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

Quantenkommunikationsnetze

Springer Vieweg

Quantenkommunikationsnetze

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

Quantenkommunikationsnetze

Springer Vieweg

Riccardo Bassoli
Centre for Tactile Internet with Human-in-the-Loop (CeTI)
Technische Universität Dresden
Dresden, Deutschland

Holger Boche
Technische Universität München, Münchner Zentrum für Quantenforschung Wissenschaft und Technologie
München, Deutschland

Christian Deppe
Technische Universität München
München, Deutschland

Roberto Ferrara
Technische Universität München
München, Deutschland

Frank H. P. Fitzek
Centre for Tactile Internet with Human-in-the-Loop (CeTI)
TU Dresden
Dresden, Deutschland

Gisbert Janssen
Technische Universität München
München, Deutschland

Sajad Saeedinaeeni
Technische Universität München
München, Deutschland

Dieses Buch ist eine Übersetzung des Originals in Englisch „Quantum Communication Networks“ von Bassoli, Riccardo, publiziert durch Springer Nature Switzerland AG im Jahr 2021. Die Übersetzung erfolgte mit Hilfe von künstlicher Intelligenz (maschinelle Übersetzung durch den Dienst DeepL.com). Eine anschließende Überarbeitung im Satzbetrieb erfolgte vor allem in inhaltlicher Hinsicht, so dass sich das Buch stilistisch anders lesen wird als eine herkömmliche Übersetzung. Springer Nature arbeitet kontinuierlich an der Weiterentwicklung von Werkzeugen für die Produktion von Büchern und an den damit verbundenen Technologien zur Unterstützung der Autoren.

ISBN 978-3-031-26325-5 ISBN 978-3-031-26326-2 (eBook)
https://doi.org/10.1007/978-3-031-26326-2

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Planung/Lektorat: Axel Garbers
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Nature Switzerland AG und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Gewerbestrasse 11, 6330 Cham, Switzerland

Vorwort

Wenn man einen kurzen Blick auf dieses Buch wirft, könnte man meinen: *Oh, hier kommt ein weiteres Buch über Quantencomputer, Quanteninformationstheorie und Quantenkommunikation!* Das mag teilweise stimmen. Die Quantenmechanik wurde zu Beginn des letzten Jahrhunderts geboren und hat im Laufe der Jahrzehnte große Popularität in der Mathematik und Physik erlangt. Darüber hinaus wurde die Quantenmechanik in den letzten 40–50 Jahren auf die Informatik und die Informationstheorie angewandt. In jüngster Zeit findet sie sich auch in derKommunikation wieder.

Wenn man also die verfügbare wissenschaftliche Literatur durchforstet, findet man zahlreiche Bücher über Quantenmechanik, Quantencomputer und Quanteninformationstheorie sowie einige Werke über Quantenkommunikation. Die Frage ist also: *Ist dieses Buch im Panorama der wissenschaftlichen Literatur notwendig?* Die Antwort ist ja, und es gibt einige wichtige Gründe, die dafür sprechen.

Erstens sind viele der Bücher nicht sehr aktuell (vor allem aus der Sicht der Kommunikation), so dass sie einige wichtige Neuerungen gänzlich fehlen. Außerdem handelt es sich bei den meisten Büchern um Monographien, die sich auf bestimmte Forschungsbereiche der Quantentheorie und ihrer Anwendungen konzentrieren.

Zweitens hat nach dem bestem Wissen der Autoren noch kein Buch die neuen Perspektiven berücksichtigt, die Kommunikationsnetze allmählich erlangt haben. Tatsächlich vollzieht sich bei den Kommunikationsnetzen derzeit ein Paradigmenwechsel, bei dem die einfachen Transportkonzepte unserer ersten Kommunikationsnetze durch Rechen- und Speicherfunktionen ergänzt werden. Diese *softwarisierten* Lösungen bieten neue Möglichkeiten zur Verringerung der Latenzzeit und zur Erhöhung der Ausfallsicherheit, haben aber aufgrund der eingeführten Rechenlatenz und des Energieverbrauchs ein inhärentes Problem. Dieses Problem kann durch hybride klassisch-quantische Kommunikationsnetze gelöst werden.

Dieses Buch übernimmt das bestehende Paradigma des Rechnens in Netzwerken und nutzt es, um zukünftige Quantenkommunikationsnetzwerke zu beschreiben (die nicht nur das Quanteninternet sein werden). Das Buch konzentriert sich dabei auf

Quantencomputing, Quanteninformationstheorie, Quantenfehlerkorrektur und Architektur auf der Systemebene als verschiedene Bausteine, die künftige Compute-and-Forward-Quantenkommunikationsnetze aufbauen werden. Der Ansatz, der für die Darstellung der Theorie von Quantenkommunikationsnetzen verwendet wird, leiht sich einige Gesichtspunkte aus der laufenden Arbeit der IETF Quantum Internet Research Group (qirg) (an der die Autoren beteiligt sind). Dieses Buch erweitert und verallgemeinert diese Ansichten jedoch auch, um dem Leser die Freiheit zu geben, neue Entwürfe und Lösungen ohne architektonische Einschränkungen zu erforschen und zu entwickeln. Dies ist besonders in einem neuen Bereich wie den Quantenkommunikationsnetzen wichtig, in dem es noch keine standardisierten Lösungen gibt.

Nicht zuletzt greift dieses Buch ein Thema auf, das in diesem Bereich noch nie in Büchern behandelt wurde: das Forschungsproblem klassisch getesteter (mittels Software-Simulationen) quantenmechanischer Systeme. Aus diesem Grund werden am Ende des Buches bestehende Simulatoren von Quantenkommunikationsnetzen vorgestellt und ihre Vor- und Nachteile hervorgehoben. Auf diese Weise wird der Leser für diese wichtige offene Frage sensibilisiert, wenn es um die Erforschung von Quantenkommunikationsnetzen geht. Schließlich werden auch einige potenzielle Anwendungen von Quantenkommunikationsnetzen beschrieben. Dies stellt auch einen praktischen Gesichtspunkt für den Leser dar.

Als Autoren, die Experten auf den Gebieten der vorgestellten Forschung sind, hoffen wir, dass das Buch die Bedeutung quantenmechanischer Ressourcen für die effektive und effiziente Entwicklung zukünftiger Kommunikationsnetze vermittelt. Als wir dieses Manuskript schrieben, wollten wir sowohl Physikern als auch Ingenieuren ein wertvolles Nachschlagewerk für ihre Forschung auf dem Gebiet der Quantenkommunikationsnetze (und ihrer Teilgebiete) an die Hand geben. Darüber hinaus haben wir die Struktur und die Terminologie so geplant, dass sie sowohl genau als auch zugänglich sind, um ein hilfreiches Hilfsmittel für Vorlesungen in der Hochschulbildung und für Schulungen in der Industrie darzustellen.

Dresden, Deutschland Riccardo Bassoli
September 2020

Danksagungen

Wir danken der Deutschen Telekom für die Unterstützung von R. Bassoli und F. Fitzek im letzten Jahr und für ihre Motivation, sich mit dem Thema der Quantenkommunikationsnetze zu beschäftigen.

Wir danken auch dem CeTI-Team für die Unterstützung von R. Bassoli und F. Fitzek. Das CeTI wird von der Deutschen Forschungsgemeinschaft (DFG) im Rahmen der Exzellenzstrategie EXC 2050/1 – Projekt ID 390696704 – Exzellenzcluster „Centre for Tactile Internet with Human-in-the-Loop“ (CeTI) der Technischen Universität Dresden gefördert.

Wir danken der Deutschen Forschungsgemeinschaft (DFG) im Rahmen des Gottfried Wilhelm Leibniz-Preises unter dem Förderkennzeichen BO 1734/20-1 für die Unterstützung von H. Boche und C. Deppe.

Darüber hinaus danken wir dem Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der nationalen Initiative für „Q.Link.X-Quantum Link Extended“ mit dem Projekt „System Design for Secure Quantum Repeater Systems: Basic Protocols and Secure Implementation“ unter dem Förderkennzeichen 16KIS0858 für die Unterstützung von H. Boche, G. Janssen und S. Saeedinaeeni und im Rahmen des Projekts „Quantum Information Theory and Communication Theory for Quantum Repeaters Beyond the Shannon Approach“ unter dem Förderkennzeichen 16KIS0856 für die Unterstützung von C. Deppe und R. Ferrara.

Wir danken auch dem Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der nationalen Initiative für „Q.COM-Quantum Communication“ mit dem Projekt „Information Theory of the Quantum Repeater: Abhörsichere Kommunikation, Angriffe und Systementwurf“ unter dem Förderkennzeichen 16KIS0118 für die Unterstützung von H. Boche und G. Janssen und mit dem Projekt „Abhörsichere Kommunikation über Quantenrepeater bei Nutzung unterschiedlicher Ressourcen“ unter dem Förderkennzeichen 16KIS0117 für die Unterstützung von C. Deppe.

Dank geht auch an das Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der nationalen Initiative „Post Shannon Communication (NewCom)“ mit dem Projekt „Grundlagen, Simulation und Demonstration für neue Kommunikationsmodelle“ unter dem Förderkennzeichen 16KIS1003K für die Unterstützung

von H. Boche und mit dem Projekt „Codierungstheorie und Codierungsverfahren für neue Kommunikationsmodelle“ unter dem Förderkennzeichen 16KIS1005 für die Unterstützung von C. Deppe und R. Ferrara.

Außerdem danken wir der Deutschen Forschungsgemeinschaft (DFG) im Rahmen der Exzellenzstrategie EXC-2111-390814868 für die Unterstützung von H. Boche und S. Saeedinaeeni.

Darüber hinaus danken wir Werner Moorfeld für seine kontinuierlichen Bemühungen, verschiedene Gemeinschaften und Expertise zusammenzubringen. Die vielen wertvollen Diskussionen, die wir gemeinsam geführt haben, bildeten den Ausgangspunkt für dieses Buchprojekt.

Schließlich möchten wir E. Soeder für das Korrekturlesen des Buches und die sprachlichen Anregungen danken.

Inhaltsverzeichnis

Über die Autoren

Riccardo Bassoli ist wissenschaftlicher Mitarbeiter am Deutsche Telekom Lehrstuhl für Kommunikationsnetze, Fakultät Elektrotechnik und Informatik, Technische Universität Dresden (Deutschland). Er erhielt seinen B. Sc. und M.Sc. in Telekommunikationstechnik von der Universität Modena und Reggio Emilia (Italien) in den Jahren 2008 bzw. 2010. Anschließend promovierte er 2016 am 5G Innovation Centre der University of Surrey (Großbritannien). Außerdem war R. Bassoli Marie Curie ESR am Instituto de Telecomunicações (Portugal) und Gastforscher bei Airbus Defence and Space (Frankreich). Von 2016 bis 2019 war er Postdoktorand an der Universität von Trient (Italien). Er ist Mitglied von IEEE und ComSoc. Außerdem ist R. Bassoli Mitglied des technischen Gremiums „Glue Technologies for Space Systems“ des IEEE AESS.

Holger Boche erhielt an der Technischen Universität Dresden 1990 den Titel Dipl.-Ing. in der Elektrotechnik, 1992 den Dipl.-Ing. in der Mathematik und promovierte 1994 zum Dr.-Ing. in der Elektrotechnik. 1998 wurde er an der Technischen Universität Berlin zum Dr. rer. nat. in reiner Mathematik promoviert. Von 1994 bis 1997 absolvierte er ein Postgraduiertenstudium an der Friedrich-Schiller-Universität Jena. 1997 wechselte H. Boche an das Heinrich-Hertz-Institut (HHI) für Nachrichtentechnik Berlin, Berlin. Von 2002 bis 2010 war er ordentlicher Professor für mobile Kommunikationsnetze am Institut für Kommunikationssysteme der Techni-

schen Universität Berlin. Im Jahr 2003 wurde er Leiter des Fraunhofer German-Sino Laboratory for Mobile Communications, Berlin, und 2004 wurde er Leiter des Fraunhofer-Instituts für Nachrichtentechnik (HHI), Berlin, Deutschland. Derzeit ist H. Boche ordentlicher Professor am Institut für Theoretische Informationstechnik der Technischen Universität München, wo er seit Oktober 2010 tätig ist.

Christian Deppe erhielt 1996 das Diplom in Mathematik von der Universität Bielefeld, Bielefeld, Deutschland, und 1998 den Dr.-Math. von der Universität Bielefeld, Bielefeld, Deutschland. Von 1998 bis 2010 war er wissenschaftlicher Mitarbeiter und Lehrbeauftragter an der Fakultät für Mathematik der Universität Bielefeld. Von 2011 bis 2013 war C. Deppe Projektleiter des Projekts „Sicherheit und Robustheit des Quanten-Repeaters“ des Bundesministeriums für Bildung und Forschung an der Fakultät für Mathematik der Universität Bielefeld. 2014 wurde er im Rahmen eines DFG-Projekts am Institut für Theoretische Informationstechnik der Technischen Universität München gefördert. Im Jahr 2015 hatte C. Deppe eine befristete Professur an der Fakultät für Mathematik und Informatik der Friedrich-Schiller Universität Jena. Derzeit ist er Projektleiter des Projekts „Abhörsichere Kommunikation über Quanten-Repeater“ des Bundesministeriums für Bildung und Forschung an der Fakultät für Mathematik, Universität Bielefeld. Seit 2018 ist zudem er am Lehrstuhl für Nachrichtentechnik an der Technischen Universität München tätig.

Roberto Ferrara erwarb seinen M.Sc. in Physik am Niels-Bohr-Institut der Universität Kopenhagen und seinen Doktortitel in Naturwissenschaften an der Abteilung für mathematische Wissenschaften der Universität Kopenhagen. In seiner Dissertation „An Information-Theoretic Framework for Quantum Repeaters“ untersuchte er die Grenzen der Destillation von zweiseitigen klassischen Schlüsseln aus Quantenzuständen, wenn die beiden Parteien die Verschränkung nur mit Hilfe einer dritten Partei, dem Quantenrepeater, teilen können, und behandelte dabei Themen wie Verschränkungsmaße, Quantenopera-

tionen und Quanteninformationstheorie. Seit 2019 ist R. Ferrara am Lehrstuhl für Nachrichtentechnik an der Technischen Universität München tätig.

Frank H. P. Fitzek ist Professor und Leiter des Deutsche Telekom Lehrstuhls für Kommunikationsnetze an der Technischen Universität Dresden und koordiniert das 5G Lab Germany. Er ist der Sprecher des DFG-Exzellenzclusters CeTI. F. Fitzek erhielt sein Diplom (Dipl.-Ing.) in Elektrotechnik von der Rheinisch-Westfälischen Technischen Hochschule (RWTH) Aachen, Deutschland, im Jahr 1997 und seinen Doktortitel (Dr.-Ing.) in Elektrotechnik von der Technischen Universität Berlin, Deutschland, im Jahr 2002 und wurde im selben Jahr außerordentlicher Professor an der Universität von Ferrara, Italien. Im Jahr 2003 wechselte er als außerordentlicher Professor an die Universität Aalborg und wurde später zum Professor ernannt. Im Jahr 2005 gewann F. Fitzek den YRP-Preis für seine Arbeit über MIMO MDC und erhielt den Young Elite Researcher Award of Denmark. Von 2007 bis 2011 wurde er mehrmals in Folge mit dem NOKIA Champion Award ausgezeichnet. Im Jahr 2008 wurde er mit dem Nokia Achievement Award für seine Arbeit über kooperative Netzwerke ausgezeichnet. Im Jahr 2011 erhielt F. Fitzek das SAPERE AUDE-Forschungsstipendium der dänischen Regierung und im Jahr 2012 den Vodafone-Innovationspreis. Im Jahr 2015 wurde ihm von der Budapester Universität für Technologie und Wirtschaft (BUTE) der Ehrentitel „Doctor Honoris Causa“ verliehen.

Gisbert Janssen war von 2010 bis 2019 als wissenschaftlicher Mitarbeiter am Institut für Theoretische Informationstechnik der Technischen Universität München tätig. Er erhielt 2010 ein Physik-Diplom von der Technischen Universität Berlin und 2016 den Dr. rer. nat. von der Technischen Universität München.

Sajad Saeedinaeeni erwarb 2010 den B.Sc. und 2015 den M.Sc. in Physik an der Royal Holloway University of London bzw. der Universität Leipzig. Er schrieb seine Masterarbeit über Quantenhypothesentests am Max-Planck-Institut für Mathematik in Leipzig. Derzeit promoviert er zum Dr. rer. nat in Physik am Institut für Theoretische Informationstechnik der Technischen Universität München (TUM) unter der Betreuung von Holger Boche.

Kapitel 1
Einführung

Die Entstehung neuer grundlegender Theorien in der Physik hat stets die Tür für weitere Fortschritte in der praktischen Physik und der theoretischen Technik geöffnet. So führte beispielsweise die Entdeckung des Elektromagnetismus im 19. Jahrhundert zur Erforschung, Gestaltung und Entwicklung von Telekommunikation und Computern im folgenden 20. Jahrhundert. Die grundlegende Theorie des letzten Jahrhunderts ist die Quantenmechanik, die erhebliche wissenschaftliche und philosophische Auswirkungen hatte, indem sie die Art und Weise, wie wir das Universum betrachten und interpretieren, verändert hat. Im letzten Jahrhundert wurden die vorläufigen Formulierungen der Quantenmechanik immer ausgereifter, indem sie gegen Ende des 20. Jahrhunderts die potenziellen technischen Perspektiven von Quantenphänomenen, wie Photonik, Computertechnik und Kryptographie, aufzeigten. Darüber hinaus wurden in den letzten zwei Jahrzehnten quantenmechanische Ressourcen zu den Hauptlieferanten für eine infrastrukturelle Weiterentwicklung bestehender Kommunikationsnetze, um die Möglichkeit zu schaffen, bestehende Herausforderungen in der Datenverarbeitung und Telekommunikation zu bewältigen.

1.1 Die Entwicklung der klassischen Kommunikationsnetze

Die ersten kommerziellen, weltweiten Kommunikationsnetze entstanden mit den bekannten Telefondiensten, die zunächst direkte Verbindungen zwischen allen Kommunikationspartnern erforderten. Anschließend wurde die Skalierbarkeit durch die Einführung einer zentralen Vermittlung verbessert, um Telefonkabel effizienter wiederverwenden zu können. Das Konzept der hierarchischen Vermittlung wurde mit dem Aufkommen der Leitungsvermittlung in Telefonnetzen eingeführt. Insbesondere in leitungsvermittelten Netzen verwenden Kommunikationspaare immer dedizierte und exklusive physikalische Ressourcen. Obwohl bei der Realisierung mehrere Sprünge über das Verbindungsequipment verwendet werden,

R. Bassoli et al., *Quantenkommunikationsnetze*,
https://doi.org/10.1007/978-3-031-26326-2_1

erscheint die resultierende Implementierung logischerweise als ein einziges dediziertes virtuelles Kabel zwischen den Kommunikationspartnern.

Dann begann die Ära der Paketvermittlung. Dieses Kommunikationsparadigma ermöglichte es, lange Nachrichten in kleinere aufzuteilen und die Konzepte einer effizienten, zeitlich geteilten, Ressourcennutzung umzusetzen. 1974 wurde eine vereinheitlichende Protokollsuite für die heterogene Kommunikation über verschiedene paketvermittelte Netze benötigt, um Interoperabilität zu ermöglichen. Diese spezielle Suite bestand aus dem Transport Control Protocol (TCP) und dem Internet Protocol (IP). Gemeinsam ermöglichten diese beiden Protokollschichten eine prozessorientierte und zuverlässige End-to-End-Kommunikation über verschiedene paketvermittelte Netze hinweg. Erst diese Ergänzung der Paketvermittlung ermöglichte die nahtlose Verbindung einzelner Netze mit dem Internet. Mit der Entwicklung des Internets wurde die Idee der Pakete und der Paketvermittlung nach dem Store-and-Forward-Prinzip vollständig übernommen.

Künftige Netze werden jedoch völlig anders beschaffen sein als die derzeitigen drahtlosen und drahtgebundenen. Aufgrund dessen wird die Normung heute vom 3GPP (drahtloser Teil) zusammen mit der IETF (drahtgebundener Teil) durchgeführt. Das derzeitige Ziel besteht darin, ein *Ökosystem* (oder eine *Pan-Infrastruktur*) zu schaffen, welches in der Lage ist, sehr heterogene Netze miteinander zu verbinden, gleichzeitig aber auch anspruchsvolle Anforderungen zu erfüllen und mehrere verschiedene Branchen zu unterstützen. Der wichtigste Faktor zur Erreichung dieses Ziels ist die Virtualisierung: die Einführung von Software-Defined Networking (SDN) [NMN+14] und Network Function Virtualization (NFV) [MSG +16] auf allen Ebenen. Das Hauptmerkmal der Netzwerkvirtualisierung ist die softwarebasierte Implementierung von Funktionen, Protokollen und Operationen, die auf Allzweckhardware ausgeführt werden.

Der so genannte Prozess der *Softwarisierung* des Netzes hat einen fruchtbaren Boden für effiziente und effektive neue Paradigmen, wie Cloud- und Edge-/Fog-Computing, eine einzigartige und flexible/rekonfigurierbare SDN-NFV-Architektur und End-to-End Network Slicing [LSC+17, RBSG16] (mit vollständiger Isolierung zwischen Slices und Diensten) geschaffen. In der Tat wurden erhebliche Forschungsanstrengungen auf die Entwicklung eines gemeinsamen/einzigartigen SDN-NFV-Systems gerichtet. Darüber hinaus zielt das neue Paradigma des Betriebssystems für drahtlose Netze (WNOS) auf extreme Flexibilität ab – Netzeinheiten werden vollständig abstrahiert, indem es einen programmierbaren Protokollstapel (PPS) und nicht nur Netzfunktionen und Routing bereitstellt.

Ein derart komplexes und heterogenes System erfordert, dass künftige Netze sich weniger auf menschliches Eingreifen und mehr auf maschinelles Lernen/Kognition für die Netzverwaltung verlassen. In der Tat konzentriert sich ein zunehmender Forschungstrend auf den Einsatz von virtueller Netzwerkorchestrierung, um die Netzverwaltung autonom zu machen. Parallel zur Virtualisierung hat die Forschungsgemeinschaft begonnen, selbstorganisierte Netze (SONs) zu untersuchen, indem sie maschinelles Lernen und kognitive Algorithmen zur Selbstheilung und Selbstverwaltung umfassend einsetzt.

Die Vision künftiger Netze beinhaltet die Realisierung von Cloud- und Edge-Computing in immer stärker verteilter Form, um unterschiedlichen rechtlichen und technischen Anforderungen gerecht zu werden und gleichzeitig die Ausfallsicherheit bei der Datenspeicherung und -verarbeitung zu erhöhen. Die Datenverarbeitung wird dabei ein wesentliches Merkmal künftiger Netze sein. Die Platzierung der Datenverarbeitung in einem bestimmten Rechenzentrum (z. B. Big, Micro, Femto usw.) wird sich auf die Sicherheit, Ausfallsicherheit, Kapazität und Latenz einer bestimmten Ende-zu-Ende-Kommunikation auswirken. Darüber hinaus kann sich der verteilte Charakter des künftigen Computerparadigmas auch auf die Endnutzer auswirken. Aufgrund der herausragenden Rolle, welche die Datenverarbeitung in den Netzen der künftigen Generation spielen wird, insbesondere wenn sie in verteilter Form erfolgt, wird sich das Paradigma des Netzes radikal ändern: von der ausschließlichen Übermittlung von Informationen zwischen zwei Orten unter Verwendung von *„Store and Forward" (Speichern und Weiterleiten)* zu einer Verarbeitung von Informationen innerhalb des Kommunikationsnetzes unter Verwendung von *„Compute and Forward"* [FGS20].

Die oberhalb kurz beschriebenen Merkmale künftiger Netze sagen einen sehr hohen Bedarf an Speicherkapazität und Recheninfrastruktur voraus. Dies wird auch den Energieverbrauch in Kommunikationsnetzen erheblich steigern. Darüber hinaus wird die Realisierung intelligenter und anpassungsfähiger Netze eine große Anzahl von Ressourcen für die sichere Datengewinnung/-verarbeitung und das verteilte Rechnen zur Entscheidungsfindung erfordern. Die intelligente Analyse von Big Data wird kontinuierlich die Netzwerkleistung und die Netzwerkinfrastruktur kennen müssen, um zukünftige Netzwerkzustände vorherzusagen. Darüber hinaus wird sich die Synchronisierung hochgradig verteilter Recheneinheiten auch auf die Anforderungen in Bezug auf Kapazität, Latenz und Zuverlässigkeit auswirken.

Was die Leistungen künftiger Kommunikationsnetze angeht, so sind einige der gewünschten Leistungskennzahlen (KPIs) [ARS16]: Latenzzeit von 1 ms für den Hin- und Rückweg, Milliarden von angeschlossenen Geräten, wahrgenommene Verfügbarkeit von 99.999 % und Reduzierung des Energieverbrauchs um fast 90 %. Diese KPI-Ziele werden es 5G- und darüber hinausgehenden Netzen ermöglichen, mehrere mögliche End-to-End-Kommunikationsparadigmen/-dienste zu unterstützen. Solche Dienste, auch *Vertikale* genannt, werden in der Regel in drei Hauptkategorien eingeteilt: Extreme Mobile Broadband (xMBB), ultrazuverlässige maschinelle Kommunikation (uMTCs) – auch Ultra-Reliable Low-Latency Communications (URLLCs) genannt – und massive maschinelle Kommunikation (mMTCs).

Die gleichzeitige Erfüllung dieser Anforderungen durch die oben beschriebenen Algorithmen und Lösungen ist auf den bestehenden Bereich der Kommunikation auf der Grundlage der klassischen Physik beschränkt. Die Anforderungen sind mit einem enormen Aufwand und einer enormen Komplexität verbunden, garantieren aber keine erfolgreiche Lösung. Im Folgenden wird dargelegt, warum die inhärenten Nachteile der Netze der künftigen Generation ihre Möglichkeiten einschränken werden.

Der Prozess der *Softwarisierung* in zukünftigen Netzen muss eine hohe Flexibilität erreichen, um die Betriebsausgaben (OpEx) und die Investitionsausgaben (CapEx) zu reduzieren. Software und Virtualisierung können dabei als die DNA der Infrastruktur von 5G und darüber hinausgehenden Netzen angesehen werden. Allerdings führt die Softwareabstraktion auch zu zusätzlichen Verzögerungen bei der Paketverarbeitung. Tatsächlich erhöht sie die Anforderungen an die Datenübertragung und die Berechnungen, so dass die Latenz relativ hoch wird. Auch wenn die vorhandenen virtuellen Switches recht schnell sind, sind virtuelle Maschinen (VMs), insbesondere die Paket-IO- und -Verarbeitungsvorgänge innerhalb der VM, langsam. Zwei Software-Bridges (oder virtuelle Switches) verbinden die virtuellen Netzwerkschnittstellen (vNICs) mit der physischen Netzwerkschnittstelle (pNIC). Dann verbindet die Integrationsbrücke alle VMs, die auf demselben physischen Knoten laufen.

Ein vorgeschlagener, zentralisierter Ansatz für die Virtualisierung führt zu einer Latenz von mehr als 2 ms innerhalb der virtuellen Kommunikationsumgebung für eine einzelne VM, die die elementare Weiterleitungsfunktion ausführt [XGU+19], was im Kontext von URLLCs inakzeptabel wird. Einige Lösungen wurden entwickelt, um die Latenz der Virtualisierung deutlich zu verringern [XGU+19], aber immer mehr Software dringt in die Netzwerkschichten ein, so dass die Latenz aufgrund der Netzwerkvirtualisierung voraussichtlich ständig zunehmen wird. Außerdem sind einige Komponenten der Latenz proportional zur verfügbaren Übertragungsbitrate und zur Datenmenge. Dem kann durch eine Erhöhung der Übertragungskapazitäten und der Komprimierung entgegen gewirkt werden, aber die Verarbeitungsverzögerungen mit ihren verschiedenen konstanten Verzögerungen beeinflussen die Latenz immer noch mit einem, nicht zu vernachlässigenden Beitrag.

Beim Einsatz der Netzvirtualisierung sind weitere wichtige Aspekte zu berücksichtigen: Zuverlässigkeit und Ausfallsicherheit (d. h. Aufrechterhaltung eines akzeptablen Dienstes im Falle von Störungen). Softwarebasierte Netzfunktionen und -anwendungen sind nämlich anfälliger für Ausfälle als hardwarebasierte, da sie mehr Fehlerpunkte aufweisen. Dies macht es schwieriger, die gewünschte Netzwerkflexibilität mit zukünftigen KPIs der Netzwerkzuverlässigkeit und Serviceverfügbarkeit in Einklang zu bringen [GB18, LJK+16]. Darüber hinaus hat die Realisierung von Cloud- und Edge-Computing in immer stärker verteilter Form auch Auswirkungen auf die Datenspeicherung und die Rechenleistung in Rechenzentren. Die Platzierung der Datenverarbeitung in einem bestimmten Rechenzentrum (z. B. Big, Micro, Femto usw.) wirkt sich auf die Ausfallsicherheit, Kapazität und Latenz einer bestimmten Ende-zu-Ende-Kommunikation aus. Darüber hinaus könnte sich der verteilte Charakter des künftigen Datenverarbeitungsparadigmas auch auf das Endgerät des Nutzers ausdehnen, wodurch weitere Verzögerungs- und Fehlerpunkte hinzukommen.

Wird Software zum Grundpfeiler künftiger Kommunikationsnetze, verbessern sich, wie oberhalb erwähnt, einige Leistungskennzahlen, jedoch eröffnen sich auch verschiedene neue Sicherheitsbedrohungen. Ein großes Sicherheitsproblem von SDN-NFV-basierten Systemen ist die Bedrohung durch die Skalierbarkeit. Controller und Hypervisoren können aufgrund der Menge an Steuerdatenverkehr, die sie

verwalten müssen, leicht zu Engpässen werden. Die Sättigung der Steuerungsebene öffnet die Tür für verschiedene Denial-of-Service- (DoS) und verteilte DoS-Angriffe (DDoS). Im Hinblick auf das Netzwerkmanagement und die Orchestrierung ist die Authentifizierung von Anwendungen von grundlegender Bedeutung. Es ist notwendig, eine Vertrauensbeziehung zwischen der Steuerungsebene und den Anwendungen herzustellen. Im SDN sind effektive Zugangskontroll- und Verantwortlichkeitsmechanismen immer noch eine offene Herausforderung. SDN kann von einem böswilligen Host angegriffen werden, der Pakete mit gefälschten Quelladressen für die mittlere Zugriffskontrolle sendet, um die Tabelle der mittleren Zugriffskontrolle eines Switches zu vergiften. Viele weitere Sicherheitsbedrohungen aufgrund der *Softwarisierung von* Netzwerken und der Berechnung von Netzwerkfunktionen sind in [ANYG15, AvW18, DCA+17, FTKS19, PHS+18, SNS16] zu finden.

Der Paradigmenwechsel von *„Store and Forward“* zu *„Compute and Forward“* wird die eingesetzten Rechenressourcen im Netz und die Größe bzw. Anzahl der Rechenzentren massiv erhöhen. Dies impliziert einen erheblichen Anstieg des Energieverbrauchs aufgrund von Virtualisierung und *Softwarisierung* [BGADR19, BIK +16, DWF16, JHA+16, JITT16]. Der Verbrauch eines großen Rechenzentrums entspricht in etwa etwa 25.000 Haushalten, und die Energiekosten für den Betrieb eines Rechenzentrums verdoppeln sich alle 5 Jahre (und diese Rate wird aufgrund des massiven Einsatzes von Computern noch steigen) [DWF16]. Ein solcher Energiebedarf bringt auch Umweltprobleme mit sich (z. B. entsprach 2005 der gesamte Stromverbrauch von Rechenzentren 1 % des gesamten Stromverbrauchs der USA und verursachte die gleiche Menge an Emissionen wie ein mittelgroßes Land [DWF16]). Für die Datenverarbeitung benötigte Energie kann dabei in zwei Hauptkategorien unterteilt werden: Energie, die von Netzwerk-/Rechenanlagen (z. B. Server, Netzwerke, Speicher usw.) verbraucht wird, und Energie, die von Infrastruktureinrichtungen (wie Kühlung, Klimaanlage usw.) genutzt wird.

Darüber hinaus werden für die Realisierung intelligenter, anpassungsfähiger Netze riesige Mengen an Ressourcen für die sichere Datengewinnung/-verarbeitung und die verteilte Datenverarbeitung zur Entscheidungsfindung benötigt. Intelligente Big-Data-Analysen benötigen kontinuierlich Informationen über die Netzleistung und die Netzinfrastruktur, um künftige Netzzustände vorhersagen zu können. Darüber hinaus wird sich die Synchronisierung hochgradig verteilter Recheneinheiten auch auf die Anforderungen in Bezug auf Kapazität, Latenz und Zuverlässigkeit auswirken.

Klassische Netze der künftigen Generation stellen auch ein *Problem der Kommunikationskomplexität* dar. Die Kommunikationskomplexität ist die Menge an Informationen (in Form von Bits), die räumlich getrennte Rechengeräte austauschen müssen, um eine Rechenaufgabe erfolgreich durchzuführen. Virtualisierungs- und Rechenparadigmen, wie Mobile Edge Computing (MEC) und verteiltes Rechnen, für Netzfunktionen beruhen auf verteilten Geräten, die netzbezogene Rechenaufgaben lösen. Es hat sich jedoch gezeigt, dass einige dieser verteilten Rechenprobleme nicht durch verteiltes Rechnen auf der Grundlage klassischer Netze gelöst werden können. Neben den lösbaren Problemen wurde gezeigt, dass die Menge der Kommunikationsbits, die für die Kommunikation zwischen verteilten Recheneinheiten

verwendet werden, einen starken Einfluss auf die Verbindungen des Netzwerks hat (Techniken zur Kompression und Kodierung sind nicht in der Lage, dieses Wachstum effektiv zu begrenzen) [BCMdW10]. Ein solches Komplexitätsproblem erinnert logischerweise an das bereits erwähnte Problem der Latenz, da die Verzögerung ebenfalls proportional zur verfügbaren Übertragungsbitrate ist.

Schließlich wird die Integration mehrerer Dienste heute durch Richtlinien auf höherer Ebene realisiert, die verschiedene Dienste auf verschiedenen logischen Kanälen zuweisen. Das Sicherheitsproblem wird in der Regel durch die Anwendung kryptographischer Techniken auf höheren Ebenen gelöst. Im Allgemeinen ist dieser Prozess ineffizient, und es gibt einen Trend zur effizienten Zusammenlegung mehrerer nebeneinander bestehender Dienste, so dass sie mit denselben drahtlosen Ressourcen arbeiten. Dies wird als Integration von Diensten auf der physikalischen Schicht bezeichnet [SB14a] und hat das Potenzial, die spektrale Effizienz von Netzen der nächsten Generation erheblich zu steigern. Es wird erwartet, dass verschiedene Anwendungen (z. B. sichere Nachrichtenübertragung, Rundsenden gemeinsamer Nachrichten und Nachrichtenübertragung) alle durch die *Integration von Diensten der physikalischen Schicht* implementiert werden. Die Referenzen [DS05, HW10a] waren die ersten Arbeiten für Quantensysteme, die eine größere Vielfalt von Diensten anbieten.

1.2 Auf dem Weg zu Quantenkommunikationsnetzen

Im vorangegangenen Unterkapitel wurde der Weg zum aktuellen, neuen Paradigma vorgestellt, das durch künftige 5G-Netze und darüber hinausgehend gefördert wird. Die Kommunikationsnetze haben sich dabei von leitungsvermittelten zu paketvermittelten Netzen entwickelt. In beiden Fällen dominiert das Ende-zu-Ende-Design, welches den transparenten Transport von Bits ermöglicht (siehe Abb. 1.1). In einem solchen System wird die Latenz durch die Ausbreitungsverzögerung der Kommunikationsverbindung beeinflusst.

Um die Ausbreitungsverzögerung zu verringern, wurden den Kommunikationsknoten Rechen- und Speicherkapazitäten hinzugefügt, um Berechnungen in der unmittelbaren Nähe zu ermöglichen (Schema in der zweiten Zeile von Abb. 1.1). Mit Hilfe der oben erwähnten Virtualisierungsparadigmen konnte die Ausbreitungslatenz erheblich reduziert werden. Das MEC war für diesen Zweck besonders grundlegend.

Doch auch wenn die Virtualisierung dazu beigetragen hat, die Kommunikationslatenz aufgrund der Ausbreitung zu verringern, hat sie die Latenz in jeder beteiligten virtuellen Maschine [XGU+19] erhöht. Der Grund liegt darin, dass alle verarbeiteten Informationsbits mehrere softwarebasierte Virtualisierungsschichten durchlaufen müssen (siehe Abb. 1.1, Schema in der Mitte). Daher können nicht nur bestehende, sondern auch zukünftige Lösungen für *softwarisierte* Netze nur Anwendungen mit einer kleinen Anzahl von virtuellen Maschinen unterstützen. Diese Einschränkung ist notwendig, um die Komplexität der Netze nicht zu schnell ansteigen zu lassen.

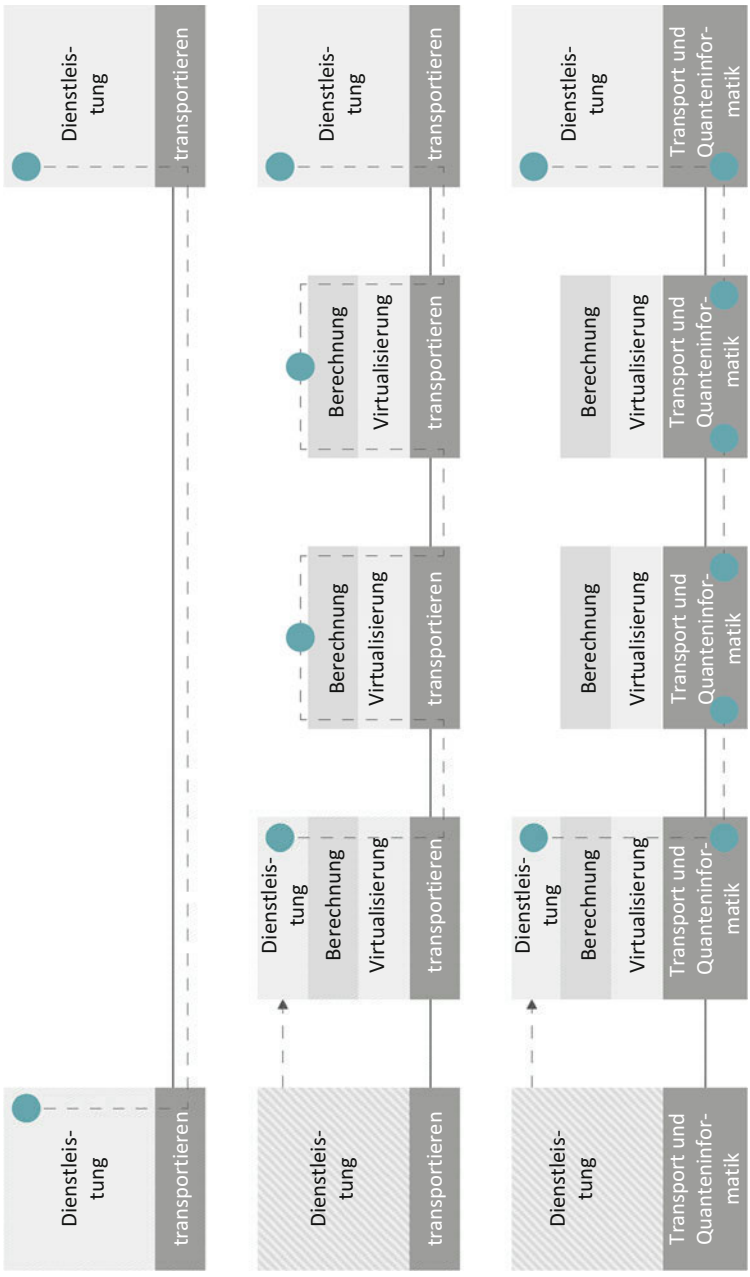

Abb. 1.1 Logisches Schema zur Darstellung des Paradigmenwechsels entsprechend der Entwicklung der Kommunikationsnetze

Alle hier und im vorangegangenen Abschnitt genannten Nachteile, die auf die inhärenten klassischen Beschränkungen sowohl der Virtualisierung als auch der Datenverarbeitung zurückzuführen sind, können nur durch die Entwicklung von inhärent anderen, auf der Quantenmechanik basierenden Netzen überwunden werden. Auf diese Weise wird das klassische Netzwerk-Computing in das quantenmechanische Netzwerk-Computing überführt: Durch den Paradigmenwechsel werden virtuelle Netzwerk-/Rechenressourcen, die auf Software basieren, in neue physikalische Quantenressourcen überführt, die auf Verschränkung beruhen, welche sich in klassischen Systemen nicht offenbart.

So wie die klassischen Netze ursprünglich auf der bestehenden Telefoninfrastruktur aufgebaut wurden, werden die heutigen quantenmechanischen Netze in hybrider Weise auf den bestehenden klassischen Netzinfrastrukturen aufgebaut.

Durch den Einsatz von verteiltem Quantencomputing anstelle von klassischem Computing kann eine einzigartige virtuelle Quantenmaschine, die aus einer großen Anzahl verschränkter Qubits besteht, die mit der Anzahl der miteinander verbundenen Geräte skaliert, eine exponentielle Beschleunigung der Rechenkapazitäten eines Netzes mit einer nur linearen Zunahme der physischen Ressourcen erreichen. Auf diese Weise können die Beschränkungen, die klassische Paradigmen der Virtualisierung und *Softwarisierung* auferlegen, durch die Ausnutzung der quantenphysikalischen Parallelität auf der Grundlage der Konzepte der Quantenüberlagerung, der Verschränkung und der Quantenmessung überwunden werden (siehe unten in Abb. 1.1).

Bestehende Ansätze, welche die Quantenmechanik in Netzen zur Gewährleistung der Sicherheit nutzen, führen hauptsächlich Protokolle für den Schlüsselaustausch zwischen einzelnen Knoten aus. In vielen Fällen wird die Quantenschlüsselverteilung (QKD) von einem Knoten zum anderen verwendet. Andererseits gibt es nur wenige Analysen, die sich mit der Komplexität und Kapazität dieser Prozesse befassen. Daher konzentrieren sich die derzeitigen Forschungen und Investitionen hauptsächlich auf die militärische und staatliche Kommunikation, während zivile Nutzer stark auf Geschwindigkeit und Komplexität bedacht sind (die die Latenzzeit und die Qualität der Kommunikation erheblich beeinflussen).

Das Potenzial der Quantenmechanik für Kommunikationssysteme wurde schon früh erkannt. Holevos Arbeit [Hol73] von 1973 betrachtet die klassische Kommunikation über Quantenkanäle. Im Jahr 1984 entwickelten Bennett und Brassard in [BB84] das erste Quantenkryptographieprotokoll. In [BB84] wurde eine nachweislich sichere Kommunikationstheorie erwähnt und berücksichtigt. Anfang 1990 wurden neue Quantenprotokolle zur Lösung von Quantenkommunikationsaufgaben über Quantenkanäle entwickelt. Dazu gehörte z. B. die Quantenteleportation. Dabei handelt es sich um ein Verfahren, bei dem Quanteninformationen mit Hilfe klassischer Kommunikation und zuvor geteilter Quantenverschränkung zwischen Sende- und Empfangsort von einem Ort zum anderen übertragen werden können. Die bahnbrechende Arbeit hierzu wurde 1993 von Bennett, Brassard, Crépeau, Jozsa, Peres und Wootters veröffentlicht [BBC+93].

Außerdem sind viele klassische Kodierungsmethoden und informationstheoretische Ansätze, die in dieser Zeit gezeigt wurden, aufgrund der Heisenbergschen

Unschärferelation quantenmechanisch nicht anwendbar. Ein prominentes Beispiel ist das No-Cloning-Theorem [WZ82]. Nach 2000 konnten mehrere exakte informationstheoretische Kapazitätsergebnisse bewiesen werden. Zu diesen Ergebnissen gehören z. B. die private Übertragung [Dev05], die Destillation von geheimen Schlüsseln und Verschränkung aus Quantenzuständen [DW05] und die Quantenabhörkanäle [CWY04]. Alle experimentellen Systeme bieten heute im Wesentlichen eine Schlüsselgenerierung in der Punkt-zu-Punkt-Kommunikation.

Die Idee hinter Quantenkommunikationsnetzen [SR00, Kim08, WEH18] besteht darin, dass die Knoten des Netzes als verteilte Teile desselben physikalischen Systems betrachtet werden können. Der Grund, warum Quantenkommunikationsnetze das klassische Internet mit relativ bescheidenen Ressourcen übertreffen können, liegt in den inhärenten Eigenschaften quantenmechanischer Systeme. Insbesondere die Verschränkung wird als Ressource für die Kommunikation genutzt.

Verschränkung ist der Hauptpfeiler für effektives verteiltes Quantencomputing, Teleportation und superdichte Kodierung (um einen effizienteren Durchsatz zu erreichen). Darüber hinaus findet die Verschränkung auch aus einer informationstheoretischen Perspektive einen Interprettionsansatz. Die Quanteninformationstheorie ist ein wichtiger Aspekt sowohl der Quanteninformatik als auch der Quantenkommunikation. Weitere quantenmechanische Aspekte sind die Unmöglichkeit des Kopierens von Informationen (No-Cloning-Theorem) und Qubits (Überlagerung möglicher Zustände).

Auf Quantenmechanik basierende Datenverarbeitung und Netze scheinen grundlegende Paradigmen zu sein, die die bestehenden Probleme, mit denen die Forschung und die Industrie bei der Konzeption und Entwicklung künftiger Netze konfrontiert sind, effizient und wirksam lösen werden. In der Tat haben sich Technologien auf der Grundlage der Quantenmechanik (vor allem unter Ausnutzung der Verschränkung) als wirksam für verteilte Systeme erwiesen und garantieren gleichzeitig die Sicherheit der Kommunikation und der Datenverarbeitung in der Cloud. Darüber hinaus ist die Realisierung kleiner, verteilter und miteinander verbundener Recheneinheiten auf Quantenbasis die quanteneffizientere Version des derzeitigen MEC-Paradigmas. Beispielsweise können Wissenschaftler verteiltes Quantencomputing nutzen, um hochkomplexe wissenschaftliche Berechnungsprobleme, wie die Analyse chemischer Wechselwirkungen für die medizinische Arzneimittelentwicklung, zu lösen. Dies ist mit klassischen Netzen und Rechnern nicht effizient und effektiv möglich.

Im Hinblick auf die derzeitigen Bemühungen um intelligente Netze auf der Grundlage von Data Mining und verteilter Datenverarbeitung können Algorithmen für maschinelles Lernen mit Quantencomputern, die auf verteilten Quantencomputerknoten laufen, sicher, effektiv und effizient (in Bezug auf die Nutzung von Netzressourcen und Energie) sein.

Darüber hinaus hat die Quantenkommunikation erhebliche Vorteile bei der Kommunikation erzielt, bei der mehrere Quellen über einen einzigen Kommunikationskanal Informationen an einen einzigen Empfänger übertragen [Nö19, LALS20]. Insbesondere der Vergleich zwischen klassischen und Quanten-Mehrfachzugriffskanälen (MAC), bei denen zwei Quellen an ein Ziel übertragen, hat

gezeigt, dass die Quantenkommunikation die Erfolgswahrscheinlichkeit der klassischen Kommunikation aufgrund der Ausnutzung der Verschränkung übertrifft.

Andererseits können Quantennetze nicht nur die Fähigkeiten der derzeitigen klassischen Netze übertreffen, sondern auch ein grundlegendes Mittel für andere Aspekte von Kommunikationsnetzen sein. Komplexe Quantennetzwerke können auf der Quantenebene, zwischen atomaren Ensembles, realisiert werden. Diese speziellen Quantennetze können dazu verwendet werden, beliebige Verbindungen innerhalb des Netzes zu erzeugen und so ein zufälliges Verhalten zu erreichen. Mit Hilfe dieser zufälligen Quantennetzwerke eröffnet sich die Möglichkeit, komplexe Probleme der realen Welt zu analysieren und zu modellieren. So könnten zufällige Quantennetze dazu beitragen, die Kommunikation in realen physikalischen oder biologischen Systemen zu modellieren, und es ergibt sich ein Erweiterungsansatz, um das Verhalten globaler Kommunikationsnetze (das klassische bestehende Internet) zu modellieren. Durch die Nutzung der Quantenkommunikation und der stochastischen Natur von Quantensystemen können schlussendlich auch die noch unentdeckten Verbindungen in der realen Kommunikation besser untersucht werden [IG12].

Schließlich sagt man Quantenkommunikationsnetzen zu, dass sie das im vorigen Abschnitt erwähnte *Problem der Kommunikationskomplexität* lösen können. Betrachten wir beispielhaft verschiedene Netzwerkknoten. Zunächst besitzen die knoten Daten und dürfen untereinander nicht kommunizieren. Ihr Ziel ist es, eine Funktion ihrer Daten zu berechnen, um Ausgabebits zu erzeugen. Eine solche Rechenaufgabe (d. h. die Berechnung einer Relation) ist nicht trivial, da sowohl die eigenen als auch die Ausgabebits auf die Parteien verteilt sind; jeder Knoten hat also nur den Wert einer seiner Teilmengen. Wie bereits erwähnt, müssen bei der klassischen Kommunikation Übertragungen zwischen den Parteien stattfinden, um erfolgreich zu sein. Die Verschränkung kann zwar die Kommunikation nicht ersetzen, aber sie kann die Kommunikationslast erheblich verringern [BCMdW10].

Die Parteien können über Bits oder Qubits miteinander kommunizieren, wobei sie *klassischerweise* Zufallsinformationen austauschen, oder alternativ verschränkte Quantenzustände austauschen, wenn Quantenkommunikation in Betracht gezogen wird (dieses Konzept wird in Abschn. 2.5 näher erläutert). Wie viele Kommunikationsbits oder Qubits sind für das Rechnen mindestens erforderlich? Die Verschränkung kann nicht zur Signalisierung verwendet werden, aber sie kann die für das verteilte Rechnen erforderliche Kommunikation reduzieren. Je nach Rechenproblem kann die Kommunikationskomplexität auf $n/2$ (durch superdichte Kodierung) oder sogar noch weiter reduziert werden, z. B. auf $\sqrt{n}$ und $\frac{n^{1/4}}{\log n}$, wenn n die Anzahl der Bits ist, welche im Falle der klassischen Kommunikation übertragen werden müssten [BCMdW10].

1.3 Aufbau des Buches

Ziel dieses Buches ist es, den Lesern einen grundlegenden Hintergrund und die Richtlinien für die Untersuchung und den Entwurf von Quantenkommunikationssystemen mit Hinblick auf die Netze der nächsten Generation zu vermitteln. Zu diesem Zweck erklärt das Buch auf verständliche Weise die grundlegenden Konzepte der Quantenmechanik, der Quanteninformationstheorie, des Quantencomputers und der Quantenkommunikationsnetze in seiner Ganzheit, wobei sowohl die Perspektive der Physiker als auch die der Ingenieure berücksichtigt wird.

Das Buch versucht dabei, ein Gleichgewicht zwischen der Vermittlung von Inhalten in einer zugänglichen Weise und der Genauigkeit, sowie Präzision herzustellen. Auf diese Weise erhält der Leser ein grundlegendes Wissen und ein tiefes Verständnis für die Forschung im Bereich der Quantenkommunikationsnetze (QCNs).

Abb. 1.2 zeigt ein logisches Venn-Diagramm zum Thema *Quantenkommunikationsnetze*. Dieses Forschungsgebiet ist die Vereinigung von Teilbereichen wie Quantencomputing und Quantenkommunikation. Diese beiden Makro-Themen überschneiden sich und stützen sich auf die Quanteninformationstheorie und die Quantenfehlerkorrektur. Schließlich umfasst der Themenbereich Quantencomputing die Problematik der Programmierung von Quantenhardware.

Abb. 1.3 zeigt die Zuordnung des Venn-Logikdiagramms zu den verschiedenen Kapiteln des Buches und schlägt die präferierte Leserichtung vor. Kap. 2 stellt die grundlegenden Konzepte vor, die zum Verständnis aller Ergebnisse und Ideen im Bereich der Quantenkommunikationsnetze erforderlich sind. Anschließend werden in Kap. 3 die Grundlagen des Quantencomputings und der Quantenschaltungen,

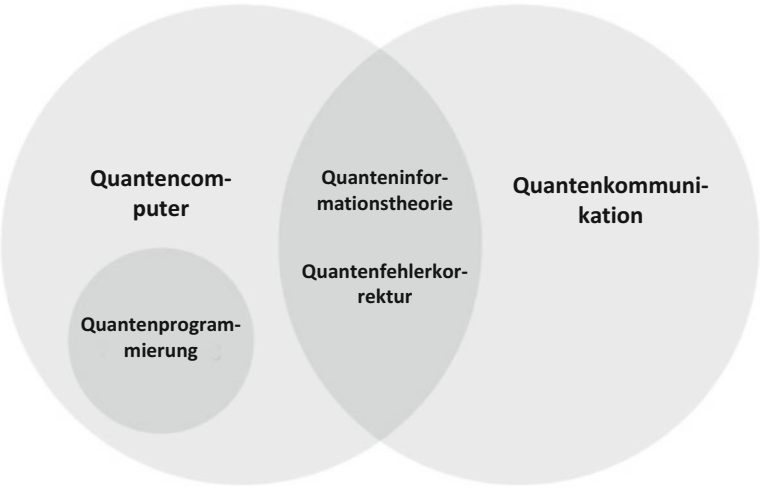

Abb. 1.2 Venn-Logik-Diagramm, welches die wichtigsten Forschungsteilbereiche (und ihre Beziehungen) auf dem Forschungsgebiet der Quantenkommunikationsnetze darstellt