book has considered the recent perspectives that communication networks have been gradually acquiring. In fact, communication networks are currently undergoing a paradigm shift that adds computing and storage to the simple transportation ideas of our first communication networks. These *softwarized* solutions break new ground in reducing latency and increasing resilience but have an inherent problem due to the introduced computing latency and energy consumption. This problem can be solved by hybrid classical-quantum communication networks.

This book inherits the existing paradigm of computing-in-networks, and it uses this to describe future quantum communication networks (which will not only be the Quantum Internet). The book focuses on quantum computing, quantum information theory, quantum error correction, and system-level architecture as various bricks that will build future *compute-and-forward* quantum communication networks. The approach, which is used for the presentation of the theory of quantum communication networks, borrows some viewpoints from the ongoing work of the IETF Quantum Internet Research Group (qirg) (in which the authors are participating). However, this book also enhances and generalizes these views in order to leave the reader free to investigate and figure out new designs and solutions without architectural limits. This becomes especially important in a new field like quantum communication networks, where there are no existing standardized solutions yet.

Last but not least, this book addresses a topic in this field, which has never been presented before in books: the research problem of classically tested (via software simulations) quantum-mechanical systems. Because of this, at the end of the book, existing simulators of quantum communication networks are presented and their pros and cons are underlined. In this way, the reader will become aware of this important open issue when approaching research on quantum communication networks. Finally, some identified potential applications of quantum communication networks are also described. This also represents a practical viewpoint for the reader.

As authors who are experts in the fields of the research presented, we hope that the book conveys the importance of quantum-mechanical resources for the effective and efficient evolution of future communication networks. When we wrote this manuscript, we had in mind providing both physicists and engineers with a valuable reference for their research in quantum communication networks (and its subfields). Moreover, we planned the structure and the terminology to be both accurate and accessible, in order to become a helpful assistant for lectures in higher education and for training courses in the industry.

Dresden, Germany
September 2020

Riccardo Bassoli

Acknowledgments

We would like to thank Deutsche Telekom for supporting R. Bassoli and F. Fitzek over the last year and for their motivation to work on the topic of quantum communication networks.

We also thank the CeTI team for supporting R. Bassoli and F. Fitzek. CeTI is funded by the German Research Foundation (DFG, Deutsche Forschungsgemeinschaft) as part of Germany's Excellence Strategy—EXC 2050/1—Project ID 390696704—Cluster of Excellence "Centre for Tactile Internet with Human-in-the-Loop" (CeTI) of the Technische Universität Dresden.

We thank the German Research Foundation (DFG) within the Gottfried Wilhelm Leibniz Prize under grant BO 1734/20-1 for their support of H. Boche and C. Deppe.

Additionally, we thank the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Q.Link.X—Quantum Link Extended" with the project "System Design for Secure Quantum Repeater Systems: Basic Protocols and Secure Implementation" under grant 16KIS0858 for their support of H. Boche, G. Janssen, and S. Saeedinaeeni and with the project "Quantum Information Theory and Communication Theory for Quantum Repeaters Beyond the Shannon Approach" under grant 16KIS0856 for their support of C. Deppe and R. Ferrara.

We also thank the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Q.COM—Quantum Communication" with the project "Information Theory of the Quantum Repeater: Eavesdrop Secure Communication, Attacks and System Design" under grant 16KIS0118 for their support of H. Boche and G. Janssen and with the project "Eavesdrop Secure Communication via Quantum Repeaters When Using Different Resources" under grant 16KIS0117 for their support of C. Deppe.

Thanks also goes to the German Federal Ministry of Education and Research (BMBF) within the national initiative for "Post Shannon Communication (NewCom)" with the project "Basics, Simulation and Demonstration for New Communication Models" under grant 16KIS1003K for their support of H. Boche and with the project "Coding Theory and Coding Methods for New Communication Models" under grant 16KIS1005 for their support of C. Deppe and R. Ferrara.

Further, we thank the German Research Foundation (DFG) within Germany's Excellence Strategy EXC-2111—390814868 for their support of H. Boche and S. Saeedinaeeni.

In addition, we thank Werner Moorfeld for his continuous effort to bring different communities together. The many valuable discussions we had together formed the starting point for this book project.

Finally, we would like to thank E. Soeder for proofreading the book and making linguistic suggestions.

Contents

About the Authors

Riccardo Bassoli is a senior researcher at the Deutsche Telekom Chair of Communication Networks, Faculty of Electrical and Computer Engineering, Technische Universität Dresden (Germany). He received his B.Sc. and M.Sc. degrees in Telecommunications Engineering from the University of Modena and Reggio Emilia (Italy) in 2008 and 2010, respectively. Next, he received his Ph.D. degree from the 5G Innovation Centre at the University of Surrey (UK) in 2016. He was also a Marie Curie ESR at the Instituto de Telecomunicações (Portugal) and a visiting researcher at the Airbus Defence and Space (France). Between 2016 and 2019, he was a postdoctoral researcher at the University of Trento (Italy). He is an IEEE and ComSoc member. He is also a member of the Glue Technologies for Space Systems Technical Panel of IEEE AESS.

Holger Boche received the Dipl.-Ing. degree in electrical engineering, Graduate degree in mathematics, and the Dr.-Ing. degree in electrical engineering from the Technische Universität Dresden, Dresden, Germany, in 1990, 1992, and 1994, respectively, and the Dr. rer. nat. degree in pure mathematics from the Technische Universität Berlin, Berlin, Germany, in 1998. From 1994 to 1997, he did postgraduate studies at the Friedrich-Schiller Universität Jena. In 1997, he joined the Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Berlin. From 2002 to 2010, he was a Full Professor in mobile communication networks at the Institute for Communications Systems, Technische Universität Berlin. In 2003, he became the Director of the Fraunhofer German-Sino Laboratory for Mobile Communications, Berlin, and in 2004, he became the Director of the Fraunhofer Institute for Telecommunications (HHI), Berlin, Germany. He is currently Full Professor at the Institute of Theoretical Information Technology, Technische Universitt Mnchen, which he joined in October 2010.

Christian Deppe received the Dipl.-Math. degree in mathematics from the Universität Bielefeld, Bielefeld, Germany, in 1996, and the Dr.-Math. degree in mathematics from the Universität Bielefeld, Bielefeld, Germany, in 1998. He was a research and teaching assistant at the Fakultät für Mathematik, Universität Bielefeld, from 1998 to 2010. From 2011 to 2013, he was project leader of the project "Sicherheit und Robustheit des Quanten-Repeaters" of the Federal Ministry of Education and Research at Fakultät für Mathematik, Universität Bielefeld. In 2014, he was supported by a DFG project at the Institute of Theoretical Information Technology, Technische Universität München. In 2015, he had a temporary professorship at the Fakultät für Mathematik und Informatik, Friedrich-Schiller Universität Jena. He is currently project leader of the project "Abhörsichere Kommunikation über Quanten-Repeater" of the Federal Ministry of Education and Research at the Fakultät für Mathematik, Universität Bielefeld. Since 2018, he is at the Department of Communications Engineering at the Technische Universität München.

Roberto Ferrara obtained his M.Sc. in physics at the Niels Bohr Institute of the University of Copenhagen and his Ph.D. in science at the Department of Mathematical Sciences of the University of Copenhagen. In his PhD dissertation "An Information-Theoretic Framework for Quantum Repeaters," he studied the limitations of distilling bipartite classical keys from quantum states when the two parties can only share entanglement with the aid of a third party, the quantum repeater, covering topics of entanglement measures, quantum operations, and quantum information theory. Since 2019, he is at the Department of Communications Engineering at the Technical University of Munich.

Frank H. P. Fitzek is a Professor and head of the Deutsche Telekom Chair of Communication Networks at the Technische Universität Dresden, coordinating the 5G Lab Germany. He is the spokesman of the DFG Cluster of Excellence CeTI. He received his diploma (Dipl.-Ing.) degree in electrical engineering from the University of Technology—Rheinisch-Westfälische Technische Hochschule (RWTH)—Aachen, Germany, in 1997 and his Ph.D. (Dr.-Ing.) in electrical engineering from the Technical University Berlin, Germany, in 2002 and became Adjunct Professor at the University of Ferrara, Italy, in the same year. In 2003, he joined the Aalborg University as Associate Professor and later became Professor. In 2005, he won the YRP award for the work on MIMO MDC and received the Young Elite Researcher Award of Denmark. He was selected to receive the NOKIA Champion Award several times in a row from 2007 to 2011. In 2008, he was awarded the Nokia Achievement Award for his work on cooperative networks. In 2011, he received the SAPERE AUDE research grant from the Danish government, and in 2012, he received the Vodafone Innovation prize. In 2015, he was awarded the honorary degree "Doctor Honoris Causa" by the Budapest University of Technology and Economics (BUTE).

Gisbert Janssen has been with the Institute for Theoretical Information Technology at the Technical University Munich as a researcher from 2010 to 2019. He received a physics diploma from the Berlin Technical University in 2010 and the Dr. rer. nat. degree from the Technical University Munich in 2016.

Sajad Saeedinaeeni received the B.S. and M.S. degrees in physics from the Royal Holloway University of London in 2010 and Leipzig University in 2015, respectively. He wrote his Master's thesis on Quantum Hypothesis Testing at the Max Planck Institute for Mathematics of Leipzig. He is currently working toward the Dr. rer. nat degree in physics at the Institute of Theoretical Information Technology of the Technische Universität München (TUM) under the supervision of Holger Boche.

Chapter 1
Introduction

The rise of new fundamental theories in physics has always opened the door for subsequent advancement in practical physics and theoretical engineering. For example, the discovery of electromagnetism in the nineteenth century resulted in the study, design, and development of telecommunications and computing during the following twentieth century. The fundamental theory of the last century is quantum mechanics, which has had significant scientific and philosophical impact by changing the way we look at and interpret the universe. In fact, in the mid twentieth century, preliminary formulations of quantum mechanics became more and more mature by subsequently revealing, in the late twentieth century, the potential engineering perspectives of quantum phenomena such as photonics, computing, and cryptography. Furthermore, in the last two decades, quantum-mechanical resources became the main suppliers for an infrastructural evolution of existing communication networks, in order to make them capable of addressing the existing challenges in computing and telecommunications.

1.1 The Evolution of Classical Communication Networks

The first commercial worldwide communication networks emerged with the well-known telephone services, which initially required direct links between all communication partners. Next, scalability was improved by introducing localized central switching to reuse telephone cables more efficiently. The concept of hierarchical switching was introduced into telephone networks with the rise of circuit switching. Especially in circuit-switched networks, communication pairs always use dedicated and exclusive physical resources. Though realized by utilizing several hops across connecting equipment, the resulting implementation logically appeared as a single dedicated virtual cable between communication partners.

R. Bassoli et al., *Quantum Communication Networks*, Foundations in Signal
Processing, Communications and Networking 23,
https://doi.org/10.1007/978-3-030-62938-0_1

Next, the era of packet switching started. This communication paradigm enabled the breaking up of long messages into smaller ones and realized the concepts of efficient time-shared resource utilization. In 1974, a unifying protocol suite for heterogeneous communications was needed on top of various packet-switched networks, to enable interoperability. This specific suite was composed of the transport control protocol (TCP) and the internet protocol (IP). Jointly, these two layers of protocols enabled a process-oriented and reliable communication end to end, across different packet-switched networks. It was this addition to packet switching that enabled the seamless interconnection of individual networks to the Internet. With the evolution of the Internet, the idea of packets and packet switching following the *store-and-forward* policy was fully adopted.

However, future networks will have a completely different nature from both existing wireless and wired perspectives. That is why, nowadays, standardization is undertaken by 3GPP (wireless part) together with IETF (wired part). In fact, the current objective is to realize an *ecosystem* (or *pan infrastructure*), capable of interconnecting highly heterogeneous networks, achieving concurrently demanding requirements and supporting several different verticals. The main enabler to achieve this scope is virtualization: the deployment of software-defined networking (SDN) [NMN+14] and network function virtualization (NFV) [MSG+16] at all levels. The main characteristic of network virtualization is the software-based implementation of functions, protocols, and operations, running on general purpose hardware.

The so-called process of *softwarization* of the network has produced the fertile ground for efficient and effective novel paradigms such as cloud and edge/fog computing, unique and flexible/reconfigurable SDN–NFV architecture, and end-to-end network slicing [RBSG16, LSC+17] (with complete isolation among slices and services). In fact, significant research effort has been focused on the design of a common/unique SDN–NFV system. Furthermore, extreme flexibility is targeted by the new paradigm of the wireless network operating system (WNOS), which will completely abstract network entities by providing a programmable protocol stack (PPS), rather than only network functions and routing.

Such a complex and heterogeneous system will require future networks to rely less on human intervention and more on machine learning/cognition for network management. In fact, an increasing research trend focuses on the deployment of cognition to make network management autonomous. The research community has started studying self-organized networks (SONs) in parallel to virtualization by extensively applying machine learning and cognitive algorithms toward self-healing and self-management.

The vision of future networks implies the realization of cloud and edge computing in a more and more distributed manner, in order to respond to different legal and technical requirements, while increasing resilience in data storage and computing. Computing will become an intrinsic characteristic of future networks. The placement of computing at a given data center (e.g., big, micro, femto, etc.) will have impact on security, resilience, capacity, and latency of a given end-to-end communication. Furthermore, the distributed nature of the future computing paradigm may also be extended to end users. Because of the prominent role, computing will have in future generation networks, especially when performed in a distributed manner, the intrinsic nature of the network will experience a radical transformation of the paradigm: from solely conveying information between two places using *store and forward* to where information is also processed within the communication network, using *compute and forward* [FGS20].

The characteristics of future networks briefly described above predict the rise of a very high demand for storage capacity and computing infrastructure. This will also significantly increase energy consumption in communication networks. Moreover, the realization of intelligent and adaptable networks will require a huge number of resources for secure data mining/processing and distributed computing for decision-making. Intelligent analysis of Big Data will continuously need network performance and network infrastructure awareness for prediction of future network states. Additionally, the synchronization of highly distributed computing entities will also affect requirements in terms of capacity, latency, and reliability.

Regarding performances of future communication networks, some of the desired key performance indicators (KPIs) [ARS16] are: 1 ms round trip latency, billions of connected devices, perceived availability of 99.999%, and reduction in energy usage by almost 90%. These KPI goals will allow 5G and beyond networks to support several possible end-to-end communication paradigms/services. Such services, also named *verticals*, are usually grouped into three main categories: Extreme Mobile Broadband (xMBB), ultra-reliable Machine-Type Communications (uMTCs)—also called Ultra-Reliable Low-Latency Communications (URLLCs)—and massive Machine-Type Communications (mMTCs).

The concurrent satisfaction of these requisites, via algorithms and solutions described above, is limited to the existing domain of communications based on classical physics. These imply an enormous effort and complexity but do not ensure a successful solution. The following underlines why the intrinsic drawbacks of future generation networks will limit their capabilities.

The process of *softwarization* in future networks must attain a high flexibility toward a reduction in operational expenditure (OpEx) and capital expenditure (CapEx). Software and virtualization can be viewed as the DNA of 5G and beyond networks' infrastructure. However, software abstraction also introduces additional packet processing delays. In fact, it increases data transfer and computation demands so that latency becomes relatively high. Even if the existing virtual switches are quite fast, virtual machines (VMs), specifically the packet IO and processing operations inside the VM, are slow. Two software bridges (or virtual switches) connect virtual network interfaces (vNICs) with the physical network interface (pNIC). Next, the integration bridge connects all VMs running on the same physical node.

A proposed centralized approach to virtualization gives more than 2 ms latency inside the virtual communication environment for a single VM running the elementary forwarding function [XGU$^+$19], which becomes unacceptable in the context of URLLCs. Some solutions have been designed to significantly reduce the latency of virtualization [XGU$^+$19], but more and more software is getting into network layers so that latency due to network virtualization is expected to constantly increase. Furthermore, some components of latency are proportional to the available transmission bitrate and to the amount of data. This can be addressed by scaling up the transmission capacities and compression, but processing delays with their various constant delays still affect latency with their contribution.

When employing network virtualization, further important aspects also have to be taken into account: reliability and resilience (i.e., keeping an acceptable level of service in case of faults). In fact, software-based network functions and applications are more prone to failures than hardware-based ones because they have more points of faultiness. This makes it harder to match the desired network flexibility with future KPIs of network reliability and service availability [LJK+16, GB18]. Moreover, the realization of cloud and edge computing in a more and more distributed manner also includes the impact of data storage and computing at data centers. In fact, the placement of computing at a given data center (e.g., big, micro, femto, etc.) has impact on resilience, capacity, and latency of a given end-to-end communication. Furthermore, the distributed nature of the future computing paradigm could also be extended to the user end device, adding more points of delay and failure.

While making software the pillar of future communication networks improves some performance metrics as mentioned above, this also opens various new security threats. A major security issue of SDN–NFV-based systems is the threat due to scalability. Controllers and hypervisors can easily become bottlenecks because of the amount of control traffic they have to manage. Control plane saturation opens the door to various Denial-of-Service (DoS) and distributed DoS (DDoS) attacks. Regarding network management and orchestration, authenticating applications becomes fundamental. It is necessary to establish a trust relationship between the control plane and applications. Next, in SDN, effective access control and accountability mechanisms are still an open challenge. Medium access control, SDN can be attacked by a malicious host, sending packets with falsified source Medium access control addresses to poison the Medium access control table of a switch. Many other security threats due to network *softwarization* and network function computing can be found in [ANYG15, DCA+17, FTKS19, SNS16, AvW18, PHS+18].

The switch of the paradigm from *store and forward* to *compute and forward* will massively increase the deployed computing resources in the network and the size and/or number of data centers. This implies a significant rise in energy consumption because of virtualization and *softwarization* [DWF16, JHA+16, JITT16, BIK+16, BGADR19]. The consumption of a big data center is about 25.000 households, and the energy costs of powering a data center double every 5 years (and this rate will grow due to massive computing deployment) [DWF16]. Such energy needs also imply environmental problems (e.g., in 2005, the total data center power consumption was 1% of the total US power consumption, creating the same quantity of emissions as a mid-sized country [DWF16]). The energy required by computing can be divided into two main categories: energy used by network/computing equipment (e.g., servers, networks, storage, etc.) and energy used by infrastructure facilities (such as cooling, air conditioning, etc.).

Moreover, the realization of intelligent adaptable networks will require huge amounts of resources for secure data mining/processing and distributed computing for decision-making. Big data intelligent analysis will continuously need network performance and network infrastructure awareness for prediction of future network states. Additionally, the synchronization of highly distributed computing entities will also affect requirements in terms of capacity, latency, and reliability.

Classical future generation networks also present a *communication complexity problem*. Communication complexity is the amount of information (in terms of bits) that spatially separate computing devices need to exchange in order to successfully perform a computational task. Virtualization and computing paradigms such as mobile edge computing (MEC) and distributed computing for network functions will rely on distributed devices solving network related computing problems. However, some of these distributed computing problems were demonstrated not to be solvable via distributed computing based on classical networks. Alongside solvable problems, the amount of communication bits used for communication among distributed computing devices was shown to have a strong impact on the links of the network (techniques for compression and encoding are not able to limit this growth effectively) [BCMdW10]. Such a problem of complexity logically recalls the previously mentioned latency one because delay is also proportional to the available transmission bitrate.

Finally, the integration of multiple services today is realized by higher-layer policies that allocate different services on different logical channels. The security issue is usually addressed by applying cryptographic techniques at higher levels. In general, this is quite inefficient, and there is a trend to merge multiple coexisting services efficiently so that they work on the same wireless resources. This is referred to as physical layer service integration [SB14a] and has the potential to significantly increase the spectral efficiency for next-generation networks. It is expected that different applications (e.g., secure message transmission, broadcasting of common messages, and message transmission) will all be implemented by *physical layer service integration*. References [HW10a, DS05] have been the first papers for quantum systems that offer a larger variety of services.

1.2 Toward Quantum Communication Networks

The previous section presented the path toward the current new paradigm promoted by future 5G and beyond networks. Communication networks have evolved from circuit-switched to packet-switched networks. In both cases, the end-to-end design has dominated, allowing for the transparent transportation of bits as given in Fig. 1.1. In such a system, latency is impacted by the propagation delay of the communication link.

Next, to reduce propagation delay, computing and storage have been added to communication nodes, in order to allow proximity-based computation (scheme in the second line of Fig. 1.1). By means of the virtualization paradigms mentioned above, the propagation latency has been significantly reduced. The MEC has been especially fundamental for such a purpose.

However, even if virtualization has contributed to reduce communication latency due to propagation, it has actually increased latency in every computing virtual

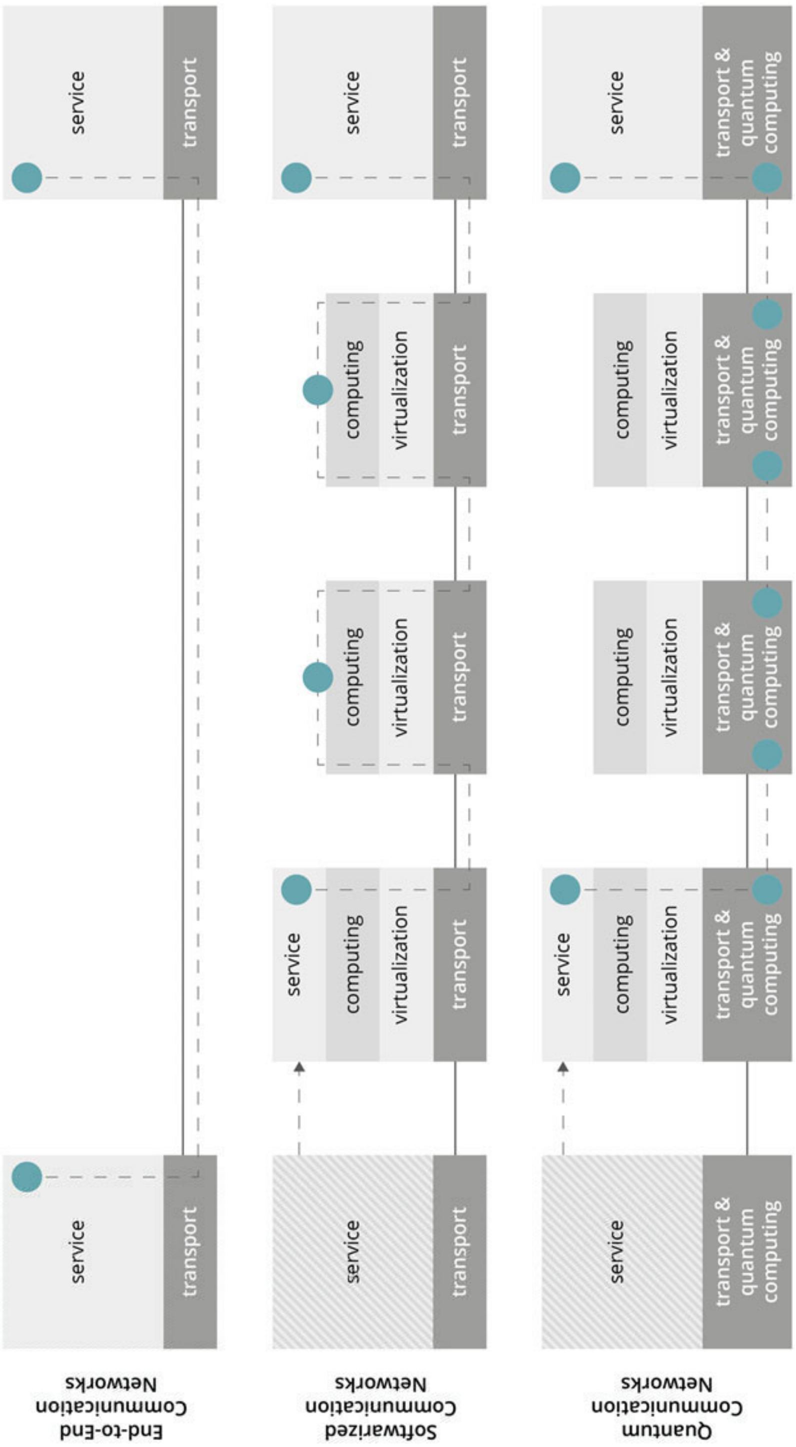

Fig. 1.1 Logic scheme representing the change of paradigms according to evolution of communication networks

machine [XGU$^+$19] involved. The reason is that all processed bits of information have to pass through several software-based virtualization layers (see Fig. 1.1, scheme in the middle). Thus, not only existing but also future solutions for *softwarized* networks can only support applications with a small number of virtual machines. Such limitation is necessary in order to not too rapidly increase networks' computing complexity.

All the aforementioned disadvantages expressed here and in the previous section, due to intrinsic classical limitations of both virtualization and computing, can only be resolved via the development of intrinsically different networks based on quantum mechanics. In this way, classical network computing is transferred to quantum-mechanical network computing: the change of the paradigm moves virtual network/computing resources based on software to new physical quantum resources relying on entanglement, which does not reveal itself in classical systems.

Just as classical networks were initially built on top of the existing legacy telephone infrastructure, current quantum-mechanical networks are going to be built in a hybrid fashion, on top of the existing classical network infrastructures.

By employing distributed quantum computing instead of classical computing, a unique virtual quantum machine consisting of a high number of entangled qubits scaling with the number of interconnected devices can achieve an exponential speed-up of a network's computing capabilities with just a linear increase in physical resources. In such a way, the limitations imposed by classical paradigms on virtualization and *softwarization* can be exceeded by exploiting quantum-physical parallelism based on the concepts of quantum superposition, entanglement, and quantum measurement (see the bottom of Fig. 1.1).

Existing approaches, using quantum mechanics in networks to provide security, mainly carry out protocols for key exchanges between individual nodes. In many cases, quantum key distribution (QKD) is used from one node to another. On the other hand, there are limited analyses focused on the complexity and capacity of these processes. Therefore, the current research and investments are principally pivoted on military and governmental communications, while civil users are strongly concerned with speed and complexity (which significantly affect latency and quality of the communications).

The potential of quantum mechanics for communication systems was recognized early on. Holevo's work [Hol73] in 1973 considers classical communication via quantum channels. In 1984, Bennett and Brassard developed the first quantum cryptography protocol in [BB84]. There, demonstrably secure communication theory was mentioned and considered. At the beginning of 1990, new quantum protocols for the solution of quantum communication tasks over quantum channels were developed. This included, for example, quantum teleportation. This is a process in which quantum information can be transmitted from one location to another, with the help of classical communication and previously shared quantum entanglement between the sending and receiving location. The seminal paper on this was published by Bennett, Brassard, Crépeau, Jozsa, Peres, and Wootters in 1993 [BBC$^+$93].

Furthermore, many classic coding methods and information theory approaches that were shown during this time do not apply quantum-mechanically, due to Heisenberg's uncertainty principle. A prominent example is the no-cloning theorem [WZ82]. After 2000, several exact information-theoretical capacity results could be proven. These results include, for example, private transmission [Dev05], distillation of secret key and entanglement from quantum states [DW05], and quantum wiretap channels [CWY04]. All experimental systems today essentially provide key generation in point-to-point communication.

The idea behind quantum communication networks [SR00, Kim08, WEH18] is that nodes of the network may be considered as distributed parts of the same physical system. The reason why quantum communication networks can outperform the classical Internet with relatively modest resources is because it comes from inherent properties of quantum-mechanical systems. In particular, entanglement is used as a resource for communication.

Entanglement (*Verschränkung*) is the main pillar for effective distributed quantum computing, teleportation, and superdense coding (to achieve efficiently higher throughput). Moreover, entanglement can also be interpreted from an information theoretic perspective. Quantum information theory is an important aspect of both quantum computing and quantum communications. Additional quantum-mechanical aspects are also the impossibility of copying information (no-cloning theorem) and qubits (superposition of possible states).

Quantum-mechanical-based computing and networking seem to be fundamental paradigms that will efficiently and effectively solve the existing problems that research and industry have been encountering in the design and development of future networks. In fact, technologies based on quantum mechanics (mainly exploiting entanglement) have been demonstrated to be effective for distributed systems while also guaranteeing intrinsic security of communication and computing in the cloud. Moreover, the realization of small quantum-based distributed and interconnected computing entities is the quantum more effective version of the current MEC paradigm. As an example, scientists can leverage distributed quantum computing to solve highly complex scientific computation problems such as the analysis of chemical interactions for medical drug development. This is not efficiently and effectively possible via classical networks and computing.

Regarding the current effort toward intelligent networks based on data mining and distributed data computing, quantum machine learning algorithms running on distributed quantum computing nodes can be secure, effective, and efficient (in terms of usage of network resources and energy).

Furthermore, quantum communications have provided significant advantages in communications, where multiple sources transmit information to a single receiver via a unique communication channel [Nö19, LALS20]. In particular, the comparison between classical and quantum multiple access channels (MAC), where two sources transmit to a destination, proved that quantum communications exceeded the success probability of classical ones because of the exploitation of entanglement.

On the other hand, apart from exceeding the capabilities of current classical networks, quantum networks can also be a fundamental means for other aspects of communication networks. Complex quantum networking processes can be realized