



UNIVERSITÀ
DEGLI STUDI
FIRENZE

UNIVERSITÀ DEGLI STUDI DI FIRENZE
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE (DINFO)
CORSO DI DOTTORATO IN INGEGNERIA DELL'INFORMAZIONE
CURRICULUM: TELECOMMUNICATIONS AND TELEMATICS

ARCHITECTURES AND PROTOCOLS
DESIGN FOR NON-TERRESTRIAL
QUANTUM NETWORKS

Candidate

Roberto Picchi

Supervisors

Prof. Francesco Chiti

Prof. Laura Pierucci

PhD Coordinator

Prof. Fabio Schoen

CICLO XXXV, 2019-2022

Università degli Studi di Firenze, Dipartimento di Ingegneria
dell'Informazione (DINFO).

Thesis submitted in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Information Engineering. Copyright © 2023 by
Roberto Picchi.

“In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of University of Florence’s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink. If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.”

*To my parents Giuseppe and Fanny
To Annalisa*

Acknowledgments

I would like to thank Prof. Romano Fantacci, who gave me the opportunity to carry out this project. I would also like to thank my supervisors, Prof. Francesco Chiti and Prof. Laura Pierucci, who followed me daily and gave me precious advice that allowed me to grow significantly from a personal and professional point of view. I also thank Prof. Dania Marabissi with whom I started working here and Prof. Tommaso Pecorella. Moreover, I want to thank all the guys I met in the DaCoNets laboratory who warmly embraced me and with whom I had a great time: Adnan Rashid, Michele Bonanni, Benedetta Picano, Francesca Nizzi, Giulio Bartoli, Alessio Bonadio, Andrea Tani, Andrea Stomaci. I thank all these wonderful people from the deep of my heart.

I would like to thank the people closest to me: my parents, Giuseppe and Fanny, and my fiancée Annalisa, who have always supported me and given me the strength to keep going. I thank all my family and Annalisa's family. I love all of you.

Roberto Picchi

*“Joy in looking and comprehending
is nature's most beautiful gift”
Albert Einstein*

Abstract

Quantum mechanics has developed during the course of the first thirty years of the twentieth century by some of the greatest minds of that time, bringing to fruition a transformation in the vision of things in the physical world. However, for a long time there was not much emphasis on the physical ways in which a quantum computing device could have been built. Richard Feynman began to think about the possibility of creating a real Quantum Computer (QC), trying to conceive a working machine based on the principles of quantum physics. In his work of 1982, he demonstrated that no classic Turing Machine could simulate certain physical phenomena without incurring in an exponential slowdown of its performance, whereas a quantum machine could have performed the simulation more efficiently. In 1985, David Deutsch of the University of Oxford described the first quantum machine by formalizing Feynman's ideas. Afterward, David Deutsch and other American scientists built models of QCs to study the differences between them and the classical ones.

During the last three decades, classical telecommunications networks have had an extraordinary development, and in recent years research is increasingly focusing on the creation of networks consisting of heterogeneous Quantum Devices (QDs). In particular, many researchers focused on the study of terrestrial quantum communications over typical Optical Fibers (OFs) links. However, this technology is affected by extremely high losses that can be faced only through the deployment of several repeaters, which in turn involve impractical costs for end-to-end (E2E) route management. Quantum Satellite Networks (QSNs) can overcome the limitations of terrestrial optical networks, such as remarkable signal attenuation over long distances and difficulty of intercontinental communications. The recent studies on quantum satellite communications motivated our research towards a Low Earth Orbit (LEO) quantum satellite backbone for interconnecting quantum on Earth Servers in order to achieve an unprecedented computational capacity. Specifically, this thesis proposes a near optimum E2E path evaluation procedure allowing an efficient switching in order to maximize the entanglement generation rate. Indeed, this is one of the main issues that involve the Data Link Layer and the Network Layer of the Quantum Internet (QI) protocol stack, which is in its early standardization phase. In particular, the architectures presented in this thesis consider the use of the Software-Defined Networking (SDN) paradigm with the aim of minimizing the number

of hops for E2E connection and maximizing network capacity. Therefore, the thesis compares distributed and centralized approaches in order to achieve a trade-off between performance and cost. Furthermore, the performance of different constellations with flight plans based on existing constellations is compared, spanning from LEO up to micro-satellites, to properly derive some guidelines for designing an efficient backbone. Specifically, the focus is on evaluating the impact of different path selection and satellite deployment solutions on the E2E capacity to achieve a trade-off between performance and cost.

In addition, the recent technological developments in terms of quantum satellite communications and the application of SDN to the satellite case, motivated our investigation on an ad hoc quantum satellite backbone design based on the SDN paradigm with a Control Plane (CP) directly integrated into the constellation itself. As a matter of fact, the aim is to outline some guidelines by comparing several options. Specifically, the focus is to analyze different architectural solutions making some considerations on their feasibility, possible benefits, and costs. Finally, we performed some simulations on the architectures we considered the most promising, concluding that the integration of the CP in the constellation itself is the most appropriate solution.

Moreover, this thesis considers the design of an ad hoc quantum satellite backbone based on the SDN paradigm with a modular two-tier CP. The first tier of the CP is embedded into a Master Control Station (MCS) on the ground, which coordinates the entire constellation and performs the management of the CP integrated into the constellation itself. This second tier is responsible for entanglement generation and management on the selected path. In addition to defining the SDN architecture in all its components, we present a possible protocol to generate entanglement on the E2E path. Furthermore, we evaluate the performance of the developed protocol in terms of the latency required to establish entanglement between two Ground Stations (GSs) connected via the quantum satellite backbone.

Finally, this thesis also considers scenarios related to metropolitan quantum networks that make use of drone technology, which are also widely used in the 5G and 6G contexts. Specifically, swarms of drones are utilized in a wide range of applications, considering that they can be deployed on-demand and are very economically affordable. Therefore, they can also have a significant role in the creation of future Quantum Networks (QNs). As a

matter of fact, the use of drones allows deploying a non-terrestrial Quantum Metropolitan Area Network (QMAN), overcoming OFs' limits, due to the large percentage of photons that scatter before reaching the receiver. However, since random fluctuations concerning drones' positions and atmospheric turbulence, the quality of the Free Space Optics (FSO) link can be affected with a significant impact on performance. Considering that Quantum Drone Networks (QDNs) require significant control, SDN technology can play a key role in their provisioning. Specifically, an SDN Controller is responsible for managing the global strategies for the distribution of E2E entangled pairs. Therefore, this thesis provides an SDN-based architecture for supporting high-performance Metropolitan Quantum Drone Networks (MQDNs) with a specific protocol that allows creating entanglement between two GSs through the swarm of drones. The proposed architecture can be employed for distributed quantum computing applications and entanglement-based Quantum Key Distribution (QKD) services. Moreover, an objective function to optimize the planning and operation of the swarm mission has been proposed. Finally, this thesis provides a performance evaluation considering the most relevant metrics, such as fidelity, entanglement rate, and the overhead of the proposed protocol.

Acronyms

ACO Ant Colony Optimization.

API Application Programming Interface.

ATP Acquisition, Tracking, and Aiming.

BS Bloch's Sphere.

BSM Bell State Measurement.

BYOD Bring Your Own Device.

CB Computational Basis.

CBS Computational Basis State.

CNOT Controlled NOT.

COTS Commercial Off-The-Shelf.

COW Coherent One-Way.

CP Control Plane.

CVQKD Continuous-Variable QKD.

DCR Detector Count Rate.

DM Density Matrix.

DP Data Plane.

DPS Differential Phase Shift.

DQC Distributed Quantum Compiler.

DTN Delay-Tolerant Networking Architecture.

DVQKD Discrete-Variable QKD.

E2E end-to-end.

EP Equatorial-Polar.

EPS Entangled Photon Source.

FIR Far-Infrared.

FSO Free Space Optics.

GCRS Geocentric Celestial Reference System.

GEO Geostationary Earth Orbit.

GHZ Greenberger-Horne-Zeilinger.

GMCS Gaussian Modulated Coherent-State.

GNSS Global Navigation Satellites Systems.

GPS Global Positioning System.

GS Ground Station.

GSO Geosynchronous Orbit.

HAP High Altitude Platforms.

HEO Highly Elliptical Orbit.

HOM Hong-on-Mandel.

IDS/IPS Intrusion Detection System/Intrusion Prevention Systems.

IMU Inertial Measurement Unit.

IoT Internet of Things.

ISL Inter-Satellite Link.

ISS International Space Station.

L2L Link-to-Link.

LAP Low Altitude Platforms.

LEO Low Earth Orbit.

LIR Long-Infrared.

LLO Low Lunar Orbit.

LO Local Oscillator.

LOS Line of Sight.

MA-QKD MA measurement-device independent QKD.

MCS Master Control Station.

MEO Medium Earth Orbit.

MIR Mid-Infrared.

ML Machine Learning.

MQDN Metropolitan Quantum Drone Network.

MRW Modified Random Walk.

NetSquid Network Simulator for Quantum Information using Discrete events.

NGN Next-Generation Network.

NIR Near-Infrared.

NORAD North American Aerospace Defense Command.

NOS Network Operating Systems.

NTN Non-Terrestrial Network.

NV Nitrogen Vacancy.

OF Optical Fiber.

OSPF Open Shortest Path First.

PDF Probability Density Functions.

QBER Quantum Bit Error Rate.

QC Quantum Computer.

QCS Quantum Computing System.

QD Quantum Device.

QDC Quantum Data Center.

QDN Quantum Drone Network.

QEC Quantum Error Correction.

QI Quantum Internet.

QKD Quantum Key Distribution.

QM Quantum Memory.

QMAN Quantum Metropolitan Area Network.

QML Quantum Machine Learning.

QN Quantum Network.

QND Quantum Nondemolition Detectors.

QoS Quality of Service.

QPS Quantum Positioning System.

QPT Quantum Phase Transition.

QR Quantum Repeater.

QSCS Quantum Satellite Control Station.

QSDN Quantum SDN.

QSN Quantum Satellite Network.

QSR Quantum Satellite Repeater.

QuISP Quantum Internet Simulation Package.

QuNetSim Quantum Network Simulator.

RKA Routing and Key Allocation.

RRA-FSQKD Routing and Resource Allocation in Free Space QKD.

RRDPS Round-Robin Differential Phase Shift.

SDN Software-Defined Networking.

SDP Simplified Deep Space Perturbations.

SeQUeNCe Simulator of QUantum Network Communication.

SGP Simplified General Perturbations.

SIR Short-Infrared.

SLR Satellite Laser Ranging.

SOA Service-Oriented Architecture.

SQUANCH Simulator for Quantum Networks and Channels.

TLE Two-Line Element set.

TOA Time Of Arrival.

UC Unified Communications.

VLEO Very Low Earth Orbit.

VQP Virtual Quantum Processor.

Contents

Abstract	vii
Acronyms	xi
Contents	xvii
List of Figures	xxiii
List of Tables	xxxiii
List of Algorithms	xxxv
List of Equations	xxxvii
I Concepts and Applications	1
1 Introduction	3
1.1 Hystory of Quantum Technologies	3
1.2 Quantum Technologies Market	8
1.3 Technological Principles	9
1.4 Proposed Architectures	14
1.5 Applications	17
1.6 Thesis Contributions	18
1.7 Thesis Organization	19
2 Physical and Technological Principles	21
2.1 Fundamentals of Quantum Information	21
2.1.1 The Postulates of Quantum Mechanics	21
2.1.1.1 First Postulate	21

2.1.1.2	Second Postulate	22
2.1.1.3	Third Postulate	22
2.1.1.4	Fourth Postulate	23
2.1.2	Quantum Informative Unit	23
2.1.3	Entanglement	26
2.1.4	No-Cloning Theorem	28
2.2	Technological Aspects	29
2.2.1	Quantum Gates	30
2.2.1.1	Pauli-X Gate	31
2.2.1.2	Pauli-Y Gate	31
2.2.1.3	Pauli-Z Gate	32
2.2.1.4	Hadamard Gate	32
2.2.1.5	Controlled NOT Gate	33
2.2.2	Swap Circuit	34
2.2.3	Multipartite Entangled States	34
2.2.3.1	Greenberger-Horne-Zeilinger State	35
2.2.3.2	W State	36
2.2.3.3	Advantages and Disadvantages	36
2.2.4	Teleportation	37
2.2.5	Superdense Coding	39
2.2.6	Trace Distance	41
2.2.7	Fidelity	41
2.2.8	Decoherence	42
2.2.9	Quantum Memories and Related Components	46
2.2.9.1	Ion Traps	47
2.2.9.2	Superconducting Qubits	48
2.2.9.3	Quantum Dots	48
2.2.9.4	Solid-State Spin	49
2.2.9.5	Topological	49
2.2.9.6	Quantum Computing Systems	49
2.2.9.7	Cooling Systems	50
2.2.9.8	Matter and Flying Qubits	53
3	Quantum Technologies Applications and Related Works	55
3.1	Fundamentals of Quantum Cryptography	55
3.1.1	Motivations	55
3.1.2	CVQKD	57
3.1.3	DVQKD	58

3.1.3.1	BB84	59
3.1.3.2	E91	64
3.1.4	Quantum Bit Error Rate	67
3.2	Feasibility Studies for Satellite Quantum Networks	68
3.3	Software-Defined Networking Satellite Backbones	69
3.4	Satellite QKD Experiments	70
3.5	Distributed Computing and Quantum Cloud	72
3.6	Positioning	76
3.7	Sensing	80
3.8	Drones	81
3.9	Quantum RADAR	82
 II Design and Performance Analysis		85
4	Quantum Networking	87
4.1	Quantum Networks Elements	87
4.1.1	Quantum and Classical Channels	88
4.1.2	Quantum Repeaters	88
4.2	The Quantum Internet Protocol Stack	90
4.2.1	Physical Layer	90
4.2.2	Link Layer	91
4.2.3	Network Layer	91
4.2.4	Transport Layer	91
4.2.5	Application Layer	91
4.3	Quantum Satellite Systems	91
4.3.1	Motivations	92
4.3.2	Possible Orbits and Constellations	92
4.3.3	Device and Components	96
4.3.4	Quantum Repeaters in Space	100
4.3.4.1	Free Space Optics	102
4.4	Software-Defined Networking	104
4.4.1	Demand	104
4.4.2	Supply	105
4.4.3	Traffic Patterns	105
4.4.4	SDN Architectural Elements	106
4.4.4.1	Control Plane	110
4.4.4.2	Data Plane	112

4.4.5	The Role of SDN in Quantum Networks	113
5	Satellite Architectures and Performance Analysis	117
5.1	Simulation Environment Features	117
5.1.1	Two-Line Element Set	118
5.1.2	Mathematical Models for the Prediction of Satellites Positions	120
5.1.3	Retrieving, Importing, and Working with TLEs	120
5.1.3.1	Satellite Visibility	121
5.2	Control Plane Deployment Solutions Analysis	122
5.2.1	LEO Constellation with a Single Ground Controller .	123
5.2.2	Multi Controller on GEO	124
5.2.3	Multi Controller on MEO	125
5.3	Single Controller on the Ground	125
5.3.1	Problem Statement	128
5.3.2	Proposed Forwarding Strategies	132
5.3.2.1	Modified Random Walk	132
5.3.2.2	Ant Colony Optimization	134
5.3.2.3	Dijkstra's Algorithm	136
5.3.3	Simulations Results	137
5.3.4	Satellite Constellations	144
5.3.5	Simulations Results	148
5.4	Satellite Control Plane Solutions Analysis	153
5.4.1	Modular two-tier Control Plane	153
5.4.1.1	Proposed Architecture	154
5.4.1.2	Protocol	155
5.4.1.3	Simulations Results	160
5.4.2	Multiple Controllers Integrated into the Constellation	162
5.4.2.1	Proposed Reference Architecture	163
5.4.2.2	Entanglement Generation Strategies	165
5.4.2.3	Simulations Results	166
6	Drones Network Architecture and Performance Analysis	171
6.1	Motivations	171
6.2	Simulation Environment	174
6.2.1	NetSquid Simulator	175
6.2.2	NetSquid Simulation Engine	175
6.2.3	NetSquid Quantum Network Elements	178

6.2.4 Other Simulation Environments	179
6.3 System Model	180
6.4 Simulations Results	191
7 Conclusions and Future Works	199
A List of Parameters	207
B Publications	209
Bibliography	211
Index	257

List of Figures

1.1	Moore’s law [1].	4
1.2	History of Quantum Information [2].	6
1.3	Layout of IBM’s four superconducting quantum bit device (false-colored). “IBM Four Qubit Square Circuit (false-colored)” by IBM Research https://www.flickr.com/photos/40748696@N07/17117194340 is licensed under CC BY-ND 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/2.0	7
1.4	Rose’s law [3]. “Scaling Quantum Computing: 17 Years of Rose’s Law ” by Steve Jurvetson https://www.flickr.com/photos/jurvetson/50399541811 is licensed under CC BY 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by/2.0	8
1.5	Examples of major investments on Quantum Computing research programmes [4].	9
1.6	Schematic diagram of a QN.	10
1.7	Quantum communication between a GS and a Satellite. A quantum channel and a classical channel are necessary.	13
2.1	A qubit is typically represented using the BS.	25
2.2	Typical entanglement generation system.	28
2.3	Representation of an X gate.	31
2.4	Representation of an Y gate.	31
2.5	Representation of a Z gate.	32
2.6	Representation of an Hadamard gate.	32
2.7	Representation of a CNOT gate.	33
2.8	A circuit that swaps two qubits in a Quantum Computer.	34
2.9	A quantum circuit that produces a GHZ state.	35
2.10	A quantum circuit that produces a W state.	36

2.11 Quantum teleportation circuit.	38
2.12 When the sender and receiver share a Bell state, two classical bits can be packed into one qubit. The lines carry qubits, while the doubled lines carry classic bits. The variables b0 and b1 are classic boolean, while $ 0\rangle$ represents a pure quantum state.	39
2.13 The iconic textbook example of a Wigner function, which can be used to study the decoherence phenomena measuring its purity. The oscillations between the two states indicate the quantum coherence between them [5] [6].“The iconic textbook example of a Wigner function” by Rundle, R. P. et al. https://journals.aps.org/prapdf/10.1103/PhysRevA.96.022117 is licensed under CC BY 3.0. To view a copy of this license, visit https://creativecommons.org/licenses/by/3.0	43
2.14 The different influence of the environment on the system in the classical and quantum cases, illustrated for the case of a macroscopic body that interacts with light incident from all directions. In the classical case, which is represented on the left, light scattering off the body will not change the motion of the body, even though the environment interacts strongly with the system. On the contrary, in the quantum case, the interaction leads to an entangled object-photon state [7].	44
2.15 Representation of the Relaxation and Dephasing processes of a qubit.	45
2.16 Electric and magnetic field configurations of the Penning trap.	47
2.17 Schematic representation of a Josephson junction.	48
2.18 Superconducting qubit circuit realized with a Josephson junction.	48
2.19 A systems view of a quantum information processor. It consists of a physical and logical layer [8].	50

2.20	A detail of a dilution refrigerator. Gold-colored coaxial cables are used to send input and output signals from inside the cooler. “Inside an IBM Dilution Refrigerator” by IBM Research https://www.flickr.com/photos/ibm_research_zurich/26093909563 is licensed under CC BY-ND 2.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-nd/2.0	51
2.21	Diagram representing the operating principle of a dilution refrigerator.	52
2.22	Diagram representing the outline apparatuses needed to create a QD.	53
2.23	Representation of a matter-flying transducer. It converts matter qubits into flying qubits and vice versa.	54
3.1	A numerical example of RSA algorithm.	56
3.2	Schematic version of a BB84 protocol implementation, using Pockels cells and a birefringent calcite prism to separate the polarized beam. “Fichier:Bb84-french.svg” https://fr.wikipedia.org/wiki/Fichier:Bb84-french.svg is licensed under CC BY-SA 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-sa/4.0/deed.en . The picture has been modified within the terms of the license translating the names of the components from French to English.	60
3.3	Vertical polarization.	60
3.4	Diagonal polarization.	61
3.5	Specific polarizing filters are used to generate the desired polarization [9] [10].	61
3.6	Diagram that summarizes the phases of the BB84 protocol.	62
3.7	Quantum teleportation circuit.	64
3.8	Logical scheme of the distributed quantum computing ecosystem described in [11].	74
3.9	Schematic representation of the network proposed in [12]. The satellites employ network-wide entangled states to interrogate their Local Oscillators (LOs) and they send the information to a specific central node. In this manner, it is possible to obtain an extremely accurate clock signal available to all.	76
3.10	Schematic representation of a QPS.	79

3.11	Interference measurement between two telescopes using an entangled state emitted from a central Entangled Photon Source (EPS).	80
3.12	Conceptual description of an entanglement-based monostatic standoff Quantum Radar [13].	82
4.1	A representation of a QN. Two quantum computers are interconnected through a QR. Each device is equipped with a classical and a quantum interface.	89
4.2	A representation of the protocol stack defined in [14].	90
4.3	Comparison of geostationary Earth orbit with GPS, GLONASS, Galileo and Compass (MEO) satellite navigation system orbits with the International Space Station, Hubble Space Telescope and Iridium constellation orbits, and the nominal size of the Earth. “File:Comparison satellite navigation orbits.svg” by cmglee https://commons.wikimedia.org/w/index.php?curid=16891766 is licensed under CC BY-SA 3.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-sa/3.0/	93
4.4	High-altitude airship used as HAPs carrier.	95
4.5	At-source strategy. The entangled photon source is integrated into the devices.	97
4.6	At-midpoint strategy. A specific device generates pairs of entangled particles and delivers them to devices that will perform teleportation.	97
4.7	At-both-endpoints strategy. A third device performs the measurement of the particles, and entanglement is generated between the involved devices	98
4.8	Entanglement swapping.	99
4.9	The E2E entanglement generation procedure starts with the entanglement generation through transmitting photons between adjacent repeater nodes. Afterward, the entanglement swapping is applied recursively until the E2E entanglement is generated.	100
4.10	In 4.10a each satellite is entangled photon pair source, whereas in 4.10b entanglement sources and QRs are placed on board of satellites [15] [16].	101

4.11	An 8-beam free-space optics laser link. The receptor is the large lens in the middle, the transmitters the smaller ones. At the top right corner is a monocular for assisting the alignment of the two heads. “File:FSO-gigabit-laser-link-0a.jpg” by Adamantios https://commons.wikimedia.org/w/index.php?curid=4792467 is licensed under CC BY-SA 3.0. To view a copy of this license, visit https://creativecommons.org/licenses/by-sa/3.0/	103
4.12	Typical representation of an SDN-based architecture.	107
4.13	In 4.13a is represented the traditional networking paradigm, whereas 4.13b represents the SDN networking paradigm [17].	108
4.14	Hierarchical SDN architecture.	111
4.15	Distributed SDN architecture.	111
4.16	Schematic diagram of an OpenFlow Switch.	112
4.17	Schematic diagram of an SDN-based QN. This network can support multiple quantum applications.	114
5.1	Typical example of a TLE. The data represented in this figure concern the motion of the ISS.	118
5.2	The plane of the horizon for the observer on the surface of Earth [18]. For an observer placed at the center of the coordinate system represented in green, it is not possible to see objects that set relative to its plane of the horizon (represented by the green square).	121
5.3	Diagram representing relevant tools for obtaining satellite trajectory data [19].	122
5.4	A possible connection between two GSs via multiple FSO satellite links.	123
5.5	Quantum Software-Defined Internetworking architecture [20] ©2020 IEEE.	126
5.6	Operating principle of QSRs. Entanglement swapping is performed between two pairs of particles executing a BSM on two of them.	129
5.7	Scheme of a quantum communication based on teleportation. A particle with quantum state $ \psi\rangle$ is teleported sending two bits on the classical channel [20] ©2020 IEEE.	129

5.8	Ants follow a specific path. If an obstacle is interposed, ants can choose to go around it following one of the two different paths with equal probability. On the shorter path more pheromone is laid down.	134
5.9	Artistic representation of an optical ISL.	138
5.10	Entanglement rate for different L2L inter-distances [20] ©2020 IEEE.	139
5.11	E2E path Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.	140
5.12	Maximum single link length Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.	141
5.13	Number of hops Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.	142
5.14	Entanglement rate Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.	143
5.15	Entanglement rate as the distance between GSs varies for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.	144
5.16	An example of Cubesats.	145
5.17	Orbits of the 24 satellites that compose the GPS constellation.	146
5.18	Orbits of the 24 satellites that compose the Iridium NEXT constellation.	147
5.19	Orbits of the 179 CubeSats launched by various space agencies.	148
5.20	E2E entanglement rate considering different distances between GSs [21] ©2021 IEEE.	149
5.21	Links of Maximum link length within an optimised E2E path as a function of the distance between the GSs for different satellite constellations [21] ©2021 IEEE.	150
5.22	PDF of the entanglement rate achievable by the different satellite constellations [21] ©2021 IEEE.	151
5.23	PDF of the path duration achievable on Iridium-NEXT [21] ©2021 IEEE.	152
5.24	Performance of the static best path in terms of entanglement rate [21] ©2021 IEEE.	152

5.25	QSDN backbone architecture. A Bell pair is generated between GSs through operations driven by the Controllers embedded in the LEO constellation.	153
5.26	Packet format used by the protocol designed for the proposed architecture [22].	156
5.27	Sequence diagram of the first phase of the protocol. The MCS performs the setup operations on the selected path [22].	158
5.28	Sequence diagram related to the second phase of the protocol. The Controllers placed on the path manage the entanglement generation and swapping operations [22].	159
5.29	Time required to establish an entanglement E2E [22].	161
5.30	QSDN backbone architecture. A Bell pair is generated between GSs through operations driven by the Controllers embedded in the LEO constellation [23] ©2022 IEEE.	164
5.31	In 5.31a is represented how the <i>at source</i> strategy works, whereas in 5.31b is depicted an example of the <i>at mid-point</i> strategy.	166
5.32	Packets exchanged for a single session using both strategies [23] ©2022 IEEE.	167
5.33	Time required to establish an entanglement E2E [23] ©2022 IEEE.	168
5.34	Packets exchanged during a single session using a single Controller on the ground and the multi Controller architecture [23] ©2022 IEEE.	169
5.35	Time required to establish an entanglement E2E [23] ©2022 IEEE.	170
6.1	Scheme of the quantum computing demonstrator housed in two 19-inch racks [24]. By Pogorelov, I. <i>et al.</i> https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.2.020343 is licensed under CC BY 4.0. To view a copy of this license, visit https://creativecommons.org/licenses/by/4.0	172
6.2	A quadcopter can be stationed for a relatively long time in a fixed position [25] [26]. In this manner, it is straightforward to interconnect and maintain them as equidistant as possible in an optimal position, facilitating quantum communication.	174

- 6.3 Timeline of the discrete event simulation engine of NetSquid. "Abstract example of simulating a quantum protocol with discrete events" by Tim Coopmans *et al.* <https://www.nature.com/articles/s42005-021-00647-8/figures/2> is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>. 176
- 6.4 NetSquid's software architecture. "Overview of NetSquid's software architecture" by Tim Coopmans *et al.* <https://www.nature.com/articles/s42005-021-00647-8/figures/10> is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>. . . 177
- 6.5 Modelling and simulation process adopted in NetSquid. "Illustrative example of a NetSquid use case" by Tim Coopmans *et al.* <https://www.nature.com/articles/s42005-021-00647-8/figures/1> is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>. 178
- 6.6 Operating principle of a drone acting as QR. Entanglement swapping is performed between two pairs of particles executing a Bell state measurement on two of them [27] ©2022 IEEE. 181
- 6.7 Oscillations that typically affect a flying object. "DJI Tello Micro-Drone" by Dennis Sylvester Hurd <https://www.flickr.com/photos/dennissylvesterhurd/49238096152> is licensed under CC BY 2.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/2.0>. The picture has been modified within the terms of the license by inserting the coordinate system [27] ©2022 IEEE. 182
- 6.8 Representation of an IMU. "Apollo Guidance, Navigation, and Control (GNC) Hardware Overview" by NASA <https://ntrs.nasa.gov/api/citations/20090016290/downloads/20090016290.pdf>. 183
- 6.9 Scheme of the modules that compose a typical drone [28]. . . 184
- 6.10 Representation of beam wandering due to atmospheric turbulence [27] ©2022 IEEE. 184

6.11	Quantum metropolitan SDN drone network. In the first phase, the mission is configured properly by calculating the coordinates of the drones according to the result of the optimization. During the second phase, the Bell pairs are generated between the GSs through operations driven by the Controller embedded in the swarm of drones [27] ©2022 IEEE.	186
6.12	Entanglement generation and swapping protocol performed by the SDN Controller. Note that the swapping operation on the drone with the Controller embedded does not require the transmission of messages [27] ©2022 IEEE.	188
6.13	Attenuation for different wavelengths at varying meteorological conditions considering the Kruse model [27] ©2022 IEEE.	192
6.14	Fidelity for different wavelengths considering a visibility of 30 km [27] ©2022 IEEE.	193
6.15	Fidelity at varying meteorological conditions at 1550 nm w.r.t. OFs [27] ©2022 IEEE.	194
6.16	Fidelity at varying the distance between the GSs at 1550 nm considering visibility of 50 km [27] ©2022 IEEE.	195
6.17	Entanglement rate at varying the number of QDs on a 10 km path. The red plot highlights the rate obtainable with fidelity greater than 0.5 with a visibility of 10 km [27] ©2022 IEEE.	196
6.18	Overhead concerning the operations of entanglement generation and entanglement swapping for a single session [27] ©2022 IEEE.	197

List of Tables

2.1	Truth table of a CNOT gate.	33
4.1	Comparison of features of SDN with respect to classical networks.	110
5.1	TLE Line 1 fields.	119
5.2	TLE Line 2 fields.	119
5.3	Values of the parameters adopted in the simulations [20] ©2020 IEEE.	138
5.4	Average and standard deviation of the evaluated parameters for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.	141
6.1	Values of the parameters adopted in the simulations [27] ©2022 IEEE.	191
6.2	Attenuation values for the wavelengths employed in the simulations reported in Fig. 6.14 [27] ©2022 IEEE.	192
6.3	Parameters concerning the attenuation w.r.t. different atmospheric conditions considered in the simulations reported in Fig. 6.15 [27] ©2022 IEEE.	194

List of Algorithms

1	Modified Random Walk	133
2	Ant Colony Optimization	136
3	Dijkstra	137

List of Equations

1.1	Cost of the best classical algorithm known w.r.t Cost of a quantum algorithm	7
1.2	Classical complexity w.r.t Quantum complexity	7
2.1	Schrödinger's equation	22
2.2	Possible result of a measurement	23
2.3	State of the system after the operation of measurement . . .	23
2.4	Classical probability	23
2.5	Completeness relation	23
2.6	Vector for state 0	24
2.7	Vector for state 1	24
2.8	Linear combinations of the possible states	24
2.9	Wave function	24
2.10	Complete wave function expressed in polar coordinates	24
2.11	Final complete wave function	25
2.12	Density operator	26
2.13	Alternative basis states	26
2.14	Alternative basis states	26
2.15	Wave function considering the alternative basis states	26
2.16	Bell pair type 1	27
2.17	Bell pair type 2	27
2.18	Bell pair type 3	27
2.19	Bell pair type 4	27
2.20	No-Cloning Theorem Demonstration Passage 1	29
2.21	No-Cloning Theorem Demonstration Passage 2	29
2.22	No-Cloning Theorem Demonstration Passage 3	29
2.23	No-Cloning Theorem Demonstration Passage 4	29
2.24	Pauli's matrix identity	30
2.25	Pauli's matrix X	30

2.26	Pauli's matrix Y	30
2.27	Pauli's matrix Z	30
2.28	Pauli's matrix Hadamard	30
2.29	Square of a Pauli matrix	30
2.30	Transformation X gate 1	31
2.31	Transformation X gate 2	31
2.32	Transformation Y gate 1	31
2.33	Transformation Y gate 2	31
2.34	Transformation Z gate 1	32
2.35	Transformation Z gate 2	32
2.36	Transformation Hadamard gate 1	32
2.37	Transformation Hadamard gate 2	32
2.38	The operation of a swap circuit	34
2.39	GHZ state definition	35
2.40	Generalized GHZ state	35
2.41	W state definition	36
2.42	Generalized W state	36
2.43	Input state of teleportation circuit	37
2.44	Results of CNOT operation in a teleportation circuit	38
2.45	Results of Hadamard operation in a teleportation circuit	38
2.46	Simplified results of Hadamard operation in a teleportation circuit	38
2.47	First qubit result in a teleportation circuit	39
2.48	Second qubit result in a teleportation circuit	39
2.49	Third qubit result in a teleportation circuit	39
2.50	Fourth qubit result in a teleportation circuit	39
2.51	Input state of superdense coding circuit	40
2.52	State after encoding in a superdense coding circuit	40
2.53	Trace distance definition	41
2.54	Trace distance inequality	41
2.55	Fidelity definition	41
2.56	Fidelity inequality	41
2.57	Fidelity and trace distance relation	42
2.58	Fidelity and trace distance relation for pure states	42
2.59	Density operator 1	42
2.60	Density operator 2	43
2.61	Density matrix	43

2.62	Decoherence time relation	44
2.63	Density matrix with relaxation and dephasing	46
3.1	Parity check on BB84 first set	63
3.2	Parity check on BB84 second set	63
3.3	Azimuthal angle (0) in the E91 protocol	65
3.4	Azimuthal angle ($\frac{1}{4}\pi$) in the E91 protocol	65
3.5	Azimuthal angle ($\frac{1}{2}\pi$) in the E91 protocol	65
3.6	Azimuthal angle ($\frac{3}{4}\pi$) in the E91 protocol	65
3.7	Azimuthal angle ($\frac{1}{2}\pi$) in the E91 protocol	65
3.8	Azimuthal angle ($\frac{3}{4}\pi$) in the E91 protocol	65
3.9	Correlation coefficient of the measurements performed by Alice and Bob in the E91 protocol	65
3.10	According to the quantum rules	65
3.11	Uncorrelated results obtained for the two pairs of analyzers of the same orientation	66
3.12	CHSH inequality and correlation coefficients	66
3.13	Required result for the CHSH inequality	66
3.14	Intervention of an eavesdropper on the CHSH inequality	67
3.15	Quantum Bit Error Rate definition	67
4.1	Probability of success in generating entanglement between two adjacent nodes	92
5.1	Entanglement generation probability	130
5.2	Link entanglement generation probability	130
5.3	Attenuation of optical wave amplitude	130
5.4	Attenuation length	130
5.5	Average time required to generate a remote entanglement between two adjacent nodes	131
5.6	Average time required to generate a remote entanglement on the route	131
5.7	Entanglement rate	131
5.8	MRW condition	133
5.9	Trail intensity update condition	135
5.10	Pheromone equation	135
5.11	Probability of going to the j -th node	135
6.1	Misalignment error on X	185
6.2	Misalignment error on Y	185
6.3	Specific optical attenuation	187

6.4	Extinction coefficient	187
6.5	η coefficient	187
6.6	Fidelity between a pure state $ \psi\rangle$ and an arbitrary state ρ . .	189
6.11	Objective function	190

Part I

Concepts and Applications

Chapter 1

Introduction

This Chapter provides an overview of the history of quantum technologies, starting from the origins of quantum mechanics to the realization of the first devices. Furthermore, it provides an overview of the market and the problems related to the realization of QDs. The problem formulation of this thesis is also explained in this Chapter, which deals with the issues related to the implementation of Non-Terrestrial QN architectures.

1.1 History of Quantum Technologies

Quantum Mechanics has had a significant development during the early years of the last century, moving from Quantum Theory to Quantum Mechanics, through the contributions of many distinguished scientists such as Schrödinger, Heisenberg, Bohr, Dirac, Pauli, Plank, De Broglie, Einstein and David Hilbert, many of them Nobel Prize winners. The natural field of application of Quantum Mechanics is within Physics. Nevertheless, in the last 40 years (starting from the 1980s) it has exceptionally expanded into the area of Information science and technologies. The main ideas come from the Postulates of Quantum Mechanics, which in the last 100 years have never been disproved, and, after a substantial reformulation, envisage extremely innovative applications, like the quantum computing, quantum coding, quantum cryptography, and quantum communications. Many of these innovations, which are consequences of the Postulates, have already had experimental verification and are the subject of an intensive research activity. As a matter of fact, the Nobel Prize in Physics 2022 was awarded jointly to Alain

Aspect, John F. Clauser and Anton Zeilinger for experiments with entangled photons, establishing the violation of Bell inequalities and pioneering quantum information science [29].

To understand the motivations that, in the early 1980s, led to studying information in the context of Quantum Mechanics, we can start from Moore's Law of electronic circuit technology. As we know, this law, stated by Gordon Moore in 1965, asserts that the complexity of electronic microchips, at equal size, doubles approximately every 18 months, and this prediction has been substantially confirmed in the last 50 years. However, it assumes an indefinite reduction in the size of components, down to the limit of atomic dimensions, where quantum effects become predominant.

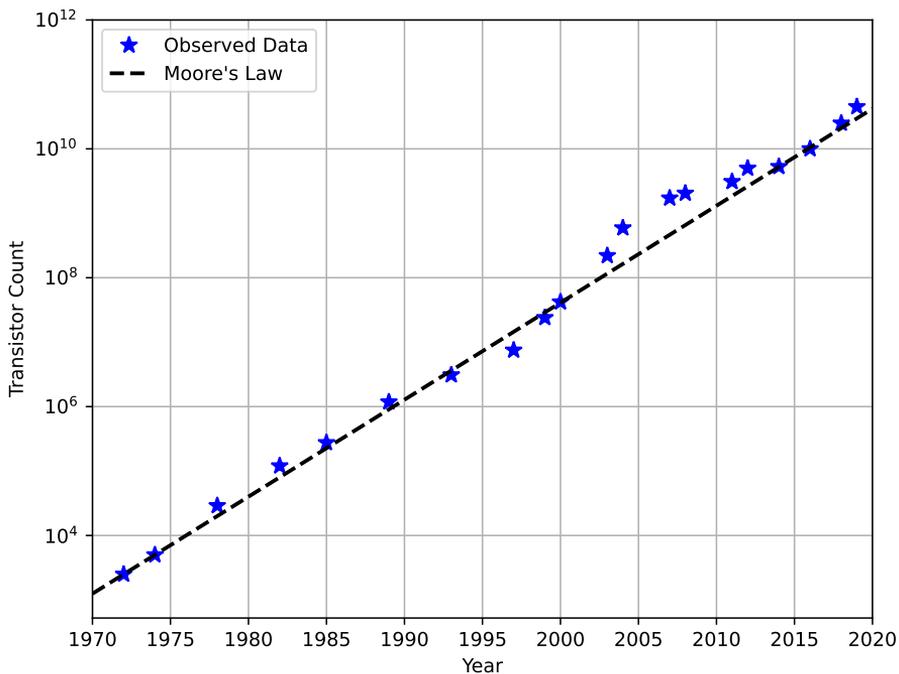


Figure 1.1: Moore's law [1].

At this point, a natural development is to try to reformulate Information Theory in the framework of Quantum Mechanics. Information Theory based on quantum principles extends and completes classical Information Theory. Specifically, the Quantum Information Theory includes quantum generaliza-

tions of classical concepts such as channels, sources, and codes, as well as two complementary, quantifiable kinds of information, which are classical information and quantum entanglement [30] [31]. Following this line of thought, Benioff, Manin, and Feynman postulated the idea of a QC, for the simulation of Quantum Systems. Subsequently, in 1985 David Deutsch proved that a QC can naturally operate in parallel mode (quantum parallelism), in the sense that it makes it possible to evaluate any function, for every value, in a single step. With this parallelism, the theoretical superiority of the QC with respect to the conventional one was demonstrated [32]. Meanwhile, Charles Bennett and Gilles Brassard explored the possibility of secure information transmission based on the laws of Quantum Mechanics [2]. The principle is related to quantum measurements derived from the Postulate 3 of Quantum Mechanics according to which, if the information is intercepted, the receiver is automatically and securely alerted. This marks the birth of Quantum Cryptography. On the other hand, in 1991 Arthur Ekert proposes another form of secure transmission based on entanglement, a phenomenon predicted by Postulate 4 of Quantum Mechanics. In any case, Quantum Cryptography, as a QKD, is one of the most concrete applications of Quantum Mechanics in the information area, and significant results have already been achieved in this area. The most prominent quantum cryptography technique is the QKD, which includes several protocols that can be divided in Discrete-Variable QKD (DVQKD) protocols [33] and Continuous-Variable QKD (CVQKD) protocols [34] [35]. Basically, the main distinction between DVQKD and CVQKD protocols consists in the detection technique that is employed [35]. The phenomenon of entanglement, typical of quantum mechanics, and totally unforeseen by the classical theory, gave origin to another research thread: superdense coding, according to which, by sending a single bit of quantum information (qubit), two bits of classical information can be transmitted [36] [37] [38]. This originated a very promising new field, Quantum Coding, steadily growing, as witnessed by the numerous papers published in various scientific journals in recent years. It should be noticed that, in this context, Shannon's Information Theory is being reviewed, giving way to Quantum Information Theory [39]. The superdense coding, a quantum communication protocol to communicate a number of classical bits of information by transmitting several qubits [36], was invented by Bennett and Wiesner [40] and experimentally implemented by Mattle, as reported in [41]. Bennett et al. [42] found another use of entanglement, quantum tele-

portation, in which separate experiments sharing two halves of entangled systems can make use of entanglement to transfer a quantum state from one to another using only classical communications. Teleportation was later experimentally realized using optical techniques and photon polarization. Furthermore, it is important to remind the milestone achieved by Peter Shor of AT&T in 1994, who demonstrated that a QC can decompose an integer number into prime factors with polynomial complexity, whereas it is conjectured that the classic computer requires exponential complexity [43] [44]. This discovery was alarming, considering that the majority of current cryptographic security systems are based on the exponential difficulty of prime factor decomposition.

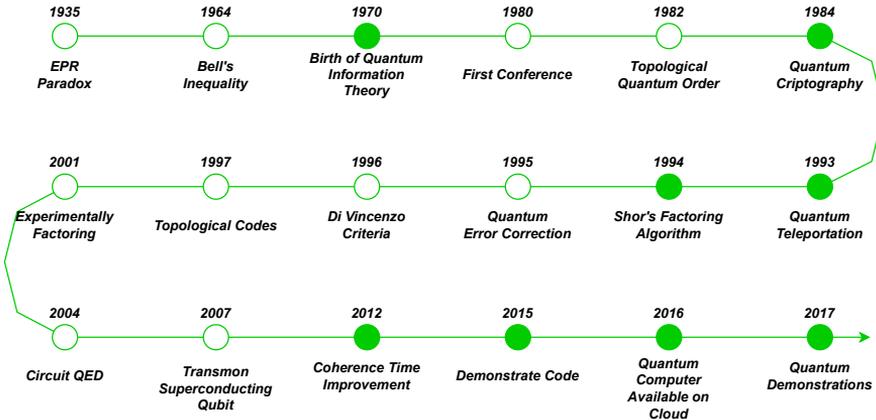


Figure 1.2: History of Quantum Information [2].

Currently, the aim of the leading developers of QCs is to achieve *Quantum Supremacy*. The Quantum Supremacy or quantum advantage is achieved when a controlled quantum system is able to perform tasks with performance that goes beyond an ordinary digital computer. Conceptually, Quantum Supremacy involves both the engineering task of building a powerful QC and the computational-complexity-theoretic task of finding a problem that can be solved by that QC and has a superpolynomial speedup over the best known or possible classical algorithm for that task [45] [46].

$$S_1 = \frac{\text{Cost of the best classical algorithm known}}{\text{Cost of a quantum algorithm}} \quad (1.1)$$

The cost of an algorithm is the amount of resources it uses, such as the number of arithmetic operations or elementary quantum operations.

$$S_2 = \frac{\textit{Classical complexity}}{\textit{Quantum complexity}} \quad (1.2)$$

The second criterion uses the concept of computational complexity, which is the minimal cost of solving a problem [46].

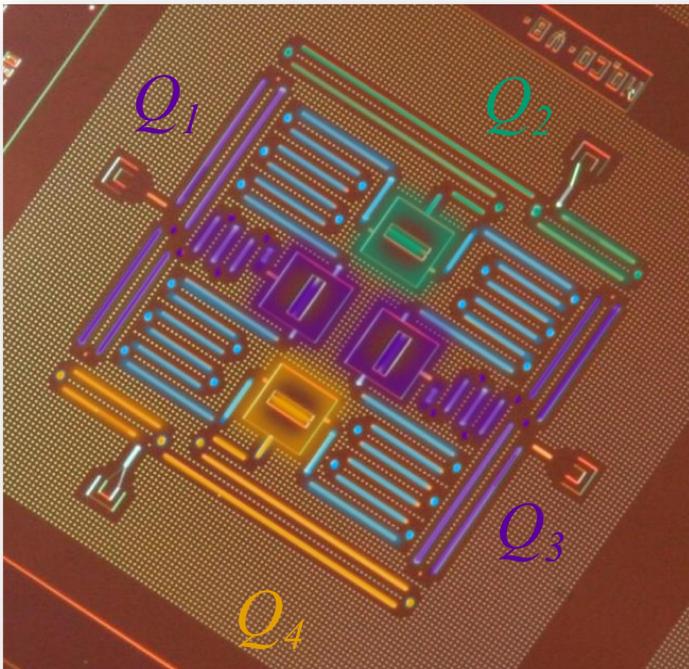


Figure 1.3: Layout of IBM's four superconducting quantum bit device (false-colored). "IBM Four Qubit Square Circuit (false-colored)" by IBM Research <https://www.flickr.com/photos/40748696@N07/17117194340> is licensed under CC BY-ND 2.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nd/2.0>.

Recently, the number of qubits that QCs are equipped with has increased significantly, and the law governing this trend is Rose’s law, which is depicted in Fig. 1.4. This law suggests quantum computing qubits should double every two years and is close to or already moving faster than Moore’s Law [3] [47].

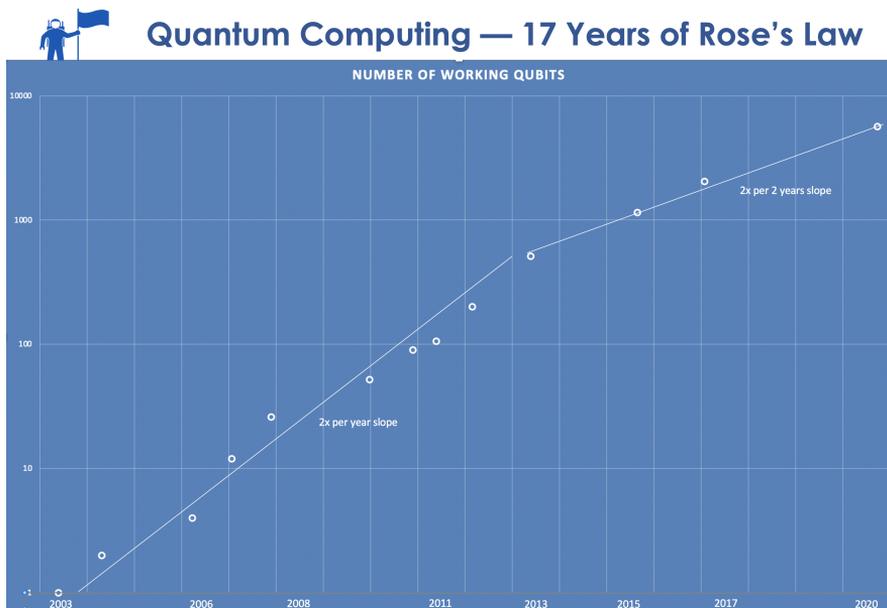


Figure 1.4: Rose’s law [3]. “Scaling Quantum Computing: 17 Years of Rose’s Law ” by Steve Jurvetson <https://www.flickr.com/photos/jurvetson/50399541811> is licensed under CC BY 2.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/2.0>.

1.2 Quantum Technologies Market

The alarming discoveries regarding the capabilities of QCs to decrypt current systems confirm the importance of investing in ideas and resources on Quantum Cryptography. Although the market is at an early stage of development, there have been encouraging signs of growth through a wide range of start-ups providing consultancy, software and devices of various kinds [4].

The United States has long been the world’s leader in attracting investments. As a matter of fact, in [48] is reported that the region also dominates private quantum investment. However, the North American quantum indus-



Figure 1.5: Examples of major investments on Quantum Computing research programmes [4].

try is not restricted to Silicon Valley. Specifically, in Canada a whole ecosystem has emerged to support quantum companies around academic hubs in Waterloo and Toronto, which have benefited from public and philanthropic investment, tax advantages and successful incubators. Nevertheless, more than 43% of quantum-technology innovations patented between 2012 and 2017 came from Chinese firms and universities. On the other hand, European investors are typically more risk-averse and have smaller budgets, but a €1-billion (US\$1.1-billion) flagship, launched by the European Union in 2018, aims to ensure that the region's strengths in basic research translate to commercial success.

1.3 Technological Principles

Even though the phenomena underlying quantum mechanics had been known for years and some applications were already known, it was only in recent years that the engineering stage was reached and real devices were made. Meanwhile, there has been a significant development of classic devices and networks. Furthermore, the exponential growth in the number of devices and the demand for new services require the development of new telecommunications networks [49] and specific devices. In particular, in order to satisfy

the needs of all users of these services who are continuously increasing, Non-Terrestrial Networks (NTNs), which include satellite networks and different kinds of aerial platforms, provide the best solution, also considering that they allow connecting areas of the planet that are underserved and where it is difficult to deploy a terrestrial infrastructure, thus complementing, e.g., the future terrestrial fifth-generation (5G) and sixth generation (6G) networks [50] [51]. For instance, a constellation of satellites deployed in LEO can be able to provide low-latency and high-bitrate [52], which are significant requisites to enable the services offered by 5G and 6G networks [53]. Therefore, the main objective is to combine non-terrestrial and terrestrial 5G/6G links in order to ensure the right Quality of Service (QoS) to meet users' requirements [54]. The classical roles of satellites to assure high-speed backhaul connectivity for content distribution (video or HD/UHD TV) and to provide anywhere global Internet of Things (IoT) connectivity, especially for mission-critical and emergency situations are increasingly current. In fact, many companies are planning emergency features on their future smartphones that will rely on satellite networks, allowing users to send messages to first rescuers in areas without cellular coverage [55]. Furthermore, several trends such as the increasing of demand, supply, and traffic are pushing network providers and users to reassess traditional approaches to network architectures. One of the most promising solutions is SDN, which is a paradigm where a central software program, called Controller, determines the overall

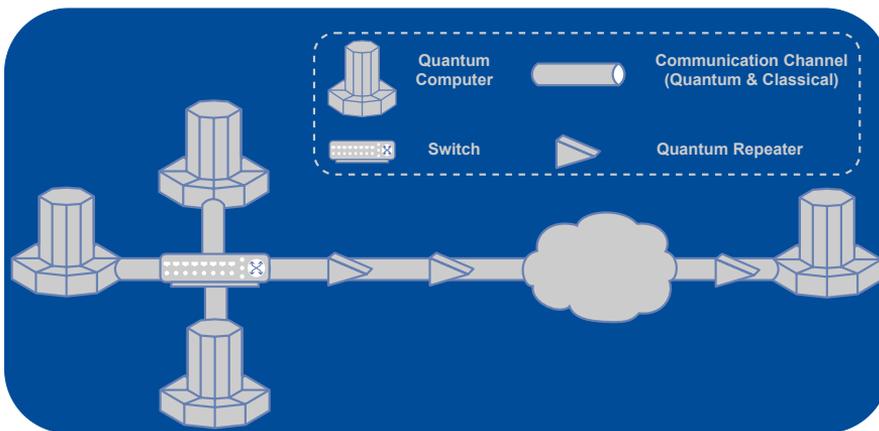


Figure 1.6: Schematic diagram of a QN.

network behavior. As a matter of fact, the Controller is a portable software that can run on commodity servers and is capable of programming the forwarding devices based on a centralized view of the network. In SDN, the network devices that compose the Data Plane (DP) are simple packet forwarding devices, while the CP is implemented in a centralized Controller [56] or set of coordinated centralized Controllers.

Based on the previous considerations, it is plausible that the synergy between classical and quantum technologies may be essential for the development of future telecommunication networks beyond the 6G [57]. Naturally, the readaptation of classic technologies is needed, but some of them such as SDN technology are considered fundamental in QNs.

Differently from classical networks, QNs, are based on the quantum entanglement [58] and quantum teleportation [59] phenomena [60] [61], and the devices that compose the QN and are based on these phenomena can be easily managed through the use of SDN technology.

In order to perform a quantum communication, two different channels are used, a classical channel and a quantum channel [62] [63], with specific purposes:

- Quantum channel: a link which can be used to generate an entangled pair between two directly connected quantum repeaters.
- Classical channel: a link between any node in the network that is capable of carrying classical network traffic. This includes background protocols such as path selection as well as signalling protocols to set up E2E entanglement generation. Furthermore, it is used to communicate classical bits of information as part of entanglement swapping and teleportation.

The channels are depicted in Fig. 1.7, which represents a typical satellite scenario. Considering the difficulties encountered in the creation of robust and efficient path selection and management protocols, the SDN technology has been considered crucial. For this reason, it has already been used in the QKD case, thus originating the so-called Quantum SDN (QSDN) [64] [65]. In particular, the CP is dedicated to the management of the devices that compose the DP, which are able to create Bell pairs between each other. Then, in the case of QSDN, the DP traffic is a flow of entangled particles sent through the quantum channel, whereas the CP traffic is composed of both the classical information needed for the teleportation process and the background

protocol traffic that is related to path selection and entanglement generation management procedures [21] [14] [20]. As a matter of fact, obtaining the entanglement between two remote devices is still very difficult considering OF links [66]. Therefore, devices called Quantum Repeaters (QRs) are used in order to extend the range of entanglement between two devices through a specific protocol that requires several steps [67]. The protocol consists in implementing recursively the *entanglement swapping* operation [21] [68] on some devices in the path, i.e. in performing measurements of the Bell states on selected nodes following a specific sequence [69], which could be properly managed by an SDN Controller. Specifically, the QRs divide the entire communication channel into multiple segments, making it possible to create pairs of entangled particles between adjacent nodes by transmitting photons entangled with their Quantum Memory (QM) [70] [22]. In fact, if the transmitted modes are entangled and light is absorbed by the set of atoms of which the memory is composed, the quantum correlations can be mapped on the collective superposition of the two final states of the atoms [71] [72]. Differently from classic repeaters, QRs can not clone quantum signals considering that their operating principle is based on uncertainty principle and the *no-cloning* theorem [73], that are the physical laws making quantum communications absolutely secure [74] [75] [76] [77].

However, considering the difficulties encountered in the conservation of Bell states due to the interaction of particles with matter that induce *decoherence*, i.e., the loss of coupling in time, it is necessary to consider also other communication media [78]. In fact, it is worth noticing that this effect is deleterious both in the case of quantum computation and quantum communication, considering that it leads qubits to be entangled with the environment corrupting both processes [23]. Specifically, several parameters, e.g., temperature or magnetic fields, constitute an uncontrollable source of noise in the system, which affects the quality of the generated entangled state [79]. Specifically, the quantum decoherence disregards the observer and the measurement process, preceding it and simulating the collapse of the wave function [80]. The collapse produces the transition from a coherent state to an incoherent one, in which the off-diagonal terms of the density matrix are zero; the decoherence instead causes a spontaneous transition from a coherent state to a decoherent one, in which the off-diagonal terms of the density matrix are asymptotically infinitesimal [81]. The channel and decoherence issues are the motivations for taking into consideration the use

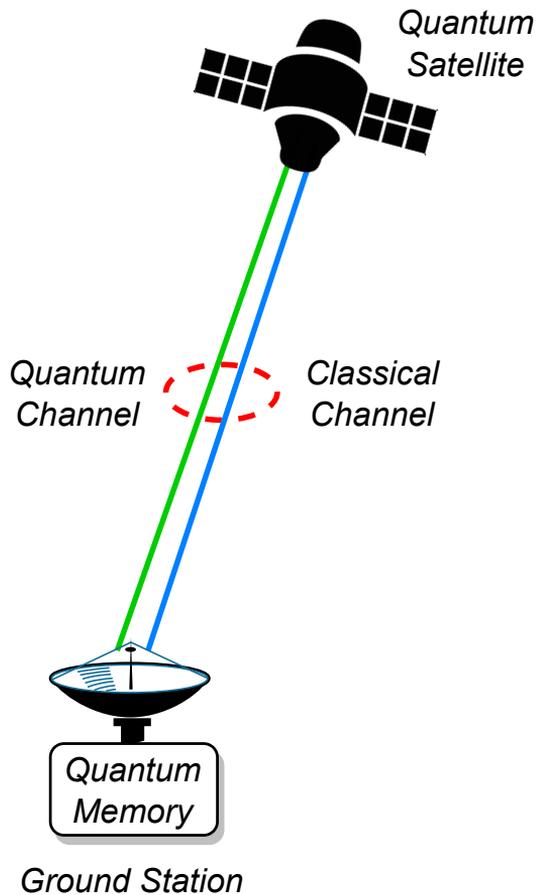


Figure 1.7: Quantum communication between a GS and a Satellite. A quantum channel and a classical channel are necessary.

of satellite and different aerial platforms such as drones [20] [21] [22] [82]. In particular, the use of satellite technology is a promising solution considering that allows to use the space vacuum as communication media as much as possible since it has better characteristics [83] [84].

Specifically, a communication through a quantum satellite backbone can be performed considering the use of two different links [85] [86]:

- Satellite-to-Satellite links: in this case, two satellites, which are in Line of Sight (LOS) can transmit entangled particles to each other.
- Ground-to-Satellite and Satellite-to-Ground links: the entangled particles are exchanged between a GSs and a satellite.

Despite the atmospheric link is very critical because it introduces diffraction losses, absorption, scattering, beam wander, beam spreading, and scintillation effects, in fair weather conditions the entanglement can be preserved [87] and these effects are negligible on the Satellite-to-Satellite links.

Moreover, in order to reduce the impact of channel losses, several quantum satellites with the function of QRs have to be deployed along the E2E path [20] and the performance can be further improved with the use of FSO technology [88] [89]. As a matter of fact, some models show that in good meteorological conditions, attenuation values even lower than those obtainable with OFs can be obtained [90] [91] [92]. This results in a significant reduction of losses, due to the scattering phenomenon and allows to reduce the number of required QRs. In fact, although the effects of the atmosphere cannot be neglected the deployment of QRs in orbit allows to realize a quantum communication covering significant distances [15]. Examples of atmospheric models are Kruse's model [90] and Kim's model [91], which allow calculating the specific optical attenuation according to the atmospheric visibility.

1.4 Proposed Architectures

As discussed in Section 1.3, the development of quantum satellite technology could potentially allow the creation of a global quantum communication network with the aim to connect any two points on the surface of Earth with reduced propagation losses as compared with OFs. Many experiments have already been conducted and consider the use of small-size and low-cost satellites, i.e., CubeSats [21] [93], using the FSO technology [94]. The availability of CubeSats and lower launch costs has led to rapid growth in satellite constellation programs and could be crucial also in the deployment of future QSNs [94]. These satellites are usually placed in LEO, allowing them to mitigate the problem of distance, which is a significant issue in quantum communications. However, the most important drawback is the high speed of the satellites, which being in LEO, rotate around Earth very quickly with speeds between 5 to 10 km/s [95] [96], making it difficult to

achieve very accurate pointing during signal transmission. Furthermore, the communication can only be performed during specific time windows due to the limited flyover time of the satellites [97].

Therefore, this thesis explores the possibility of realizing QSNs by taking advantage of the peculiarities offered by SDN technology that was initially developed in the classical domain. Specifically, an architecture with the SDN Controller deployed in a dedicated MCS is proposed. In particular, the performance of some path selection algorithms is analyzed, making a comparison between distributed and centralized solutions that are enabled by SDN technology. Moreover, considering that an efficient path selection algorithm is only part of the solution, the performance on various Medium Earth Orbit (MEO) and LEO constellations are studied.

In addition, considering that the integration of the CP into the constellation [98] itself has not yet been studied in the quantum case, the thesis proposes many architectures with multiple SDN Controllers deployed into the constellation. Furthermore, specific protocols with related performance analyses have been developed. Several approaches have been proposed in the literature for multi-Controller architectures that fall into two categories: hierarchical approaches and fully distributed approaches. In hierarchical solutions [99] [100], distributed Controllers operate on a partitioned network view, while decisions that require network-wide knowledge are taken by a logically centralized root Controller. In distributed approaches, Controllers operate on their local view, or they may exchange synchronization messages to enhance their knowledge. Distributed solutions are more suitable for supporting adaptive SDN applications [101].

Satellites can enable to cover large distances and allow the creation of global networks, however, in more limited contexts such as in metropolitan areas, swarms of drones are envisioned as a significant component, especially for the creation of new generation networks. As a matter of fact, the deployment of multiple drones allows delivering cellular and Internet services to remote regions or areas where a massive number of users are *temporarily* gathered or where terrestrial infrastructure is unavailable or difficult to deploy. Moreover, drones can be disposed above the desired area *on-demand* in order to assist the communication at any given time and according to the dynamic requirements [102].

As explained in [103], the Bell pairs, that are couples of maximally entangled photons, meaning that they have the strongest correlations of all

possible two-qubit states [79], can be generated onboard drones, that therefore act as QRs. However, besides the atmospheric phenomena, the quality of the FSO link can be severely impacted by the change of drones' position and orientation due to their random fluctuations [104]. Specifically, pointing errors and atmospheric turbulence contribute to increased losses [105]. These effects are known as *beam wandering* and can significantly deteriorate the communications performance [106]. Therefore, these losses depend on the fraction of power that falls onto the photo-detector. The drones are equipped with specific systems that could contribute to mitigating these effects [107], however, especially in a quantum communication these losses cannot be completely ignored. Given all the previous considerations, the swarm of drones can be taken into account to create efficient ad hoc MQDNs for specific critical missions. However, many of the studies conducted so far only consider simplified scenarios consisting of a limited number of drones [108,109]. Considering that the SDN is a suitable technology for the management of mobile QNs [20–23,64], this thesis explores an architecture based on SDN that can be used to manage and control a MQDNs adapting it to possible quantum applications. Specifically, in a MQDNs, the SDN Controller can set up the E2E drones' path by sending control messages on a specific classical control channel [79]. Through the SDN technology, it is possible to further mitigate pointing errors by compensating the trim changes due to atmospheric agents [110]. Moreover, the integration of the CP into the swarm allows the reduction of the overhead considering that many operations can be executed locally without sending specific messages through a channel.

The considered architectures could be used to implement the most significant applications, which fall in the area of distributed quantum computing, which allows creating *Quantum Cloud* with an unprecedented computational capacity [111] [11] [112], and quantum cryptography, which makes quantum communication extremely secure [113]. Some of the most significant QKD protocols have been partly implemented on scenarios consisting of drones [108], and studies on QKD have also been conducted in the satellite field [114]. However, many of the QKD protocols applied so far do not involve multiple drones, and only a few studies concern the implementation of entanglement-based protocols such as E91 [115] [92]. Indeed, despite some efforts have been dedicated to perform quantum communication through *couple* of drones, it is still unclear how the E2E paths between two Ground Stations (GSs) can be optimally configured.

The proposed architecture provides also accurate mission planning and control, allowing the reduction of the effects due to quantum *decoherence* [116]. Specifically, in a scenario consisting of drones, it is possible to adopt some expedient to limit the phenomenon. As explained in [66], by positioning the QRs equidistant, it is possible to mitigate the effect of decoherence, and, therefore, the drones that compose the swarm must be positioned as equidistant as possible. It is possible to plan the mission properly by optimizing specific objective functions, and SDN technology can contribute to controlling drones. Naturally, it is not feasible to arrange satellites following this logic, but from some of the experiments conducted in this thesis, it is possible to infer some design guidelines for the creation of future QSNs. Therefore, in this case, it will be necessary to invest also in high-quality hardware in order to compensate for the effects of the Ground-to-Satellite and Satellite-to-Ground links and the difficulty in performing maintenance.

1.5 Applications

The defined architectures and the results obtained in this thesis are a contribution towards the realization of the so-called QI, that compared to the classic Internet, has as its most significant feature security [117].

Nevertheless, security is not the only benefit that can be obtained from such a network. Some of the applications that can be identified are related to distributed computing that can enable advanced Cloud systems. In particular, considering k remote QDs, which dedicate at least one qubit for the teleportation, a virtual QD consisting of up to $kn - k$ qubits is obtained. The obtained computational capacity is extremely high and could allow the processing of a huge amount of data in a very short time. The ultimate goal is to interconnect clusters of QCs, i.e. different Quantum Data Centers (QDCs) that operate in a coordinated manner, an objective that can be achieved through the use of specific QSNs [118]. Some studies featured in this thesis also consider the use of SDN technology applied to QSNs and drones, which can be used to achieve the goal of interconnecting QDCs distributed on a global scale. This goal can be achieved with a Service-Oriented Architecture (SOA) [119], which is an approach that addresses the requirements of loosely coupled, standards-based, and protocol-independent distributed computing. In this kind of architectures, it is irrelevant whether services are local or remote, the interconnect scheme or protocol to effect the in-

vocation, or which infrastructure components are required to establish the connection [120] [121]. The integration of satellites and drones into current telecommunications networks following this paradigm is also one of the prerogatives of 5G and 6G [122] [123]. In some experiments that are illustrated in this thesis, the SDN technology has been used with the aim of managing the satellite network and the operations necessary to establish entanglement between two GSs [20] [21] [22]. Furthermore, a network of quantum satellites could be deployed around Earth in order to improve the current positioning systems considerably [12] [124]. As a matter of fact, the traditional Global Navigation Satellites Systems (GNSS) present an error in the range of 10 to 15 m , which may be unacceptable for many applications [125] [126] [127] as geodesy, gravitational wave observation, and synthetic aperture optical astronomy [128] [129]. However, many of these errors are related to clock synchronization and can be mitigated by the use of QSNs, allowing to achieve an unprecedented level of accuracy [127] [12]. Moreover, the quantum entanglement can be used in order to quadratically improve the sensitivity of measurements [130], QSNs can also be used in order to perform some studies in the field of quantum physics [12] [124]. These types of networks are also useful for applications such as interferometry, which makes use of the principle of superposition to combine waves in a way that will cause the result of their combination to have some meaningful property that is diagnostic of the original state of the waves [131]. However, phase fluctuations and photon loss introduced by the communication channel between the telescopes put a limitation on the baseline lengths of the optical interferometers. This limitation can be potentially avoided using quantum teleportation. In general, by sharing EPR-pairs using QRs, the optical interferometers can communicate photons over long distances, providing arbitrarily long baselines [132].

1.6 Thesis Contributions

This thesis brings together some studies conducted on quantum satellite backbones and the applications that they can enable. In particular, the issues explored in this thesis are the following:

- Basic concepts of quantum mechanics and technological principles.
- An in-depth analysis of state of the art and experiments conducted so far in the field of QNs addressing the following fields and applications:

- Quantum satellite networks.
 - Quantum satellite repeaters and backbones coordinated by the SDN technology.
 - Quantum distributed computing and Cloud.
 - Synchronization of atomic clocks and Quantum Positioning System (QPS).
 - Quantum sensing and interferometry.
 - Quantum drone networks.
- System models and the experiments conducted in this thesis concerning the following scenarios:
 - Introduction to possible scenarios of satellite QNs with related discussion.
 - Analysis of path selection algorithms and constellations on scenarios with a single SDN Controller on the ground and performance evaluation.
 - Analysis of several scenarios with multiple SDN Controllers integrated in the constellation and performance evaluation.
 - Drone networks with performance evaluation and comparison with OFs.
 - Conclusions and future developments.

1.7 Thesis Organization

This thesis is divided into two parts. Part I contains preliminary concepts and describes possible applications. Specifically, Part I is composed of three Chapters organized as follows: Chapter 1 first outlines the history of quantum information starting from the discovery of physical principles to the realization of the first devices. Furthermore, the Chapter includes a Section on the market in which the countries that invest the most in research are indicated. This Chapter also explains the main technical issues related to QNs by providing some basic principles. Finally, this Chapter describes the architectural principles, contributions of this thesis, and how it is organized.

Chapter 2 describes the physical and technological principles behind QNs in depth. The Chapter starts by describing the quantum information unit

and proceeds by describing the physical principles necessary for the realization of QNs and the technological solutions based on them. Specifically, the Chapter describes specific circuits for different purposes and explores adoptable technological solutions for the realization of a QM.

Chapter 3 illustrates many possible applications and the state of the art by referring to experiments conducted in various contexts. First of all, some basic principles and protocols of quantum cryptography are described. Specifically, the Chapter examines some feasibility studies of QKD in the area of QSNs. Furthermore, some studies related to the implementation of other specific applications are explored. In particular, the Chapter describes studies related to Quantum Cloud, positioning systems, and sensing realized through quantum technologies in synergy with SDN technology.

On the other hand, Part II describes the simulations and provides the analysis of the results. Specifically, Part II is composed of four Chapters organized as follows: Chapter 4 describes QNs by considering both the hardware elements required for their operation and the protocol stack. Although the protocol stack has still to be defined, there are some papers in the literature that attempt to define some guidelines for its realization. The Chapter also provides some elements of satellite networks and discusses the possibility of realizing QSNs based on SDN technology.

Chapter 5 describes the proposed architectures and experiments conducted in this thesis with related results. Initially, an overview of possible satellite constellations and functional solutions is provided. Moreover, this thesis describes the experiments performed by applying some distributed and centralized routing algorithms on a LEO satellite network and the experiments conducted considering different constellations. The Chapter also explores the proposed solutions that integrate the SDN Controller in the constellation with its results.

Chapter 6 presents an architecture studied for metropolitan contexts. This architecture is based on drones and integrates an SDN Controller into the swarm itself. Furthermore, some typical performance of QNs is evaluated, and an objective function is introduced to optimize the number of drones that compose the E2E path.

Finally, Chapter 7 summarizes the overall work presented in the previous Chapters and reports the conclusions and future developments.

Chapter 2

Physical and Technological Principles

This Chapter describes the physical and technological principles which are the basis of QNs. Specifically, Section 2.1 describes the physical principles necessary for the realization of QNs and the technological solutions starting from the basics. Furthermore, Section 2.2 describes many technological aspects from quantum gates to the realization of QMs.

2.1 Fundamentals of Quantum Information

This Section describes the most significant physical and technological aspects necessary to understand the operating principle of quantum communications, while the experiments that are described in the following Sections.

2.1.1 The Postulates of Quantum Mechanics

Quantum Mechanics is based on four assumptions which are called *postulates* [133]. The entire universe is ruled by these postulates and only a few effects constitutes an exception [134].

2.1.1.1 First Postulate

The actual state of any closed physical system can be described by means of a so-called state vector v having complex coefficients and unit length in a

Hilbert space V , i.e. a complex linear vector space (state space) equipped with an inner product.

The state of the system can be represented by means of a two-dimensional vector an orthonormal basis vectors of an Hilbert space. The coordinates of a quantum state vector are often referred as probability amplitudes because they play the role of amplitudes in Schrödinger wave functions describing the location of particles.

2.1.1.2 Second Postulate

The evolution of any closed physical system in time can be characterized by means of unitary transforms depending only on the starting and finishing time of the evolution.

The above definition describes the evolution between discrete time instants, which is more suitable in the context of quantum computing. Its original continuous-time form is known as the Schrödinger equation which is reported in the following [135] [136]:

$$H |\psi\rangle = i\hbar \frac{\partial |\psi\rangle}{\partial t} \quad (2.1)$$

where \hbar denotes the Planck's constant and $\frac{H}{\hbar}$ represents the so-called Hamiltonian, a Hermitian operator characterizing the evolution of the system. If the Hamiltonian of a system and the Planck's constant \hbar are known, it is possible to understand it is possible to understand the dynamics of the system completely, at least in principle [38] [137].

2.1.1.3 Third Postulate

Any quantum measurement can be described by means of a set of measurement operators M_m , where m stands for the possible results of the measurement.

If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is expressed as follows:

$$p(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle \quad (2.2)$$

After the operation of measurement, the state of the system is:

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \quad (2.3)$$

Considering that classical probability theory requires that:

$$\sum_n p(m) = \sum_n \langle\psi|M_m^\dagger M_m|\psi\rangle = 1 \quad (2.4)$$

the measurement operators have to satisfy the completeness relation:

$$\sum_n M_m^\dagger M_m = I \quad (2.5)$$

Considering that measurements are not reversible, they represent the only exception under the unitarity constraint. A significant example of a measurement is the measurement of a qubit in the *Computational Basis (CB)*.

2.1.1.4 Fourth Postulate

The state space of a composite physical system W can be determined using the tensor product of the individual systems $W = V \otimes Y$. Furthermore having defined $v \in V$ and $y \in Y$ then the joint state of the composite system is $w = v \otimes y$ [138].

2.1.2 Quantum Informative Unit

The elementary unit of measure used in classical computation and classical information is the bit, which is represented alternately, with the digits 0 and 1. The basic state of a two-dimensional quantum system is the quantum bit (qubit) [139]. Some of the possible states for a qubit are $|0\rangle$ and $|1\rangle$, which form an orthogonal basis for this vector space, known as the *computational basis*. The Computational Basis States (CBSs) correspond to the states 0 and 1 in which a classical bit can be found. The mathematical notation used to define these quantum states is called Dirac notation or Dirac formalism

and is the standard notation.

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (2.6)$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2.7)$$

The main difference between a classical bit and a qubit is that it can be in a state other than 0 or 1. In fact, it is possible to form linear combinations of the possible states, called superpositions:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2.8)$$

All pure states can be represented on the Bloch's Sphere (BS) depicted in Fig. 2.1 as a superposition of both CBS, resulting in a wave-function like the following:

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \quad (2.9)$$

The values α and β are complex numbers, hence the state of a qubit is a vector in a two-dimensional complex vector space. Differently to the classical case, in the quantum case is not possible to examine a qubit to determine its quantum state, that is, the values of α and β . When a qubit is measured we get either the result 0, with probability $|\alpha|^2$, or 1, with probability $|\beta|^2$ since $|\alpha|^2 + |\beta|^2 = 1$. Geometrically, we can interpret this as the condition that the qubit's state be normalized to length 1. Thus, in general a qubit's state is a unit vector in a two-dimensional complex vector space [38].

The complete wave function is:

$$\begin{aligned} |\psi\rangle &= e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right) = \\ &= e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + (\cos \phi + i \sin \phi) \sin \frac{\theta}{2} |1\rangle \right) \end{aligned} \quad (2.10)$$

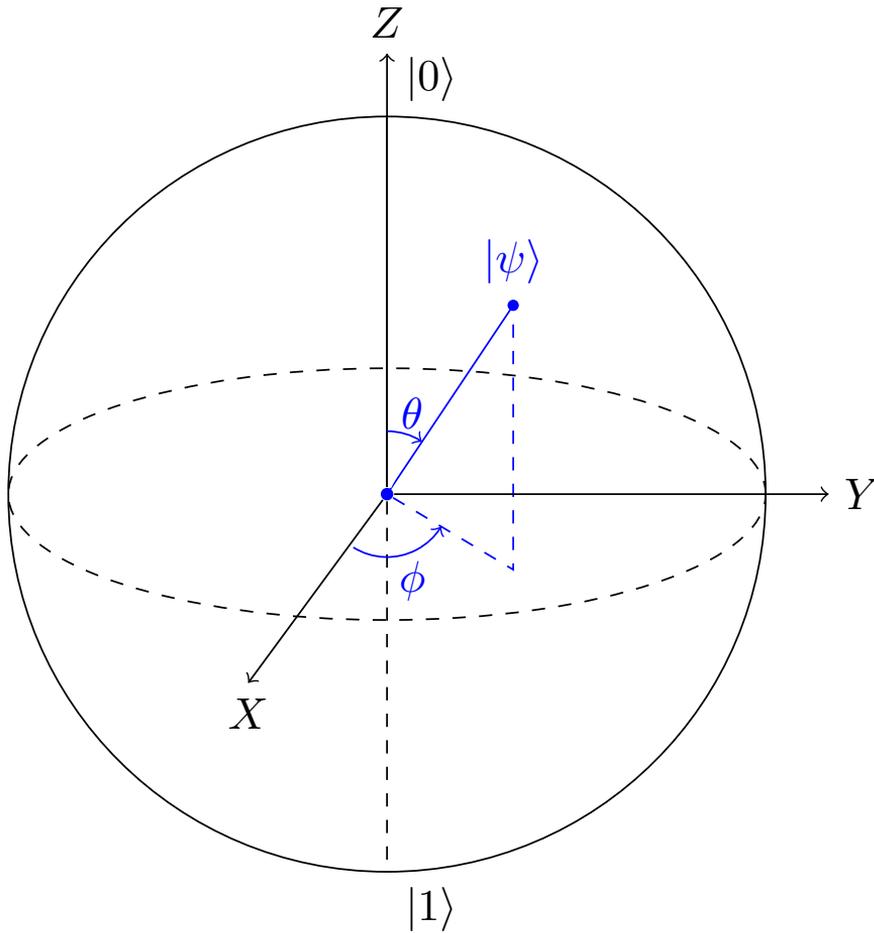


Figure 2.1: A qubit is typically represented using the BS.

The factor $e^{i\gamma}$ can be ignored, considering that it has no observable effects. Therefore the wave function in 2.10 can be expressed as follows:

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \quad (2.11)$$

Then, given a generic qubit on Hilbert space $H_{2 \times 1}$, the density operator

is defined as [140] [141]:

$$\rho \equiv |\psi\rangle \langle\psi| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix} = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{bmatrix} \quad (2.12)$$

The elements on the main diagonal of the Density Matrix (DM) represents the probabilities or outcomes obtained as a consequence of the quantum measurement process on qubits [117].

Furthermore, in order to represent the states $|0\rangle$ and $|1\rangle$, there are many possible choices of basis states, like the following set:

$$|+\rangle \equiv \frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \quad (2.13)$$

$$|-\rangle \equiv \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \quad (2.14)$$

The state can then be expressed as:

$$\begin{aligned} |\psi\rangle = \alpha |0\rangle + \beta |1\rangle &= \alpha \frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta \frac{|+\rangle - |-\rangle}{\sqrt{2}} = \\ &= \frac{\alpha + \beta}{\sqrt{2}} |+\rangle + \frac{\alpha - \beta}{\sqrt{2}} |-\rangle \end{aligned} \quad (2.15)$$

It is possible to use this base in the same manner as the CBS [38].

2.1.3 Entanglement

Entanglement describes the quantum physical fact that multi-particle systems of two or more particles can no longer be described as a combination of independent one-particle states, but only as a common state, which in principle must be described within a *single* wave function [142,143]. The entangled connection does not depend on the position of the particles in space. In fact, even if the entangled particles are separated by billions of miles, a variation in one particle induces a change in the other. Actually, even though quantum entanglement appears to transmit information instantaneously, it doesn't violate the classical speed of light [144].

The *Bell states*, also defined as *Bell pairs*, *EPR states* or *EPR pairs*, are maximally entangled pure two-qubit states [145]. Maximal entanglement means that Bell pairs have the strongest non-classical correlations of all possible two qubit states [79].

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (2.16)$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad (2.17)$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \quad (2.18)$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (2.19)$$

These four pure states, which are maximally entangled, form an orthonormal basis of the Hilbert space of the two qubits [146].

The Bell pairs are used in the teleportation process described in Section 2.2.4. Moreover, in the analysis of QNs, one of the parameters that is measured is the *entanglement rate*, which as explained in [20] is a special kind of throughput. Basically, it is the number of transmitted entangled states per second and is measured as EPR pairs per second [147] [148].

A typical entanglement generation system is depicted in Fig. 2.2. The system represented in Fig. 2.2, is realized with boxes that use the electronic spin associated with a single Nitrogen Vacancy (NV) defect centre in a diamond chip.

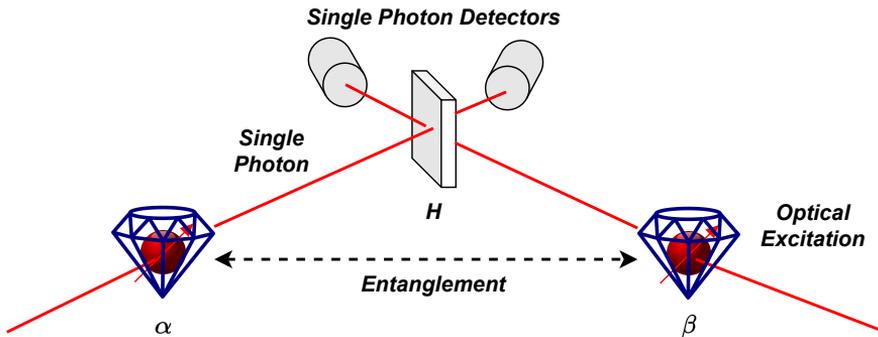


Figure 2.2: Typical entanglement generation system.

A trigger produces entanglement between the communication qubits of α and β (diamonds) and two qubits (photons) traveling over the channel to the heralding station H , which measures the photons by observing clicks in the left or right detector giving the heralding signal. Three results can be obtained that also denote the kind of the generated Bell state:

- Failure if none or both click are detected.
- Success Ψ^+ with a left click.
- Success Ψ^- with a right click [149].

The NV center in diamond is a promising candidate to act as a node in such QNs thanks to a combination of long spin coherence and spin-selective optical transitions that allow for high-fidelity initialization and single-shot readout. The diamond chips are mounted in closed-cycle cryostats with $T = 4\text{ K}$ in different locations. The electronic spin state of each NV centre is controlled with microwave pulses applied to on-chip striplines [150] [151].

2.1.4 No-Cloning Theorem

The no-cloning theorem is a result of quantum mechanics, which forbids the creation of *identical* copies of an arbitrary unknown quantum state [152]. Considering the properties of linearity of quantum mechanics, it is possible to provide a simple demonstration. Suppose that a device can implement a

linear transformation T in order to copy two orthogonal quantum states:

$$T |\psi\rangle |\psi\rangle = |\psi\rangle |\psi\rangle \quad (2.20)$$

$$T |\phi\rangle |\phi\rangle = |\phi\rangle |\phi\rangle \quad (2.21)$$

where $|\psi\rangle$ and $|\phi\rangle$ are two orthogonal quantum states and $|0\rangle$ is the ready state of the target system. It follows:

$$\begin{aligned} T(a |\psi\rangle + b |\phi\rangle) |0\rangle &= aT |\psi\rangle |0\rangle + bT |\phi\rangle |0\rangle \\ &= a |\psi\rangle |\psi\rangle + b |\phi\rangle |\phi\rangle \end{aligned} \quad (2.22)$$

However, if the transformation T cloned arbitrary inputs, we would have:

$$\begin{aligned} T(a |\psi\rangle + b |\phi\rangle) |0\rangle &= (a |\psi\rangle + b |\phi\rangle)(a |\psi\rangle + b |\phi\rangle) = \\ &= a^2 |\psi\rangle |\psi\rangle + b^2 |\phi\rangle |\phi\rangle + ab |\psi\rangle |\phi\rangle \\ &\quad + ab |\phi\rangle |\psi\rangle \end{aligned} \quad (2.23)$$

which differs from 2.22 unless a or b is zero [153] [154].

The no-cloning theorem is the fundamental principle on which quantum cryptography is based, and there is no equivalent in the field of classic communications. The no-cloning theorem forbids eavesdroppers from creating copies of a transmitted quantum cryptographic key.

2.2 Technological Aspects

This Section provides some technological aspects regarding the realization of QDs. Specifically, the single gates and more complex circuits required to perform teleportation and superdense coding are analyzed. Finally, the Section explains the working principle of QMs and related issues.

2.2.1 Quantum Gates

The quantum gates can be represented by **Pauli's matrices** and the **Hadamard matrix**. Each Pauli matrix specifies a half turn (180°) rotation around a particular axis of the BS up to a global phase [155] [156].

$$\sigma_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (2.24)$$

$$\sigma_1 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (2.25)$$

$$\sigma_2 = \sigma_y = i(|0\rangle\langle 1| - |1\rangle\langle 0|) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad (2.26)$$

$$\sigma_3 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (2.27)$$

$$H = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|] = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (2.28)$$

The Pauli matrices are involutory, meaning that the square of a Pauli matrix is the identity matrix and, therefore, two translation gates in sequence cancel [155].

$$I^2 = X^2 = Y^2 = Z^2 = -iXYZ = I \quad (2.29)$$

The logic gates that are associated with the previously defined matrices

are defined as follows:

2.2.1.1 Pauli-X Gate

The Pauli-X gate is the quantum equivalent of the NOT gate for classical computers with respect to the standard basis $|0\rangle, |1\rangle$, which distinguishes the z axis on the Bloch sphere. It is sometimes called a bit-flip.

$$|0\rangle \rightarrow |1\rangle \quad (2.30)$$

$$|1\rangle \rightarrow |0\rangle \quad (2.31)$$

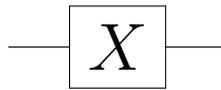


Figure 2.3: Representation of an X gate.

2.2.1.2 Pauli-Y Gate

The Pauli-Y gate is a single-qubit rotation through π radians around the y-axis.

$$|0\rangle \rightarrow i|1\rangle \quad (2.32)$$

$$|1\rangle \rightarrow -i|0\rangle \quad (2.33)$$

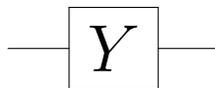


Figure 2.4: Representation of an Y gate.

2.2.1.3 Pauli-Z Gate

Pauli Z leaves the basis state $|0\rangle$ unchanged and maps $|1\rangle$ to $-|1\rangle$. Due to this nature, Pauli Z is sometimes called phase-flip.

$$|0\rangle \rightarrow |0\rangle \quad (2.34)$$

$$|1\rangle \rightarrow -|1\rangle \quad (2.35)$$



Figure 2.5: Representation of a Z gate.

2.2.1.4 Hadamard Gate

The Hadamard gate performs a rotation of π about the axis $(\hat{x} + \hat{z})/\sqrt{2}$ at the Bloch sphere.

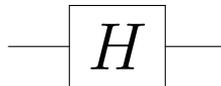


Figure 2.6: Representation of an Hadamard gate.

It creates an equal superposition state if given a computational basis state:

$$|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+\rangle \quad (2.36)$$

$$|1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle \quad (2.37)$$

2.2.1.5 Controlled NOT Gate

A multi-qubit quantum logic gate is the Controlled NOT (CNOT) gate, which has two input qubits, known as the control qubit and the target qubit, respectively. The circuit is represented in Fig. 2.8. The top line represents the control qubit, while the bottom line represents the target qubit. The action of the gate can be described as follows. If the control qubit is set to 0, then the target qubit is left alone. If the control qubit is set to 1, then the target qubit is flipped [157]. These operations are described in Table 2.1.

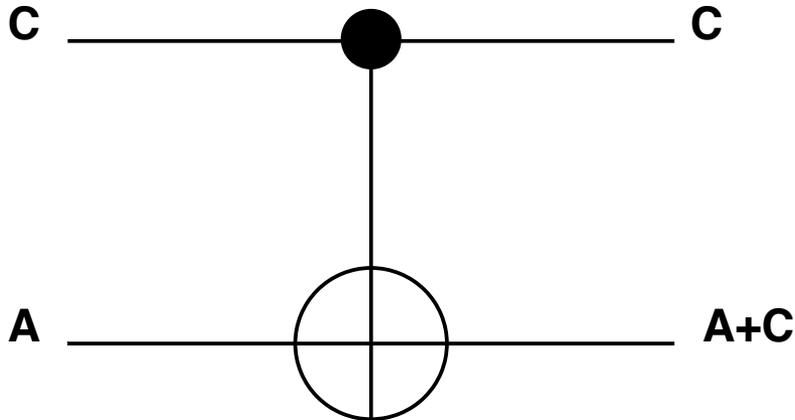


Figure 2.7: Representation of a CNOT gate.

Input		Output	
C	A	C	A+C
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$

Table 2.1: Truth table of a CNOT gate.

Another way of describing the is as a generalization of the classical gate, since the action of the gate can be summarized as $|A, C\rangle \rightarrow |A, B \oplus A\rangle$, where the symbol \oplus is addition modulo two, which is exactly what the XOR

gate does. Therefore, the control qubit and the target qubit are XORed and stored in the target qubit [158] [38].

2.2.2 Swap Circuit

The SWAP circuit is particularly important for practical reasons: in the current generation of quantum computing hardware, 2-qubit gates can only be applied among certain pairs of qubits. For example, when employing one of the most prevalent quantum hardware technologies, 2-qubit gates can only be applied to qubits that are physically adjacent on a chip. Thanks to the SWAP, as long as the connectivity graph of the qubits on the device is a connected graph, 2-qubit gates can be applied to any pair of qubits: if the qubits are not directly connected on the graph (e.g., physically located next to each other on the chip), we just need to SWAP one of them as many times as is necessary to bring it to a location adjacent to the other qubit. This way, we can assume that each qubit can interact with all other qubits from a theoretical point of view, even if from a practical perspective this may require extra SWAP gates.

Specifically, if two qubits are in a product state $|\Psi\rangle \otimes |\Phi\rangle$ the operation of a swap circuit performs the following operation [159] [160]:

$$SWAP(|\Psi\rangle \otimes |\Phi\rangle) = |\Phi\rangle \otimes |\Psi\rangle \quad (2.38)$$

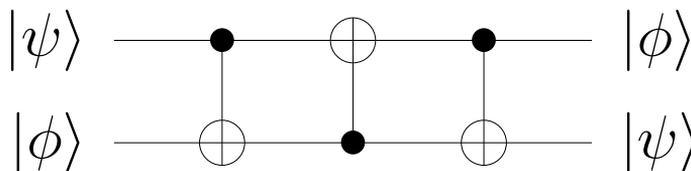


Figure 2.8: A circuit that swaps two qubits in a Quantum Computer.

2.2.3 Multipartite Entangled States

The type of entanglement described in Section 2.1.3, is referred to as *bipartite entanglement*, which has been extensively studied in literature and is described through the Bell states or EPR pairs. These states are, among the two-qubit states, the maximally entangled ones, namely, the states providing

the maximum amount of nonclassical correlation. When it comes to larger systems, the classification of the entangled states becomes broader. In the following the focus is on *multipartite entangled states* that may be of interest from a communication engineering perspective. Specifically, the multipartite systems, composed by 3 qubits and namely *tripartite systems* are discussed. Two kinds of tripartite entanglement are represented by the $|GHZ\rangle$ and the $|W\rangle$ states. These states are used in quantum communications [161] [162] and quantum computations [163] [164].

2.2.3.1 Greenberger-Horne-Zeilinger State

As defined in [165] [166], a Greenberger-Horne-Zeilinger (GHZ) state is a certain type of entangled quantum state that involves at least three subsystems. Specifically, for 3 qubits the GHZ state can be defined as:

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \quad (2.39)$$

The generalized GHZ state is an entangled quantum state of $M > 2$ subsystems and is expressed as follows:

$$|GHZ\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes \dots \otimes |i\rangle = \frac{1}{\sqrt{d}} (|0\rangle \otimes \dots \otimes |0\rangle + \dots + |d-1\rangle \otimes \dots \otimes |d-1\rangle) \quad (2.40)$$

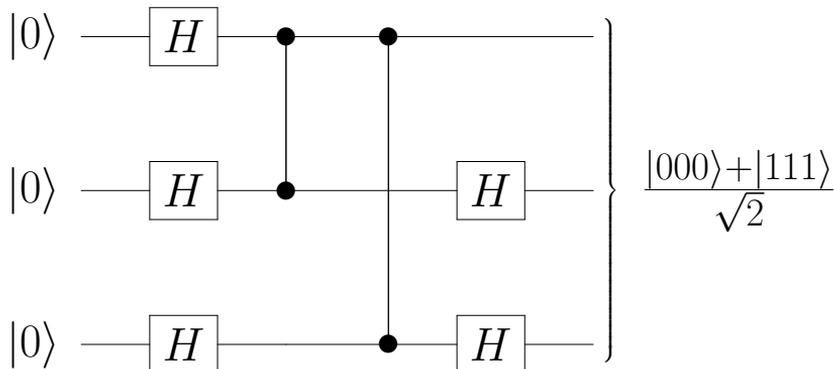


Figure 2.9: A quantum circuit that produces a GHZ state.

2.2.3.2 W State

The W state is an entangled quantum state of three qubits which has the following shape [167] [166]:

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle) \quad (2.41)$$

As explained in [166], the configuration of a W state can be generalized for n qubits:

$$|W\rangle = \frac{1}{\sqrt{n}}(|100\dots 0\rangle + |010\dots 0\rangle + \dots + |00\dots 01\rangle) \quad (2.42)$$

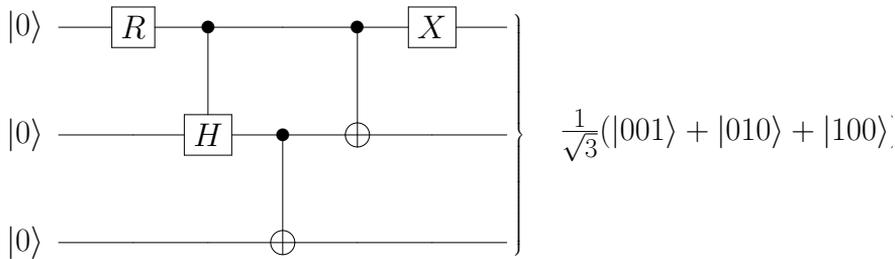


Figure 2.10: A quantum circuit that produces a W state.

2.2.3.3 Advantages and Disadvantages

Considering the persistency property, which denotes the minimum number of qubits that need to be measured to guarantee that the resulting state is separable [168] [169], W states significantly outperform GHZ states. Specifically, if an accidental measurement occurs on one of the qubits of a 3-qubit W state, it collapses in an unentangled state with probability equal to $\frac{1}{3}$, while preserving maximal entanglement with probability equal to $\frac{2}{3}$. Conversely, any accidental measurement completely erases any entanglement within a GHZ state, which collapses into a fully separable state. This behavior of W and GHZ states with reference to the persistence property can be generalized to n-qubit states. In particular, a n-qubit W state collapses into an unentangled state with a probability linearly decreasing with n and equal to $\frac{1}{n}$. The persistency property of W states makes them robust against losses

or accidental measurement of a qubit, whereas GHZ states are a reliable resource for generating EPR pairs [169].

Furthermore, as explained in [170], these states may have several practical applications, e.g., in quantum communication or quantum metrology, as they offer an increased stability against noise and decoherence without the need for active error correction.

2.2.4 Teleportation

Quantum teleportation is a technique for moving quantum states linking the quantum state of the sender to the receiver's one [171]. The first experimental demonstrations of quantum teleportation were performed with photons in Rome and Vienna in 1997 [172] [173]; in particular, the Vienna experiment was conducted by the group of Anton Zeilinger, who won the Nobel Prize in 2022 together with Alain Aspect and John Clauser [29].

In order to perform teleportation, an entangled pair needs to be distributed between the source and destination [60]. The source then entangles the qubit it intends to transmit, which state is indicated with $|\psi\rangle$ in Fig. 2.11, with its end of the pair and performs a Bell State Measurement (BSM). This consumes the Bell pair's entanglement, turning the source and destination qubits into independent states. The measurements yields two classical bits which the source sends to the destination over a *classical* channel. Based on the value of the received two classical bits, the destination performs one of four possible Pauli corrections on its end of the pair, which turns it into the unknown qubit state that we wanted to transmit. This requirement to communicate the measurement read out over a classical channel means that entanglement cannot be used to transmit information faster than the speed of light [79]. The following part analyses the phases of the teleportation process in more detail considering the circuit depicted in Fig. 2.11.

The state to be teleported is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are unknown amplitudes, while the input state of the circuit is:

$$\begin{aligned} |\psi_0\rangle &= |\psi\rangle |\Phi^+\rangle = \\ &= \frac{1}{\sqrt{2}} [\alpha|0\rangle (|00\rangle + |11\rangle) + \beta|1\rangle (|00\rangle + |11\rangle)] \end{aligned} \quad (2.43)$$

The first two qubits, which are identified as $Q1$ and $Q2$ in the scheme

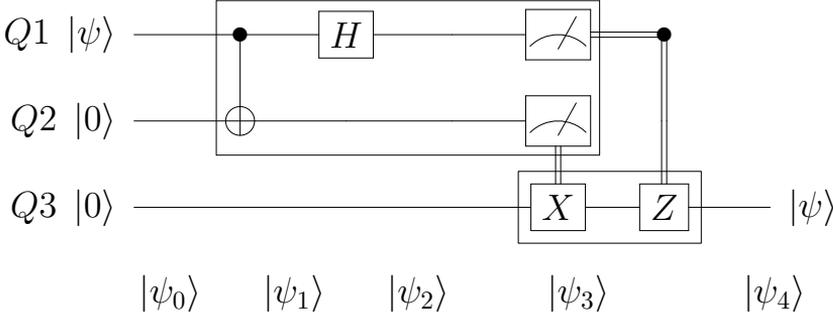


Figure 2.11: Quantum teleportation circuit.

represented in Fig. 2.11, are present in each term of the equation. Both the qubits are part of the first system, while $Q3$ is held by the second system. The $Q1$ and $Q2$ qubits are sent through the CNOT port [174] [158] [175] obtaining:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)] \quad (2.44)$$

The $Q1$ qubit is then sent through the Hadamard gate [174] [175], which maps the basis state $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$, and the state $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$ obtaining [139]:

$$|\psi_2\rangle = \frac{1}{2} [\alpha (|0\rangle + |1\rangle) (|00\rangle + |11\rangle) + \beta (|0\rangle - |1\rangle) (|10\rangle + |01\rangle)] \quad (2.45)$$

The equation can be rewritten as follows:

$$|\psi_2\rangle = \frac{1}{2} [|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)] \quad (2.46)$$

Depending on the outcomes of the measurements made on qubits $Q1$ and $Q2$, the $Q3$ qubit results in one of the following possible states:

$$|\psi_3\rangle = [\alpha |0\rangle + \beta |1\rangle] \quad (2.47)$$

$$|\psi_3\rangle = [\alpha |1\rangle + \beta |0\rangle] \quad (2.48)$$

$$|\psi_3\rangle = [\alpha |0\rangle - \beta |1\rangle] \quad (2.49)$$

$$|\psi_3\rangle = [\alpha |1\rangle - \beta |0\rangle] \quad (2.50)$$

The measurement outcome is sent through the classical channel to the other system, which applies the appropriate quantum gates on his qubit in order to recover the state $|\psi\rangle$.

Considering that the measurement at the source destroys the entangled pair if another qubit needs to be teleported, it is necessary to distribute a new Bell pair between the source and the destination [176].

2.2.5 Superdense Coding

The superdense coding is a quantum communication protocol to communicate a number of classical bits of information by transmitting several qubits,

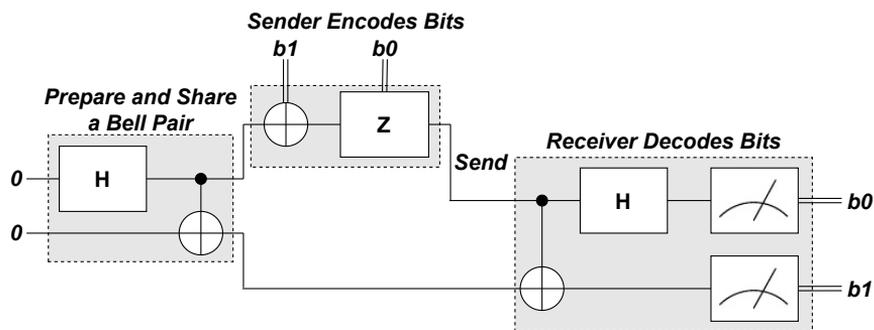


Figure 2.12: When the sender and receiver share a Bell state, two classical bits can be packed into one qubit. The lines carry qubits, while the doubled lines carry classic bits. The variables b_0 and b_1 are classic boolean, while $|0\rangle$ represents a pure quantum state.

under the assumption of sender and receiver pre-sharing an entangled resource [37] [38]. The superdense coding circuit is depicted in Fig. 2.12.

As can be seen from Fig. 2.12, the protocol consists of the following 5 steps:

- Preparation
- Sharing
- Encoding
- Sending
- Decoding

The protocol starts with the *preparation* of an entangled state (one *ebit* in one of the four Bell states), which is later shared between Alice and Bob. Suppose the following Bell state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B) = \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \quad (2.51)$$

After the preparation of the Bell state $|\Phi^+\rangle$, there is the *sharing* phase. Specifically, the qubit denoted by subscript A is sent to Alice and the qubit denoted by subscript B is sent to Bob.

During the *encoding* phase, Alice applies one of four unitary operations $\{I, X, Z, XZ\}$ to her share of the above state. The state becomes one of the following four Bell states (up to a global phase), depending on the message that Alice chooses:

$$|\Phi^+\rangle_{AB} \quad |\Phi^-\rangle_{AB} \quad |\Psi^+\rangle_{AB} \quad |\Psi^-\rangle_{AB} \quad (2.52)$$

In the *sending* phase, Alice transmits her qubit to Bob using a QN through some conventional physical medium.

Finally, there is the last phase of the protocol, which is *decoding*. Bob performs a Bell measurement (a measurement in the basis $|\Phi^+\rangle_{AB}, |\Phi^-\rangle_{AB}, |\Psi^+\rangle_{AB}, |\Psi^-\rangle_{AB}$) to distinguish the four states perfectly he can distinguish the states because they are all orthogonal to each other. In other words, Bob will perform the CNOT unitary operation, with A as control qubit and B

as target qubit. Furthermore, the Hadamard quantum gate is only applied to A. Thus, Alice can transmit two classical bits (corresponding to the four messages) if she shares a noiseless ebit with Bob and uses a noiseless qubit channel [36].

2.2.6 Trace Distance

The trace distance is a metric on the space of density matrices, which gives a measure of the distinguishability between two states. The trace distance between two quantum states ρ and σ is defined as:

$$D(\rho, \sigma) \equiv \frac{1}{2} \text{Tr} |\rho - \sigma| \quad (2.53)$$

It is a number between 0 and 1:

$$0 \leq D(\rho, \sigma) \leq 1 \quad (2.54)$$

Furthermore, the trace distance is an optimal bias that can be used to correctly determining which of the two states was prepared [177] [38] [178].

2.2.7 Fidelity

The quality of the teleportation is characterized by the quantum fidelity:

$$F(|\psi\rangle, \rho) = \text{Tr} \sqrt{\langle\psi|\rho|\psi\rangle|\psi\rangle\langle\psi|} = \sqrt{\langle\psi|\rho|\psi\rangle} \quad (2.55)$$

The fidelity is a number between 0 and 1 [179]:

$$0 \leq F(|\psi\rangle, \rho) \leq 1 \quad (2.56)$$

Fidelity is equal to 0 if and only if $|\psi\rangle$ and ρ have orthogonal support, and it is equal to 1 if and only if $|\psi\rangle = \rho$. When $|\psi\rangle$ and ρ are supported on orthogonal subspaces they are perfectly distinguishable, hence, in this case the fidelity is minimized [38] [180] [146].

Basically, the fidelity describes how *close* two quantum states are. In particular, it can be used to characterize drastic changes in quantum states when

systems are affected by Quantum Phase Transitions (QPTs) [181]. If values below 0.5 are obtained, it means that the created state is distant from the one intended to be created and is therefore not useful for computation [79].

Fidelity is strictly related to trace distance through the following inequality:

$$1 - \sqrt{F(|\psi\rangle, \rho)} \leq D(|\psi\rangle, \rho) \leq 1 + \sqrt{F(|\psi\rangle, \rho)} \quad (2.57)$$

Moreover, if we consider pure states the trace distance is equal to the upper bound:

$$D(|\psi\rangle, \rho) = 1 + \sqrt{F(|\psi\rangle, \rho)} \quad (2.58)$$

2.2.8 Decoherence

The interaction of an open quantum system with its surroundings creates correlations between the states of the system and of the environment. The environment carries information on the open system in the form of these correlations. For certain system-environment interactions the environment behaves similarly to a quantum probe performing a kind of indirect measurement on the open system: after tracing over the environmental degrees of freedom a certain set of states of the open system's Hilbert space exhibits strong stability properties, while superpositions of these states are destroyed over time, often very rapidly or even nearly instantaneously. This environment-induced, dynamical destruction of quantum coherence is called decoherence [84] [7]. It leads to a dynamical selection of a distinguished set of pure states of the open system and counteracts the superposition principle in the Hilbert space of the open system. The theory of decoherence allows a number of interesting physical applications, ranging from fundamental questions of quantum mechanics to technological applications in quantum information processing [182].

A quantum state vector $|\psi_i\rangle$ encapsulates maximum knowledge about the state of a physical system. We can also define the *density operator* ρ corresponding to such a pure state $|\psi\rangle$ as:

$$\rho \equiv |\psi\rangle \langle\psi| \quad (2.59)$$

If we express $|\psi\rangle$ as a superposition of basis states $|\psi_i\rangle$:

$$|\psi\rangle = \sum_i c_i |\psi_i\rangle \quad (2.60)$$

the corresponding DM written in this basis $|\psi_i\rangle$ can be expressed as follows:

$$\rho = |\psi\rangle \langle\psi| = \sum_{ij} c_i c_j^* |\psi_i\rangle \langle\psi_j| \quad (2.61)$$

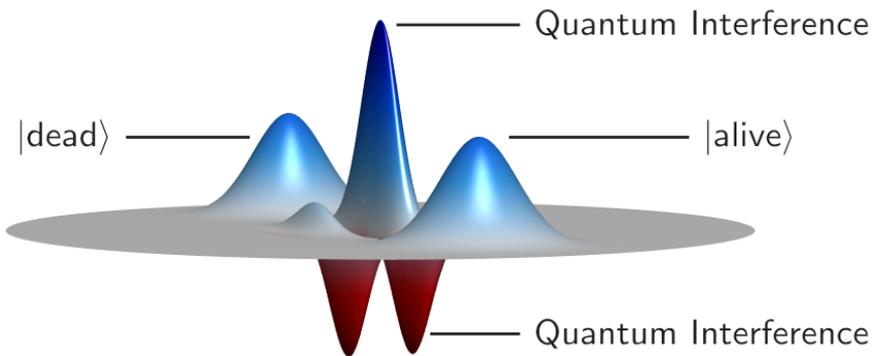


Figure 2.13: The iconic textbook example of a Wigner function, which can be used to study the decoherence phenomena measuring its purity. The oscillations between the two states indicate the quantum coherence between them [5] [6].“The iconic textbook example of a Wigner function” by Rundle, R. P. et al. <https://journals.aps.org/prapdf/10.1103/PhysRevA.96.022117> is licensed under CC BY 3.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/3.0>

The terms $i \neq j$ on the right-hand side of this equation embody the quantum coherence between the different components $|\psi_i\rangle$. Accordingly, they are usually referred to as interference terms, or off-diagonal terms [183]. Decoherence diminishes the off-diagonal elements of the DM so that with time it tends to become a diagonal matrix. Such a DM cannot be obtained from a pure quantum state but rather resembles a classical mixture of two quantum states of the particle. The quantum decoherence disregards the observer and the measurement process, preceding it and simulating the collapse of the wave function [80]. In particular, the collapse produces the transition from

a coherent state to an incoherent one, in which the off-diagonal terms of the DM are zero; the decoherence instead causes a spontaneous transition from a coherent state to a decoherent one, in which the off-diagonal terms of the DM are asymptotically infinitesimal [81]. Due to the large number of such particles (and, hence, degrees of freedom), the overlap between their different joint states will rapidly decrease as a result of the buildup of many interaction events. Therefore, the exponential decay of coherence is governed by an average lifetime defined as *decoherence time* τ_d characteristic for that specific system [116] [7]:

$$\propto e^{-\frac{t}{\tau_d}} \quad (2.62)$$

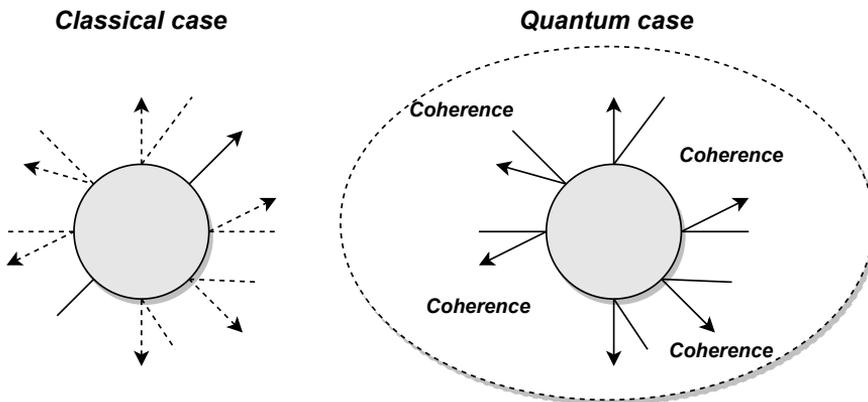


Figure 2.14: The different influence of the environment on the system in the classical and quantum cases, illustrated for the case of a macroscopic body that interacts with light incident from all directions. In the classical case, which is represented on the left, light scattering off the body will not change the motion of the body, even though the environment interacts strongly with the system. On the contrary, in the quantum case, the interaction leads to an entangled object-photon state [7].

The entanglement is the most valuable resource for transmitting quantum information, but it is also a perishable resource. Indeed, due to the inevitable interactions with the external environment, there exists a loss of the entanglement between the entangled entities as time passes. Hence, a quantum routing metric must explicitly account for the quantum decoher-

ence [66]. Furthermore, as explained in [184], considering that decoherence can be due to different causes, it is system-specific, and the time decay can proceed also considering the change of several parameters, e.g., material and isotope composition, temperature, magnetic fields, confinement geometry, and gate potentials.

The interactions with the environment degrade the peculiar quantum property of the system (e.g. superposition and entanglement) resulting in energy dissipation and decoherence. Therefore, there are two main mechanisms that are necessary to consider in order to have a more realistic picture of qubit dynamics. These mechanisms are relaxation and dephasing [185] [186] [187], which are represented in Fig. 2.15 and are described as follows.

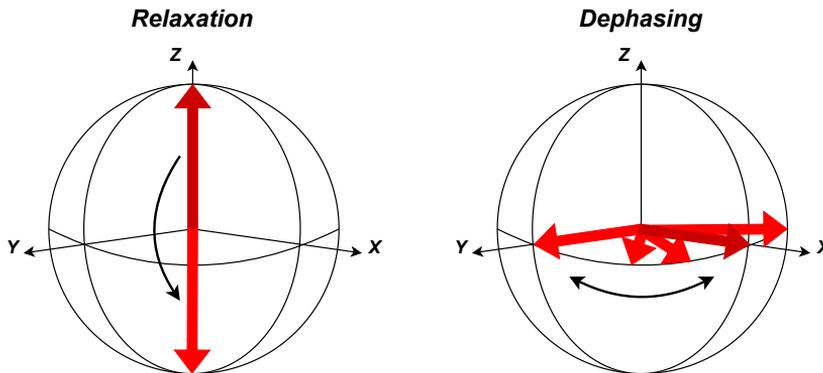


Figure 2.15: Representation of the Relaxation and Dephasing processes of a qubit.

The decay of the diagonal part of the DM in the eigenstate basis $|0\rangle, |1\rangle$ involves the $|0\rangle \rightarrow |1\rangle$ qubit transitions, with the energy transferred to the environment. This event restores the qubit to its ground state, and it happens at a random time [188]. Specifically, this phenomena changes the latitudinal component of the Bloch vector as depicted in Fig.2.15. The time scale that qubit spontaneously relaxes its energy is called the *relaxation time* and is indicated by T_1 [187].

The dephasing phenomena thus involves longitudinal fluctuations [186] [188]. The variation of the longitudinal component of the Bloch sphere is depicted in Fig.2.15. The time scale that the qubit loses its coherence is usually called the *dephasing time* and is indicated by T_2 [187].

Both relaxation and dephasing phenomena can be taken into account with the DM [38]:

$$\rho(t) = \begin{bmatrix} \cos^2 \theta (1 - e^{-\frac{t}{T_1}}) & \sin \theta \cos \theta e^{i\phi} e^{-\frac{t}{T_2}} \\ \sin \theta \cos \theta e^{-i\phi} e^{-\frac{t}{T_2}} & \sin^2 \theta e^{-\frac{t}{T_1}} \end{bmatrix} \quad (2.63)$$

The matrix that we obtain after decoherence no longer corresponds to a wave function. Every wave function gives a DM, but not every DM gives a wave function. The matrix that we have after decoherence describes classical probabilities. The quantum behavior tends to vanish very quickly with all the interactions that every particle constantly has, whether or not they are measured. The DM describes only one single particle. Once they are measured, it is with probability 1 either in one state or in the other. But this would correspond to a DM which has one diagonal entry that is 1 and all other entries 0.

2.2.9 Quantum Memories and Related Components

In quantum telecommunications equipment, it is necessary to make a distinction between *matter* and *flying qubits*. They are identified as matter qubits, the qubits used for information processing/storing, i.e., those that compose the quantum memories, while flying qubits are the qubits that pass through the quantum communication channel. The QM is an important component of quantum information processing applications such as QN, QR, linear optical quantum computation or long-distance quantum communication [189]. Some of the main technologies used for the realization of the quantum gates that compose quantum memories are the following:

- Ion traps
- Superconducting qubits
- Quantum dots [190]
- Solid-State Spin
- Topological

2.2.9.1 Ion Traps

An **ion trap** is a combination of electric or magnetic fields used to capture charged particles in a system *isolated* from an external environment [191] [192]. The two most common types of ion trap are the Penning trap [193], which forms a potential via a combination of electric and magnetic fields, and the Paul trap which forms a potential via a combination of static and oscillating electric fields [194].

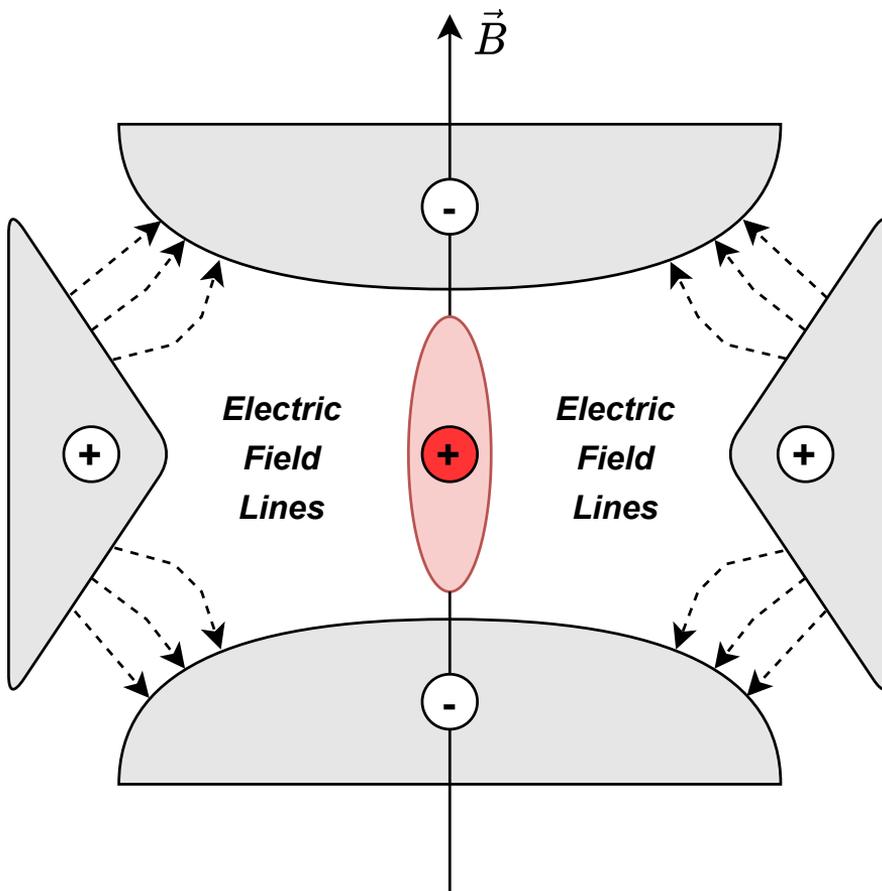


Figure 2.16: Electric and magnetic field configurations of the Penning trap.

2.2.9.2 Superconducting Qubits

Superconducting qubits consist of simple circuits that can be described as the parallel combination of a Josephson tunnel element with inductance L_J , a capacitance C , and an inductance L [195]. Fig. 2.17 represents a Josephson junction, while Fig.2.18 represents a Superconducting qubit circuit.

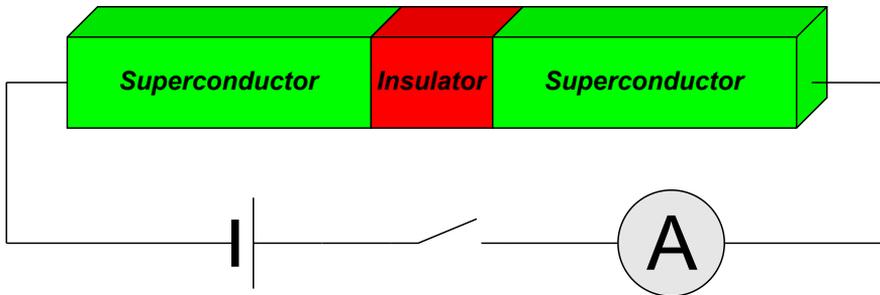


Figure 2.17: Schematic representation of a Josephson junction.

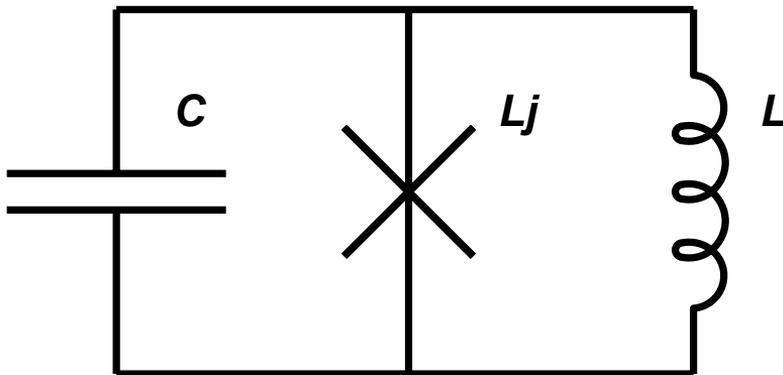


Figure 2.18: Superconducting qubit circuit realized with a Josephson junction.

2.2.9.3 Quantum Dots

Quantum dots are semiconductor particles a few nanometres in size, having optical and electronic properties that differ from larger particles due to quantum mechanics. Quantum dots are sometimes referred to as artificial

atoms [196] [197]. These devices are significant for applications in quantum information processing given their characteristics, such as the fast operation rates and the possibility of on-chip integration [198] [199].

2.2.9.4 Solid-State Spin

The Solid-State Spin qubits are nuclear or electron spin of donor atoms in a semiconductor or NV centers in diamond. The Solid-State Spin qubits are intrinsically compatible with industrial semiconductor processing. However, nuclear spins are more difficult to manipulate than electron spins and are often considered too slow for quantum information processing [200] [201].

2.2.9.5 Topological

These types of memories have been proposed by the physicist Alexei Kitaev [202]. This technology is based on the existence of topological states of matter whose quasiparticle excitations are neither bosons nor fermions, but are particles known as non-Abelian anyons, meaning that they obey non-Abelian braiding statistics. Quantum information is stored in states with multiple quasiparticles, which have a topological degeneracy. The unitary gate operations that are necessary for quantum computation are performed by braiding quasiparticles and then measuring the multi-quasiparticle states [203] [204].

2.2.9.6 Quantum Computing Systems

A Quantum Computing System (QCS) can be envisioned within a layered structure as shown in Fig. 2.19. Specifically, it consists of a physical and logical layer. The physical layer provides the error correction and consists of a physical quantum processor that has both input and output lines that are controlled by the Quantum Error Correction (QEC) processor. The QEC processor is in turn controlled by the logical layer, where the encoded qubits are defined and the logical operations are performed for the specific quantum algorithm [8].

Several possible applications that a quantum computer like the one represented in Fig. 2.19 can run include the possibility to perform quantum algorithms such as Shor's factoring, Grover's search, or digital quantum simulations of real world chemical molecules and dynamics [8], banking and financial applications, and advanced manufacturing [205].

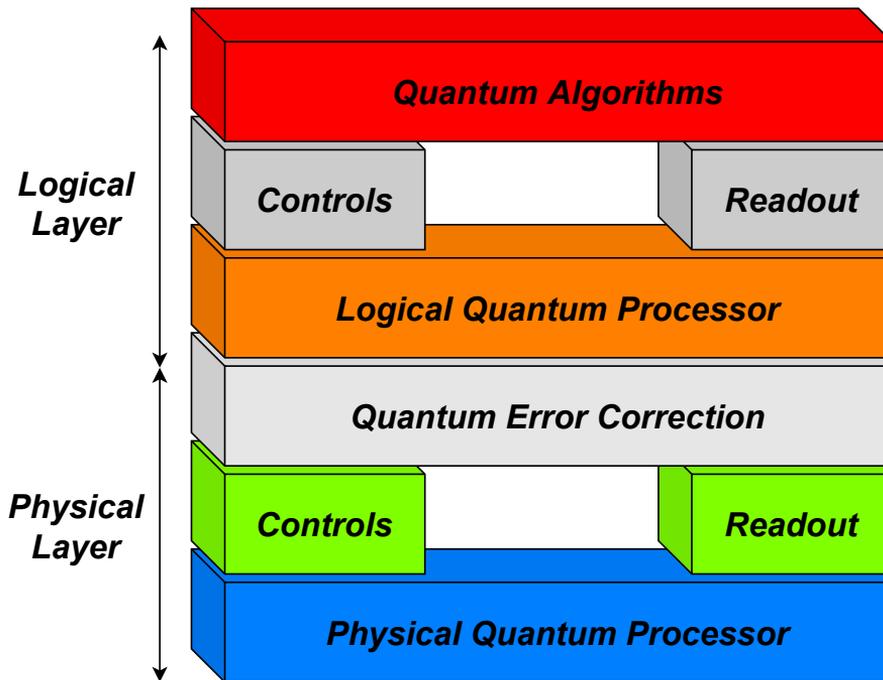


Figure 2.19: A systems view of a quantum information processor. It consists of a physical and logical layer [8].

2.2.9.7 Cooling Systems

The cooling system is a step towards meeting the practical challenges of operating large-scale QCs with many qubits and many cryogenic cooling solutions have been adopted. However, these specific cooling systems are not only necessary for QCs. As a matter of fact, considering that QMs are key ingredients for the realization of QRs [206] [207] [71], these devices also need a cooling system [208] [209]. Specifically, these apparatuses consist of either an open bath or an open continuous-flow cryostat that use 4 K liquid helium or 77 K liquid nitrogen as coolant [210].

As depicted in Fig.2.21, the physical qubit processor is located at the bottom plate of a dilution refrigerator at a temperature of 15 *mk*.



Figure 2.20: A detail of a dilution refrigerator. Gold-colored coaxial cables are used to send input and output signals from inside the cooler. “Inside an IBM Dilution Refrigerator” by IBM Research https://www.flickr.com/photos/ibm_research_zurich/26093909563 is licensed under CC BY-ND 2.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nd/2.0>.

Microwave pulses are generated at room temperature using synthesizers, arbitrary waveform generators, and mixers to control the system in such a way as to realize specific qubit rotations and controlled operations. These pulses are filtered and attenuated to assure negligible noise at the qubit. High-fidelity readout of the qubit state requires quantum-limited and other cryogenic amplification to overcome thermal noise for digitization and weighted homodyne measurement. The QEC processor sits above and orchestrates the physical control and readout functions, to perform the error correction protocol [8].

In Fig. 2.22 are depicted the necessary apparatuses that enable a QD to operate. Specifically, the scheme also illustrates the electrical connections

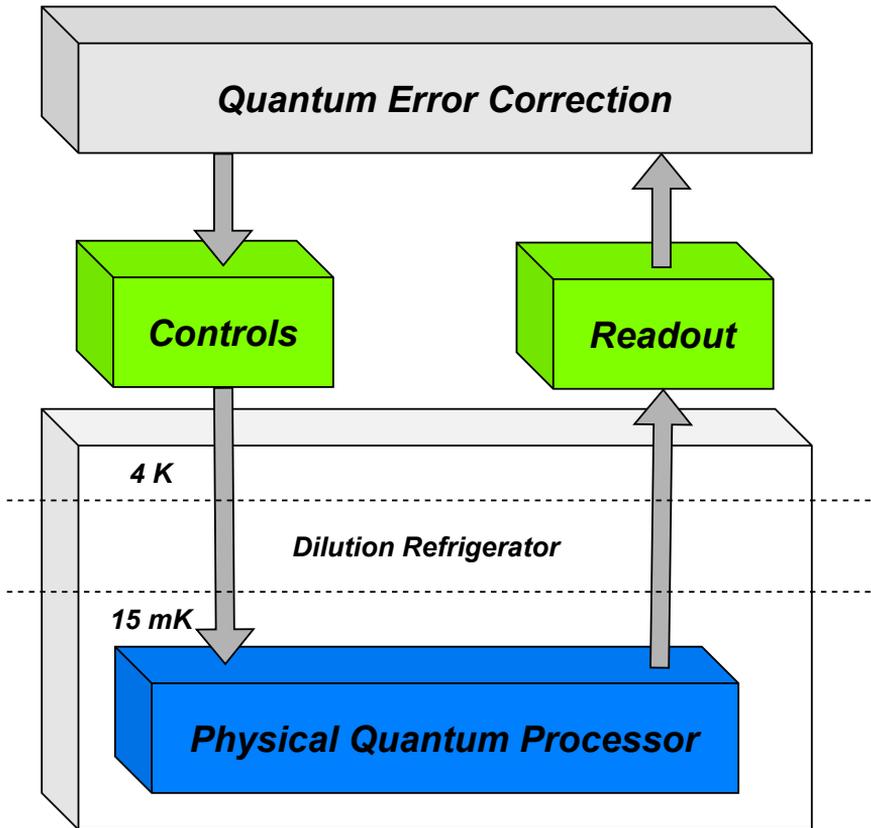


Figure 2.21: Diagram representing the operating principle of a dilution refrigerator.

and the cooling system, which includes the pumps to flow the coolant. What might be inferred from looking at Fig. 2.22 is that these devices require high power consumption. As explained in [211], quantum computation requires less energy consumption compared to traditional computation. However, as QCs increase in size, the total energy used by a QDC, including the cooling, can become significant. The cooling requirements of QCs, which operate at temperatures near absolute zero, are determined by computing system parameters, including the number and type of physical qubits, the packaging efficiency of the system, and the split between circuits operating at cryogenic temperatures and those operating at room temperature [212].

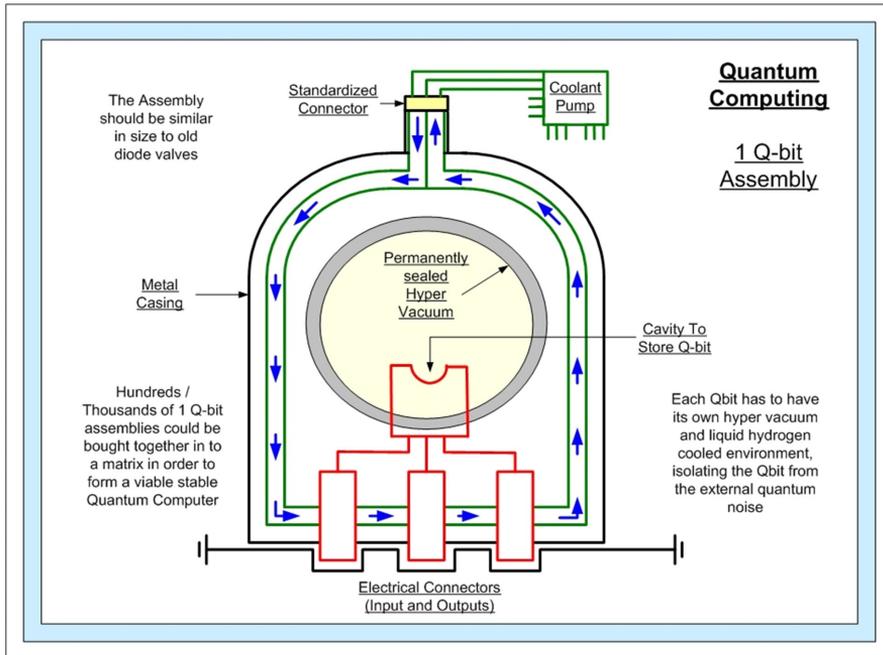


Figure 2.22: Diagram representing the outline apparatuses needed to create a QD.

2.2.9.8 Matter and Flying Qubits

Conversely, as regards to the flying qubits, there exists a general consensus about adopting photons as qubit substrate [213]. However, heterogeneity arises by considering the different physical channels the photons propagate through, ranging from free-space optical channels (either ground or satellite free-space) to OFs. Thus, a transducer for matter-flying conversion is necessary [11]. From an engineering perspective, the interface should be compatible also with the peculiarities of the physical channels the flying qubits propagate through. In fact, there exist different physical channels for transmitting flying qubits, ranging from free-space optical channels (either ground or satellite free-space) to OFs [176]. Communication models need to take into account such a technological heterogeneity, with the aim of providing a black box for upper protocol layers with *one common logic* [11]. Fig. 2.23 represents a typical interface between a QD and the communication channels.

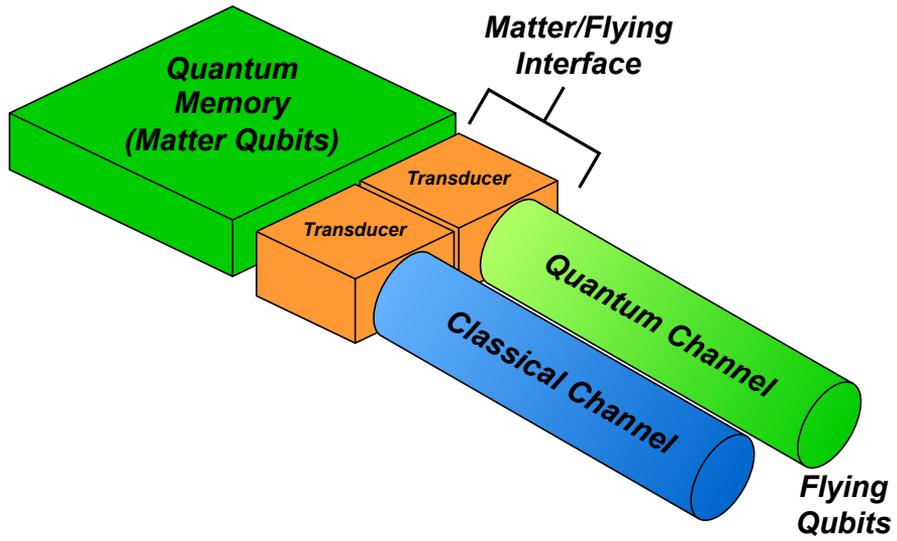


Figure 2.23: Representation of a matter-flying transducer. It converts matter qubits into flying qubits and vice versa.

Chapter 3

Quantum Technologies Applications and Related Works

This Section describes many of the experiments conducted towards the realization of future quantum satellite networks. The first experiments are feasibility studies towards the creation of quantum satellite networks and the implementation of QKD. Some of them are studies aimed at the creation of backbone controlled through SDN technology, considering the possibility of interconnecting specific Cloud systems through them and the implementation of QPS.

3.1 Fundamentals of Quantum Cryptography

This Section provides some elements of quantum cryptography. The reasons for the transition from systems based on classical cryptography to those using quantum cryptography are described. Furthermore, after an initial overview of the various protocols, some of the most significant and so far used protocols are described in detail.

3.1.1 Motivations

It is imperative to introduce the key players in most cryptographic scenarios: Alice and Bob are the parties that want to securely communicate and Eve is the malicious eavesdropper. Communication is achieved by the encoding of a secret message into what is called *cypher text* by Alice and then

transmission of the cypher text over the channel to Bob, who then decodes the cypher text into the original message. This communication is called *secure* if despite having full access to the cypher text, Eve cannot decode the message. Whether Eve can decode the message or not depends on what resources we give her, and this point raises the first important definitions: a communication protocol is called computationally secure if Eve requires *exponential* computational resources to break the cypher text. In contrast, an information-theoretic secure protocol does not make any assumptions on Eve's computational power. These schemes do not usually guarantee future security, meaning that an eavesdropper could simply store the cypher text until he/she has enough computational power to crack it.

An example of public key cryptography is the RSA protocol [214] [215] that is widely used on the Internet. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977 and it works as follows:

- To generate his public and private keys, Bob first chooses two large *prime numbers* p and q , and computes their product: $n = pq$.
- Bob then chooses a number $3 < e < (p - 1)(q - 1)$ such that e and $(p - 1)(q - 1)$ have no common factor; i.e. $\nexists k \in \mathbb{Z}, s.t. \frac{e}{k} \in \mathbb{Z} \text{ and } \frac{n}{k} \in \mathbb{Z}$.
- Bob then calculate d such that $ed = 1 \pmod{(p - 1)(q - 1)}$.
- Finally Bob publishes his public key pair $(e; n)$ and keeps his private key pair $(d; n)$ secret.
- When Alice wants to communicate with Bob, she encodes her message m as: $c = m^e \pmod n$, and sends this message over a channel.
- When Bob receives Alice's cypher text, he decodes by performing: $c^d \pmod n = m^{ed} \pmod n = m$.

A numerical example of RSA algorithm is reported in Fig. 3.1.

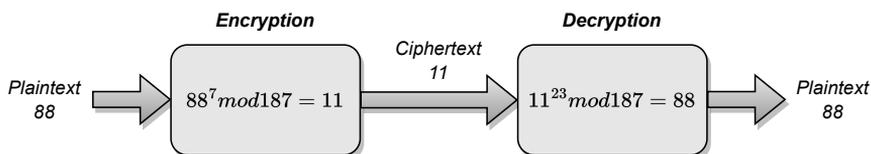


Figure 3.1: A numerical example of RSA algorithm.

The security of the RSA scheme relies on the difficulty of finding d even if one knows the public key pair $(e; n)$. And this in turn, relies on the difficulty of factoring n (which is known) into its prime factors p and q (since if Eve were able to do this, then she could compute d in exactly the same way Bob did). Therefore, RSA is obviously a computationally-secure scheme [216]. However, Peter Shor of AT&T in 1994, demonstrated that a Quantum Computer can decompose an integer number into prime factors with polynomial complexity, whereas it is conjectured that the classic computer requires exponential complexity. It is an alarming discovery because the majority of current cryptographic security systems are based on the (exponential) difficulty of prime factor decomposition [61].

The best known example of quantum cryptography is QKD are provably secure protocols, by which private key bits can be created between two parties over a public channel. The key bits can then be used to implement a classical private key cryptosystem, to enable the parties to communicate securely. The only requirement for the QKD protocols is that qubits can be communicated over the public channel with an error rate lower than a certain threshold. The security of the resulting key is guaranteed by the properties of quantum information [38].

The final aim of quantum cryptography is to create a global infrastructure for key distribution involving both fiber optic communication channels and open space including optical connections between low orbit satellites [217].

3.1.2 CVQKD

Basically, the main distinction between DVQKD and CVQKD protocols consists in the detection technique that is employed: single-photon detection for DVQKD protocols and homodyne or heterodyne for CVQKD [35]. The main advantage of using CVQKD systems consist on the fact that is possible to reuse devices already developed for classical optical communication systems, which are commercially available. Hence, this technology can be easily integrated into existing telecommunications networks [218] [35]. In the CVQKD scheme, the measurement are based on homodyne or heterodyne detection and involve measuring data that are real amplitudes instead of discrete events [219] [220]. Specifically, in CVQKD protocols information is encoded in the quadratures of the quantised electromagnetic field, such as those of coherent states [221] [222]. Many CVQKD protocols have been proposed and are classified considering the states:

- Single-mode coherent or squeezed states, two-mode squeezed states.
- On the choice of modulation for single-mode states, Gaussian or non-Gaussian.
- On the choice of detection, homodyne or heterodyne.
- On the type of error correction or else, reconciliation, direct or reverse [34] [35].

Recently, the multicarrier CVQKD has been introduced through the adaptive quadrature division modulation [223], which is described in [224]. Furthermore, Gaussian protocols based on the Gaussian modulation of Gaussian states have received an increasing attention recently, considering that they can be easily described through the mean value and the covariance matrix [225] [226]. One of the most straightforward and widely developed CV-QKD protocols is the Gaussian Modulated Coherent-State (GMCS) protocol, which constitutes the basis of the most recent implementations [227] and it is summarized as follows:

1. Alice produces two random numbers χ_A and ϕ_A from random numbers following a Gaussian distribution with a variance of $\nu_A \eta_0$, where η_0 is the vacuum noise unit.
2. Alice prepares a coherent state $|\chi_A + i\phi_A\rangle$ and sends it to Bob through an untrusted quantum channel.
3. Bob chooses homodyne (heterodyne) detection to measure χ and ϕ randomly (simultaneously) and obtains the outcomes χ_B and ϕ_B .
4. After repeating this process N times, Alice and Bob sift the measurement results using a classical channel and obtain N pairs of raw keys, i.e., the correlated Gaussian variables, in the homodyne detection protocol ($2N$ pairs in the heterodyne detection protocol).
5. Alice and Bob perform postprocessing on the raw key including parameter estimation, error correction, and privacy amplification.

3.1.3 DVQKD

In DV protocols information is typically encoded in the polarisation or phase of weak coherent pulses simulating true single-photon states; hence the corresponding implementations employ single-photon detection techniques [221] [228].

According to [33], the DVQKD protocols can be classified in the following fashion:

- Single-photon protocols, refer to a class of protocols that use different quantum states of a single photon for encoding and decoding to achieve key distribution in the key distribution process.
- Entangled-photon protocols realize QKD by using the properties of quantum entangled states. Differently from single-photon protocols, the entangled-photon protocols communicate with a pair of mutually entangled photons.
- Other DV protocols, can be divided into two main categories, which are distributed phase reference protocols and discrete variable two-way protocols. The distributed phase reference protocols mainly include Differential Phase Shift (DPS) protocol [229] and Coherent One-Way (COW) protocol [230]. Other significant protocols are Round-Robin Differential Phase Shift (RRDPS) [231], Ping-Pong [232] and LM05 protocol [233].

The most significant DVQKD protocols are described in the following Sections.

3.1.3.1 BB84

The most well-known Single-photon DVQKD protocol is the BB84, which has been conceived by Bennett and Brassard in 1984 [234].

A schematic version of a BB84 protocol implementation, using Pockels cells is shown in Fig. 3.2. Specifically, a Pockels cell is an electro-optic device which rotates the polarization vector of the light passing through it in proportion to the applied voltage. These electrically controlled cells thus make it possible to produce the various desired states of polarization [235].

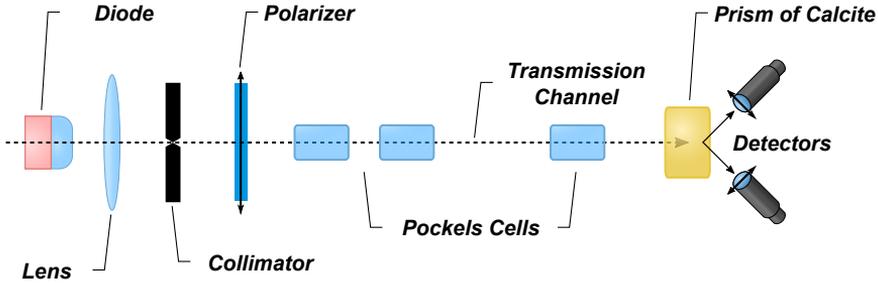


Figure 3.2: Schematic version of a BB84 protocol implementation, using Pockels cells and a birefringent calcite prism to separate the polarized beam. “Fichier:Bb84-french.svg” <https://fr.wikipedia.org/wiki/Fichier:Bb84-french.svg> is licensed under CC BY-SA 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/4.0/deed.en>. The picture has been modified within the terms of the license translating the names of the components from French to English.

As a matter of fact, the information that Alice exchanges with Bob on the quantum channel is composed of single photons at a given polarization [236] [237]. Therefore, Alice synchronizes her Pockels cell with the single-photon source and applies the correct voltages to produce polarization rotations of 0° , 45° , 90° , or 135° .

In this way she can send a string of binary data which is encoded in either of the two polarization bases at her choice. The photons emerging

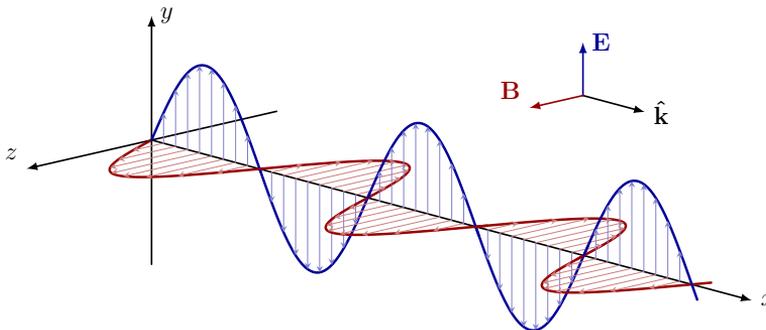


Figure 3.3: Vertical polarization.

from Alice's apparatus are received by Bob who has a polarization measurement system. Bob applies the correct voltage to this Pockels cell to rotate the polarization vector of the incoming photon by either 0° or -45° at his choice. The two choices are equivalent to detecting in the \oplus and \otimes bases, respectively [235].

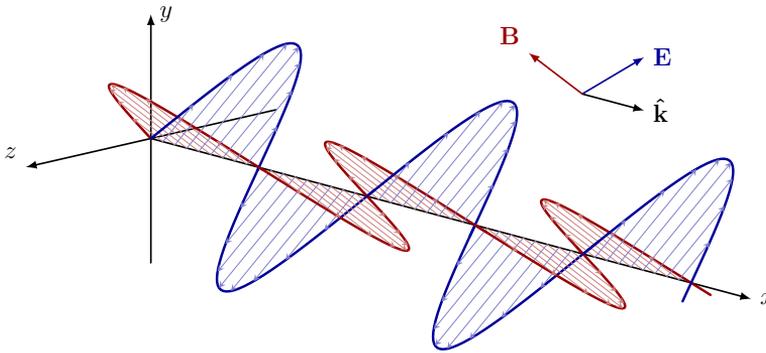


Figure 3.4: Diagonal polarization.

Therefore, the BB84 protocol transmits one of two orthogonal states chosen at random, encoded in one of two randomly chosen non-orthogonal bases [238]. As depicted in Fig. 3.6, two channels are established between Alice and Bob, the quantum channel, which is only a one-way channel, and a classical channel, that is used by Alice and Bob to perform the classical phase.

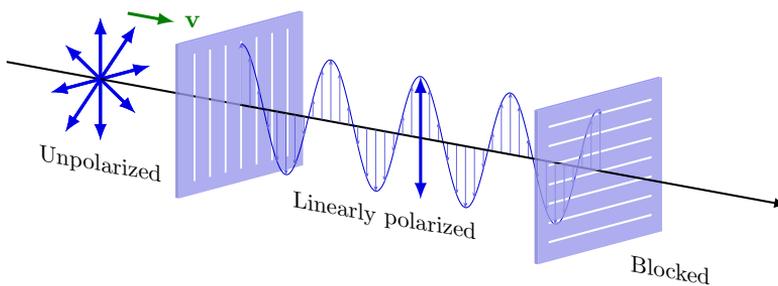


Figure 3.5: Specific polarizing filters are used to generate the desired polarization [9] [10].

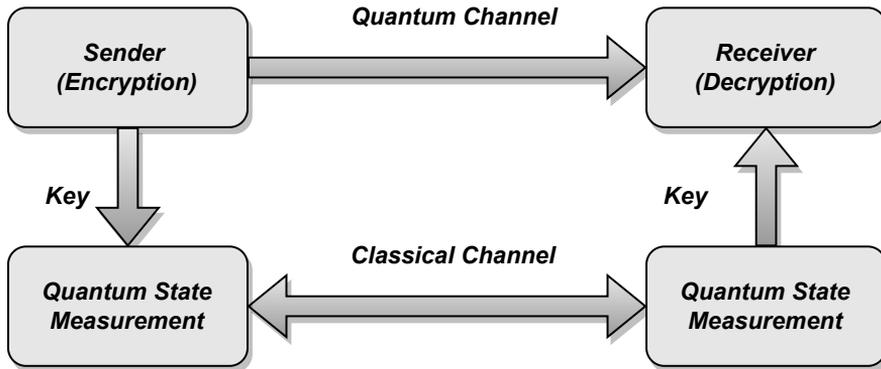


Figure 3.6: Diagram that summarizes the phases of the BB84 protocol.

The steps that characterize the BB84 protocol are described as follows:

1. Alice and Bob have to first agree on how bits will be encoded in the polarization directions for each filter.
2. In the modulation phase, Alice generates a uniform random bit string that constitutes her raw data. Then selects a sequence of random polarization filters with diagonal and rectilinear polarization. Hence, each bit, which represents one of two orthogonal states chosen, is encoded in one of two randomly chosen non-orthogonal bases [239].
3. Alice sends the resulting train of polarized photons to Bob.
4. Bob chooses, independently and randomly for each photon, a sequence of reading bases. He reads the photons accordingly, recording the results in two tables, one of rectilinearly received photons and one of diagonally received photons. Because of losses in his detectors and in the transmission channel, some of the photons may not be received at all, resulting in holes in his tables.
5. At this time, Bob makes his guess as to which basis Alice used, and announces it to Alice.
6. Alice reports to Bob the corresponding results, by telling him which basis she had actually used.

7. After matching, they discard all the bits in which the wrong bases were used and use the remaining data to generate a sifted key. To test for tampering, they compute the Quantum Bit Error Rate (QBER) of a randomly selected subset of data and verify that it is below a certain threshold value [240] [241].

At this point they perform the error correction phase, which consists in the operations of *reconciliation* and *privacy amplification* [242].

The operation of information *reconciliation* consists of generating a classical error correction code:

- Alice and Bob divide the remaining bits of the raw key into subsets of length l , chosen such that there is unlikely to be more than one error per subset.
- For each subset, Alice and Bob perform the parity check (the parity P of a binary string $\{b_1, b_2, \dots, b_l\}$ is defined as $P = b_1 \oplus b_2 \oplus \dots \oplus b_l$), discarding the last bit each time.
- If the parities of a given subset are different between Alice and Bob, they detect and eliminate the erroneous bit through binary search in the following way: divide the subset in two, look for the parities of the new blocks, as follows:

$$P_1 = b_1 \oplus b_2 \oplus \dots \oplus b_{(l-1)/2} \quad (3.1)$$

$$P_2 = b_{((l-1)/2)+1} \oplus b_{((l-1)/2)+2} \oplus \dots \oplus b_{l-1} \quad (3.2)$$

The bisection is repeated on the block where the parities are different, and so on. Each time Alice and Bob delete the last bit of the blocks whose parity is publicly announced, preventing Eve from getting information from their parity checks. Finally, Alice and Bob have the same string of bits.

Privacy amplification reduces Eve's information about the final secret key to arbitrarily small values through the following protocol:

- Considering s as a security parameter and n be the number of remaining bits of the key, Alice and Bob estimate (through the percentage error R) the maximum number k of bits known to Eve and randomly choose $n - k - s$ subsets of their key.
- The parities of these subsets become the *final key*, which is much more secure than the previous one since Eve must know every bit of a subset to obtain information about its parity [238].

3.1.3.2 E91

Another famous DVQKD protocol is the E91 [243], which uses entangled photons in order to guarantee the security of the communication, relying on the no-cloning theorem. Considering that the measurement results performed on the EPR pairs are either completely co-related or completely non-related, it is easy for Alice and Bob to discover any possible eavesdropper. The errors that occur just by default and not because of some eavesdropper, can be corrected to a degree with various techniques. As for the other QKD protocols, the distilled key is a result from a procedure known as privacy amplification [244].

EPR pairs are distributed among communicating partners that choose a measurement basis. If the two partners choose the same basis, the measured bit is considered equal, otherwise the bit is discarded [218] [34].

Specifically, a system that performs the E91 protocol, consists of a source that generates and emits pairs of particles with spin- $\frac{1}{2}$, in a singlet state, as depicted in Fig. 3.7.

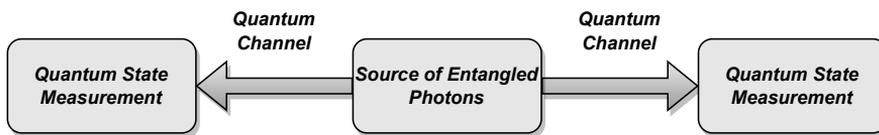


Figure 3.7: Quantum teleportation circuit.

The particles fly apart along the z axis, towards the two legitimate users, Alice and Bob. Once both the users receive the respectively particles, perform measurements on spin components along one of three directions given by unit vectors α_i ; and β_j , ($i, j = 1, 2, 3$), respectively, for Alice and Bob. The α_i and β_j vectors lie in the x - y plane, perpendicular to the trajectory

of the particles, and are characterized by the following azimuthal angles:

$$\phi_1^\alpha = 0 \quad (3.3)$$

$$\phi_2^\alpha = \frac{1}{4}\pi \quad (3.4)$$

$$\phi_3^\alpha = \frac{1}{2}\pi \quad (3.5)$$

and:

$$\phi_1^\alpha = \frac{1}{4}\pi \quad (3.6)$$

$$\phi_2^\alpha = \frac{1}{2}\pi \quad (3.7)$$

$$\phi_3^\alpha = \frac{3}{4}\pi \quad (3.8)$$

The users choose the orientation of the analyzers randomly and independently for each pair of incoming particles. Each measurement, which can potentially reveal one bit of information, yield two results, +1 (spin up) and -1 (spin down). The correlation coefficient of the measurements performed by Alice along α_i and by Bob along β_j , is expressed as follows:

$$E(\alpha_i, \beta_j) = P_{++}(\alpha_i, \beta_j) + P_{--}(\alpha_i, \beta_j) - P_{+-}(\alpha_i, \beta_j) - P_{-+}(\alpha_i, \beta_j) \quad (3.9)$$

The quantities $P_{\pm\pm}(\alpha_i, \beta_j)$ are the probabilities that result ± 1 has been obtained along α_i and along β_j . According to the quantum rules:

$$E(\alpha_i, \beta_j) = -\alpha_i\beta_j \quad (3.10)$$

Considering quantum mechanics, the results obtained for the two pairs

of analyzers of the same orientation ($\alpha_2\beta_1$ and $\alpha_3\beta_2$) are completely uncorrelated:

$$E(\alpha_2, \beta_1) = E(\alpha_3, \beta_2) = -1 \quad (3.11)$$

The following quantity, defined in [245], is the *CHSH inequality*. It is composed of the correlation coefficients for which the involved users applied analyzers of different orientation:

$$S = E(\alpha_1, \beta_1) - E(\alpha_1, \beta_3) + E(\alpha_3, \beta_1) + E(\alpha_3, \beta_3) \quad (3.12)$$

The following result is required:

$$S = -2\sqrt{2} \quad (3.13)$$

After the transmission, Alice and Bob announce the orientations of the analyzers they have chosen for each particular measurement and divide the measurements into three separate groups:

- A group for which they used different orientation of analyzers.
- A second group for which they used the same orientation of their analyzers.
- A third group for which they cannot do any measurement. They discard this group of measurement.

At this point, they reveal publicly the results they obtained within the first group of measurements, which allows them to compute the value of S . If the particles were not directly or indirectly disturbed, the computation should yield the quantity obtained from (3.13). Thereby, users are assured that the results yielded by the second group of measurements are anticorrelated and can be converted into a secret string of bits, i.e., the key.

The eavesdropper cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The useful component of the information is available only after Alice and Bob perform measurements and communicate in public afterwards. The eavesdropper may try to substitute his own prepared data for the legitimate users to misguide them, but as he does not know

which orientation of the analyzers will be chosen for a given pair of particles, there is no good strategy to escape from being detected. The intervention of an eavesdropper implies:

$$-2\sqrt{2} \leq S \leq 2\sqrt{2} \quad (3.14)$$

which contradicts (3.13). Therefore, the generalized Bell's theorem is a fundamental physical law that protects the system, and as long as quantum theory is not refuted as a complete theory the system is secure.

Methods of attacking the system and altering the state of the particles consist on performing a brute measurement of the spin components or substituting a source that produces a state of two correlated particles with another quantum system on which the actual measurement will be performed by the eavesdropper [243] [240].

3.1.4 Quantum Bit Error Rate

The QBER, is defined as the number of different bits shared by the two entities in communication over the total bits exchanged:

$$QBER = \frac{\bar{p}}{p + \bar{p}} \quad (3.15)$$

where p is the probability of sharing the same bit and \bar{p} is the probability of the two systems not sharing the same bit [246]. The generated encryption key is considered acceptable if this parameter is below a specific threshold [247], which depends on if the *advantage distillation*. The advantage distillation is a procedure, which uses a two-way classical communication to select parts of the raw key with a high correlation is used or not. The procedure consists of classically post-process the obtained raw key in order to increase the correlation between the two communication systems. In this manner, it is possible to obtain an advantage over the eavesdropper [248]. For instance, an implementation of the BB84 protocol subjected to depolarizing noise without advantage distillation can tolerate up to 11 % QBER. However, if the advantage distillation is performed, the noise tolerance can be increased to 20 % QBER [249]. However, if this parameter exceeds a certain threshold, it doesn't only mean that the channel is too disturbed to

generate a secure key. In fact, high QBER values may also indicate that key generation has been disturbed by an eavesdropper [250].

3.2 Feasibility Studies for Satellite Quantum Networks

Despite the fact that a constellation composed of quantum satellites has not yet been launched, some models and frameworks aimed at understanding the performance currently achievable and providing some guidelines regarding the design have already been made. The studies that have been conducted are not limited to an analysis of the inter-satellite link, but they also propose different architectures.

In [251] a rate calculation for a repeater architecture described in Fig. 4.10a has been performed. In this type of architecture, many satellites disseminate Bell pairs between the GSs, and the entanglement can be extended by performing the entanglement swapping on the GSs themselves [252]. In particular, they have evaluated the daily entanglement rate by varying the distance between GSs from 4000 to 20000 *km* considering from 4 to 8 inter-satellite links. In addition, the daily entanglement rate at 20000 *km* distance has been measured by varying the memory efficiency, always considering a different number of links. Finally, the rate has also been evaluated considering the Quantum Nondemolition Detectors (QND) efficiency under the same operating conditions. As explained in [253], the objective is to implement measurement schemes in which feedback noise is not coupled to the quantity of interest. This quantity then is not affected by the measurement process, allowing repeated measurement operations that can be performed with extremely high precision.

In [16], they studied different approaches for global quantum networking considering space and ground networks scenarios. In order to connect two GSs, they considered satellites equipped with QMs, which operate as QRs deployed in free-space. This research group implemented MA measurement-device independent QKD (MA-QKD) protocols to achieve high rates and device-independent security onboard satellites in a LOS setting. They confirm that the deployment of QRs in space allows achieving better performance in terms of entanglement rates on a global scale w.r.t. other solutions. They have analyzed a Vienna-Sydney link separated by nine GSs considering different weather conditions and effects. The results show that considering

these effects the solution shown in Fig. 4.10a is impractical w.r.t. the solution depicted in Fig. 4.10b. The paper also investigates the impact of losses considering different kinds of QMs and efficiency values.

An attempt to provide some guidelines for the creation of a quantum satellite network was made in [254]. The paper states that the future global QNs could consist of subnets of LEO satellites, connected in turn to a network of Medium Earth Orbit (MEO) and Geostationary Earth Orbit (GEO) satellites. Specifically, this network can be of fundamental importance in scenarios that consider the IoT architectures, which comprise widely distributed nodes connected via different types of channels to enable new functionalities in communication, sensing, and computing and require a high level of security.

Such architectures that include the use of multiple constellations have also been considered in other studies. For instance, in [74] a double-layer quantum satellite network architecture has been proposed. In particular, this study, in addition to proposing a double layer architecture consisting of GEO and LEO satellites also proposes a Joint GEO-LEO Routing and Key Allocation algorithm specifically designed to resolve the E2E key distribution problem. Specifically, they obtained the results considering a scenario composed of 66 LEO satellites, 3 GEO, and 25 GSs distributed across Earth.

3.3 Software-Defined Networking Satellite Backbones

The studies that have been explained in Section 3.2 do not consider the use of SDN technology, which as described in [14], proves to be very useful in the management of QNs. In fact, as mentioned in Section 4.4, the SDN Controller, having complete control of the network, can manage the creation of the Bell pairs in an effective manner on the entire E2E path.

Considering that quantum satellites can be used to generate secret keys for terrestrial nodes, in [255] is proposed a network architecture managed by SDN Controllers on the ground with different roles, which are interfaced to the LEO satellite network composed of quantum satellites through a network of GEO satellites in order to effectively distribute quantum keys. They have simulated and verified the performance of different QKD constellations considering a specific Routing and Resource Allocation in Free Space QKD (RRA-FSQKD) algorithm. Their results show that the key relay perfor-

mance of the constellation is related to the form of an inter-satellite link. Furthermore, the success probability of the constellation increases considering the existence of satellites in different orbital planes. When there are only satellites in the same plane, satellites deployed in different orbits cannot perform key distribution, and the number of satellite orbits has a significant impact on system performance.

The quantum satellite backbones can improve existing and enable new applications. In fact, many applications for the QI are still unknown. Nevertheless, some possible applications of QI can already be identified and classified [256]. This Section describes some possible applications that could be enabled by the described architectures, along with related experiments.

3.4 Satellite QKD Experiments

Security has been an important area in research, engineering, and operations for the classical Internet [257]. The current online services store or transfer users' sensitive information, which represents a key target for hackers. Furthermore, many organizations and companies can also be affected by cyber-attacks that can cause significant economic losses [258]. In order to deal with these attacks, a classical network security system typically relies on multiple layers of protection and consists of different components, including networking monitoring and security software along with specific hardware and appliances [259]. Nevertheless, the advancement of quantum computing technologies also makes it necessary to study new technologies in the area of network security. In fact, with a QC it is possible to solve the prime-number factorization problem exponentially faster w.r.t. a classical computer [260]. Even if quantum computing is not yet a consolidated reality, some experiments have been conducted in several laboratories with success [9]. In order to address these problems Quantum cryptography has been considered and it has already been tested in the FSO context [261]. As explained in [260], many experiments have been carried out for satellite QKD, considering the reasons explained in Section 4.3.1.

An Italian research group built an experiment that mimics a single photon source on a satellite, exploiting the telescope at the Matera Laser Ranging Observatory of the Italian Space Agency in order to detect transmitted photons and verify the possibility of establishing a quantum channel between Earth and a single satellite. The LEO satellite Ajisai, which orbit has a

perigee height of 1485 *km* has been used in order to simulate a single-photon source on a satellite using the retroreflection of a weak laser pulse from a Satellite Laser Ranging (SLR). In particular, it has been observed the number of detected photons per second, i.e., the Detector Count Rate (DCR), which constitutes an initial step toward the measurement of the individual photons in quantum communication [262].

Furthermore, in [114] an Italian research group has demonstrated that it is possible to preserve the polarization of a single photon over a satellite-to-ground channel. In order to measure two different polarizations they used two single-photon detectors at the receiver, and they derived the QBER. The study analyzes four specific 10 *s* intervals considering four different polarization input states and shows four histograms of the obtained counts at the receiver for each single-photon detector as a function of the detection time. Furthermore, the bare QBER and the QBER calculated after the background subtraction for each of the four considered satellites are shown. This study demonstrates the feasibility of the BB84 protocol from satellite to ground, which requires an average QBER below 11 %. Finally, detection rates and link budgets for each satellite have been considered.

The launch of the Micius satellite in 2016, which orbits at an altitude of 500 *km*, enabled many experiments to be performed. Five GSs for optical communications have been built in different locations in China in order to perform the experiments [263]. As described in [264], in a joint experiment involving Chinese and Austrian researchers a quantum communication between multiple locations on Earth at a continental scale distance of maximum 7600 *km* has been demonstrated. Specifically, in the experiments that followed, some photos were transmitted and a video conference lasting 75 *min* was also held.

As reported in [265], the key rate that can be achieved through the Micius satellite in a satellite to ground communication considering a distance of 1200 *km* is of the order of kilohertz, which is about 20 times the order of magnitude achievable with fiber optics. This study evaluates the sifted key rate and the QBER as a function of time and physical distance between the satellite and the GS. Finally, the efficiency of the satellite link is compared with a terrestrial optical fiber link. In the satellite case, the link efficiencies have been calculated by dividing the intensity of the photons arrived at the GS detector with that measured at the output of the satellite transmitter. The result is consistent with other data reported in the experiment,

confirming the higher efficiency of the satellite link.

In the experiment described in [266], they have demonstrated the distribution of two entangled photons from a satellite to two GSs at a distance of 1203 *km*, considering the scheme described in Fig. 4.10a, and they have observed the survival of the entangled particles. This result is significant because it demonstrates the viability in implementing entangled-based QKD protocols such as the E91, which is described in [243].

In [267], the feasibility of a satellite ground link through the use of CVQKD technology has been analyzed. They obtained the probability distribution of the transmission efficiency of the quantum channel, from which they derived the secret key generation rate in different cases. Considering the channel fluctuations, which are typical of satellite communications, a method of data analysis based on orbit subdivision has been proposed. The analysis shows that coherent state modulation and detection is a viable option for quantum communication with LEO satellites. The communication with higher orbits, achievable in the asymptotic limit, can be affected by finite-size effects if the transmission rate is low or the orbit subdivision is not optimized. Nevertheless, by merging multiple satellites passes, it would be possible to extend the communication range beyond 2000 *km*.

Although the experiments conducted so far show the feasibility of these technologies, many problems remain open. Considering that these QR systems are also equipped with classic components and interfaces, the most critical issues concern the classical parts of the system. Specific attacks that involve quantum and classical parts must be considered for designing new architectures as robust as possible [257].

3.5 Distributed Computing and Quantum Cloud

Considering the extraordinary development of QCs that has recently occurred, it is possible that the security of the current Cloud systems would become compromised. In fact, given their high computational capacity, these systems are able to easily bypass current security measures [268]. For this reason, it is necessary to design new Cloud systems that include the use of QCs and quantum communication technologies in order to resist any potential attacks.

In [269] the constituent elements of a Quantum Cloud system are described. In particular, it is composed of the following elements:

- The quantum hardware that contains the fundamental elements that compose the quantum computer, i.e. the qubits. These elements can be made using different technologies.
- The control system that contains the elements necessary to operate the quantum hardware in order to guide its evolution and retrieve the final result.
- The executor that orchestrates the control system to run quantum programs and return measurement results to the user.
- The compiler that considering the quantum programs produces instrument binaries for the executor.

As explained in [111] and [270], a network of quantum nodes which comprises k nodes each with n quantum bits has a state space of dimension 2^{kn} . Hence, if we consider k remote QCs, by devoting at least one qubit at each device for the teleporting process, a virtual quantum device consisting of up to $kn - k$ qubits is obtained. The operations must be properly orchestrated between the single devices and considering this, an initial architectural scheme for distributed computing has been provided in [11]. As can be seen from Fig. 3.8, the lowest level consists of quantum processors, repeaters, and the classical and quantum channels. The Virtual Quantum Processor (VQP) acts as an interface for the Distributed Quantum Compiler (DQC). The DQC optimizes the circuit so that it can be executed, independently of the underlying network type. It maps a quantum algorithm into a sequence of local and remote operations, optimizing the available computing resources considering the hardware and the network constraints. The DQC could interface with an SDN Controller that performs the operations described in some experiments shown in the previous Section [20] [21] [22]. This peculiarity could be fundamental especially if we consider a time-varying network as in a satellite scenario. Moreover, thanks to the control obtained through the use of SDN technology, it is possible to optimize the paths in order to better manage the operations of entanglement generation between remote QCs so as to exploit fully and efficiently the space of states that is obtained by joining multiple quantum devices. In fact, as illustrated in [118], the ultimate goal is to interconnect clusters of QCs, i.e. different QDCs. However, to achieve this goal, it is necessary to have tight control over the network, which could include mixed scenarios, both terrestrial and satellite, and different technologies used in the creation of classical and quantum hardware.

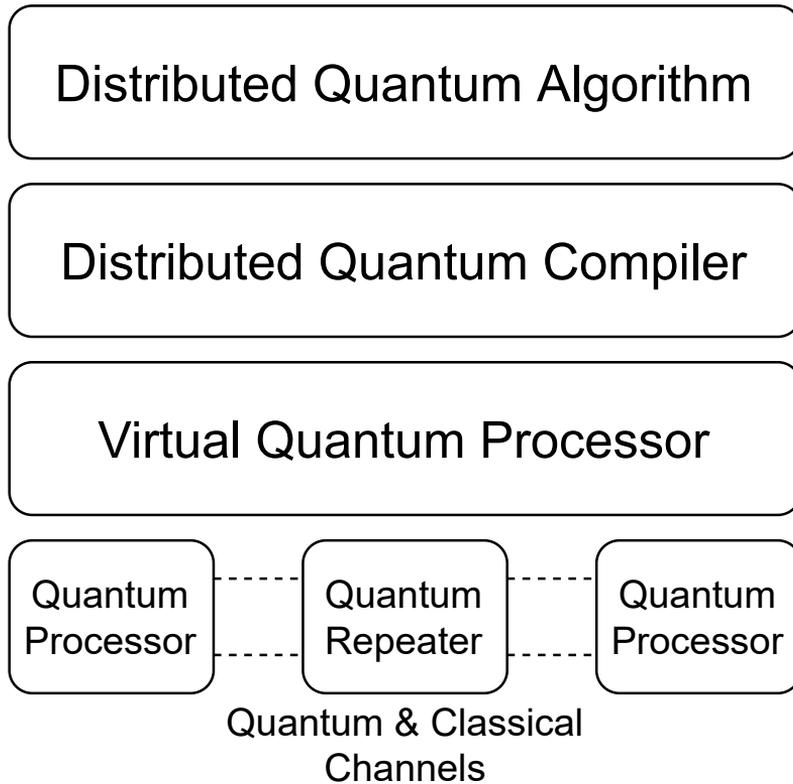


Figure 3.8: Logical scheme of the distributed quantum computing ecosystem described in [11].

Specifically, the interconnection of multiple QCs in an urban environment could be accomplished through existing fiber optic segments, but the interconnection of multiple geographically distributed QDCs that work in a coordinated manner could be performed thanks to the use of architectures described in Section 3.3 that use the capabilities of SDN technology.

Other studies have been done in an attempt to analyze and define a quantum Cloud architecture [271]. Many of them are aimed at using quantum technologies to secure Cloud systems [272]. The objective of the proposed model is to authenticate the users in the Cloud using quantum cryptography. Specifically, they have analyzed the performance of the BB84 protocol in order to establish a secured quantum channel.

Although a definitive architecture for a quantum Cloud system does not yet exist, in [273] a QNs security framework is proposed. The paper proposes an application of a Quantum Key model in order to increase the security of the system. Specifically, it introduces a secure key layer, which acts as a middle-man between the host kernel and containers. Furthermore, the introduction of quantum keys can further improve system security. The levels consist of control between containers and container daemons, ad hoc network links among servers within a Data Center and among servers in different Data Centers. When a container starts and an image is extracted from the Docker daemon, it will run, by default, in a mode that has limited privileges. Then, the container and the associated applications have limited capabilities in order to access resources in the host kernel. However, if root privileges are requested by an application, a request is sent through a classical channel between the host server and the Quantum server. The Daemon sends requests to the Quantum server for different applications like routing, file modifications, and networking. The system considered in [273] works considering the principles described in Section 2.1 as follows:

1. A Quantum Server includes an EPR source, which generates EPR pairs.
2. The EPR pairs are exchanged between the Quantum Server and the host server.
3. The part of the EPR pair that remains on the QS interacts with the information qubit.
4. The key data are converted to quantum information qubits by Quantum Encryptors.
5. The created qubit's secure key is used in order to establish secure communication.
6. Root privileges are assigned to containers for which the keys have been successfully created.

The study also states that it is necessary to develop additional algorithms for an efficient update of the QNs topology, and routing tables, also considering the distributed EPR pairs among QCs. Furthermore, it is also necessary to develop purification protocols in order to also consider other issues such as fragility, the quantum noise [274], and decoherence typically associated with quantum data.

3.6 Positioning

Timing accuracy is a key resource for financial applications considering that transactions must be settled with a microsecond accuracy [275]. However, one of the most useful applications in both the civilian and military sectors is navigation, considering the direct correspondence with precision in applications such as the Global Positioning System (GPS). In [12] an approach to maximize the performance of a network composed of multiple clocks has been considered.

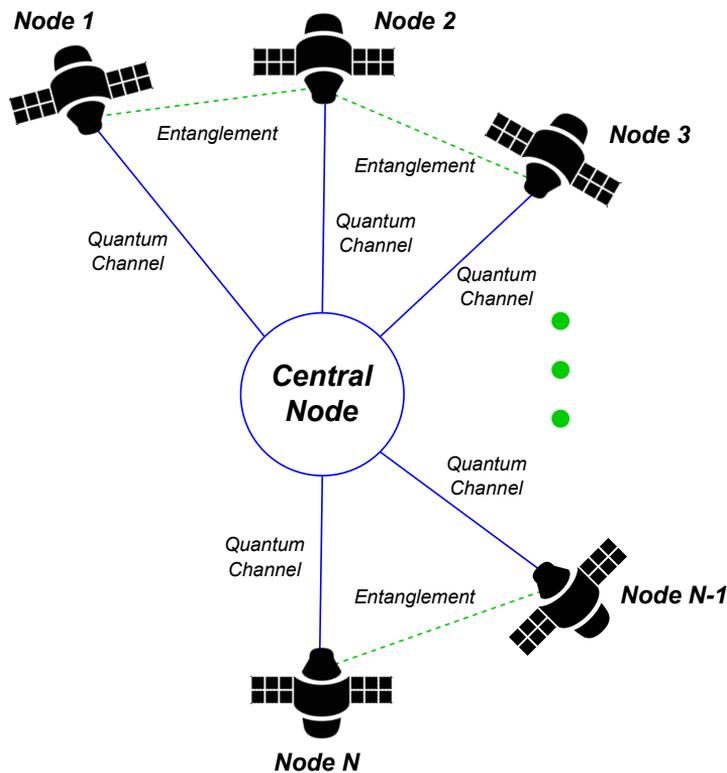


Figure 3.9: Schematic representation of the network proposed in [12]. The satellites employ network-wide entangled states to interrogate their Local Oscillators (LOs) and they send the information to a specific central node. In this manner, it is possible to obtain an extremely accurate clock signal available to all.

The strength of this approach lies in the possibility of taking advantage of all the resources on each node. A distributed network composed of quantum-limited clocks separated by large distances, for instance, for satellite-based clocks can be managed as a world clock, where all members combine their individual resources in a quantum coherent manner in order to achieve greater clock stability and distribute this international time scale in real-time. In order to achieve this result, it is necessary to combine the technologies of modern atomic clocks that use highly phase-coherent lasers with quantum communication techniques that are based on the phenomenon of quantum entanglement, which enables distant quantum objects to be connected in QNs. This approach has already been considered in single atomic clocks to improve their performance [276].

In this distributed architecture, the stability of the local clock signal of each participant that is part of the network is enhanced by a factor, which is proportional to the total number of parties without compromising security or sovereignty. With the use of quantum communication techniques, the system achieves the highest possible security level, considering that only parties contributing to its operation takes the benefits of an extremely accurate clock signal. A set of N atomic clocks that compose the nodes of the network are considered. Each node is based on a large number of atoms, i.e. clock qubits, serving as a specific frequency reference at different geographical locations. Each clock has its own independent LO. The qubits are periodically queried and the measurement data are used to stabilize the LO frequency at the reference frequency of the atomic transition keeps the time by interrogating its qubits periodically. Each node that composes the network allocates some of its qubits to form entangled states stretching across all the other nodes. As depicted in Fig. 3.9, the acquired information is sent to a particular node, serving as a center, where it is used to stabilize a center-of-mass mode of the different LOs. When queried within a properly designed measurement scheme, such entangled network states provide extremely accurate information about the deviation of the center-of-mass of all local oscillators from the atomic resonance. Hence, a clock cycle consists of three phases:

- Initialization: preparation of the clock atom state.
- Measurement: interrogation by the LOs.
- Feedback: correction of the laser frequency according to the measurement outcome.

After a few cycles, the LOs corresponding to each individual node achieve an accuracy and stability effectively resulting from interrogating atoms in the entire network.

In addition to serving as a real-time clock for the international time scale, the proposed QNs is a large-scale quantum sensor that can be used to probe the fundamental laws of physics, allowing to better understand relativity and the laws governing space-time and quantum physics.

The QPS, for the first time proposed in [124], can significantly improve the position accuracy of the traditional GNSS as required by the new location applications. GNSS systems provide several location services aimed to find the position and navigation of vehicles on the roads, in the sea, in the air, and for agriculture by using a constellation of satellites providing signals from space that transmit positioning and timing data to GNSS receivers. Starting from the well-known GPS launched by the US Defense Department for military purposes and then extended to civil operations, the vehicles (i.e., the GPS receiver on the board) can determine the position by measuring the Time Of Arrival (TOA) of the different signals received from four satellites, and automatically calculate the longitude and latitude of the vehicles. Despite the extensive coverage of GPS, the position information cannot provide continuously due to the occlusion of signals, for example, in urban environments and with an accuracy of about 5 m in the best case. Moreover, security issues can occur as the signal can be overwritten or eavesdropped. The QPS improves the localization accuracy by a value equal to \sqrt{MN} , where M is the number of frequency-entangled pulses and the factor \sqrt{N} is obtained by employing squeezed pulses of N quanta [277] [278]. Moreover, the no-cloning theorem of the quantum signal ensures intrinsically the security of the positioning system.

An interesting review on QPS can be found in [279], which introduces the main concepts of a quantum navigation system from the aspects of quantum navigation classification, core technology, and development trend. A QPS, which requires optical communication and Acquisition, Tracking, and Aiming (ATP) techniques, uses the same technologies commonly used in classical satellite laser communications already consolidated. In a QPS, the positioning and clock synchronization processed are independent. The clock difference between the user clock and the system clock, which are located near the origin of the coordinate system, is accurately measured through the second-order quantum coherence. The user clock is synchronized to the

system clock, and clock synchronization has only short-term stability requirements for both the clocks, considering that the two-photon coincidence count measurement of the Hong-on-Mandel (HOM) interferometer [280] [281] only requires the clock to remain stable for a short measurement period.

Moreover, some guidelines for designing a QPS are described in [282]. The quantum active navigation system uses satellites as the signal source for transmitting and receiving quantum signals. The quantum localization system is composed of three main parts: ground unit, satellite system, and user. The QPS architecture needs two satellites at low orbit for each direction of a coordinate perpendicular system where the Earth center is in the origin. For each direction X, Y, Z a light source transmits towards the two satellites which reflect the signal to the user. Adjusting an optical delay unit the dual photons can reach the user's interferometer at the same time. Finally, knowing the distance between the satellites and the delay the position of a user can be determined [279] [282].

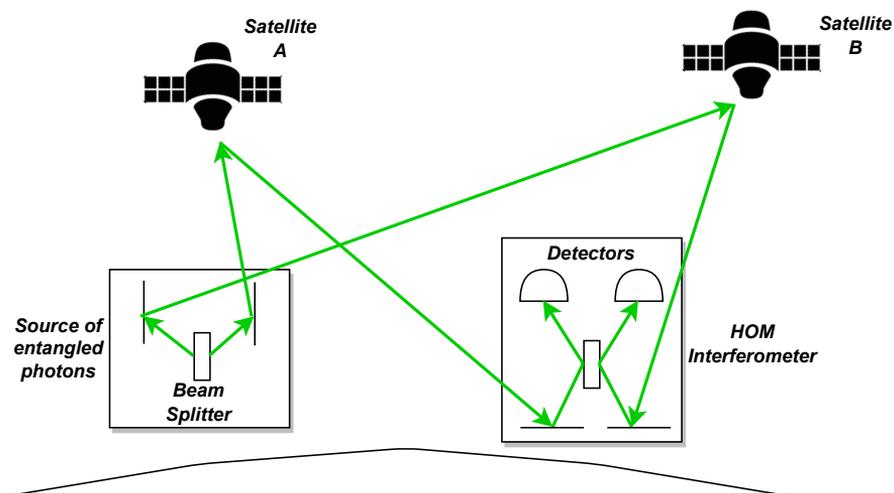


Figure 3.10: Schematic representation of a QPS.

The QPS practical implementation is mainly influenced by the preparation of photons entangled states, efficient detection of photon detectors close to 100 %. Furthermore, the attenuation of the atmosphere has a significant impact on about 10 km above the Earth surface, influencing the position

of ground users. However, it is not so relevant for the positioning of the spacecraft. Finally, a QPS requires the maintaining of HOM interferometer stability only for a short measurement period, while traditional location systems need to maintain the stability of the clock synchronization for longer periods of time.

3.7 Sensing

High sensitivity sensing refers to applications that leverage quantum phenomena to achieve reliable nanoscale sensing of physical magnitudes. For example, [283] uses an entangled QN for measuring the average phase shift among multiple distributed nodes. Spatially distributed sensing of parameters at multiple locations in a network is relevant for applications from local beam tracking to global-scale clock synchronization. The development of QNs enables new strategies for achieving enhanced performance in such sce-

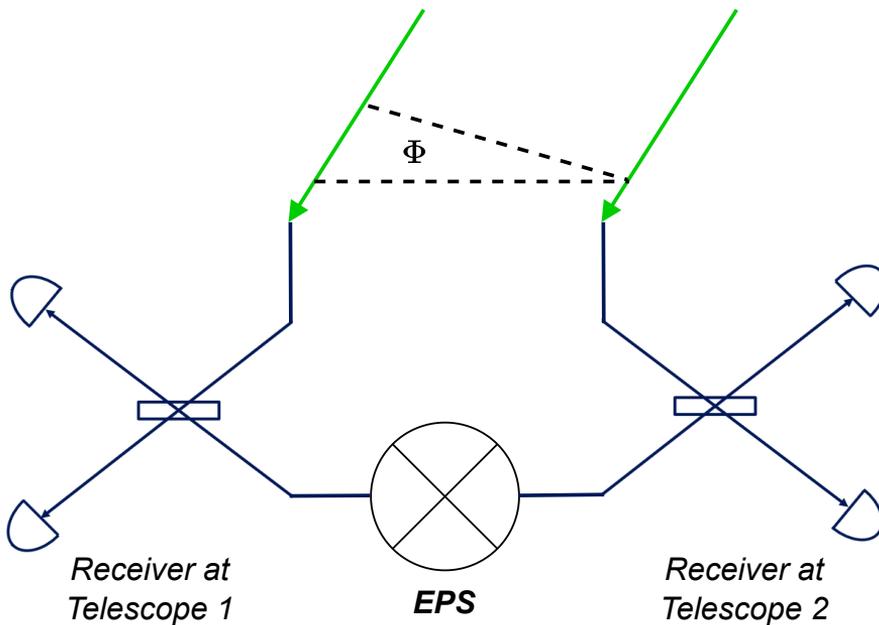


Figure 3.11: Interference measurement between two telescopes using an entangled state emitted from a central Entangled Photon Source (EPS).

narios. Theoretical works have shown that entanglement can improve sensing capabilities in a network using either twin photons or GHZ states combined with photon number-resolving detectors or using continuous variable entanglement for the detection of distributed phase space displacements.

Interferometric techniques are used to combine signals from two or more telescopes to obtain measurements with higher resolution than what could be obtained with either telescope individually. It can make measurements of very small astronomical objects if phase fluctuations and photon loss introduced by the communication channel between the telescopes put a limitation on the baseline lengths of the optical interferometers. This limitation can be potentially avoided using quantum teleportation. In general, by sharing EPR-pairs using QRs, the optical interferometers can communicate photons over long distances, providing arbitrarily long baselines [132].

3.8 Drones

Considering that using OFs, a significant fraction of the photons scatter before reaching the receiver, it is necessary to evaluate different communication media. In particular, free-space quantum communication through drones equipped with quantum hardware has been proposed in [103]. A network constituted by quantum drones is an easily disposable on-demand solution to cover limited areas where ad hoc quantum computation could be requested. This solution also allows overcoming the static deployment typical of OFs.

In [107], there is an example of a quantum cryptographic network created using a couple of multi-copter drones. Specifically, it is focused on the development of an optical payload for QKD capable of maintaining pointing between two drones in flight. Moreover, in [284] the air-to-air signal coupling between a couple of drones has been evaluated.

The BB84 QKD protocol has been tested in [108] on a scenario composed of a drone and a GS, measuring the QBER at different distances.

The entangled photons can also be generated onboard drones, as in [103], where the scenario consists of a drone that generates the entangled photons and relays them to a second drone for retransmission to the destination. Furthermore, in [109] the quality of the entanglement states generated by a single drone that connected two GSs has been verified in different daylight and weather conditions.

Compared to the state of the art, this thesis provides some guidelines for designing a network of mobile QRs onboard drones optimizing and controlling its topology on the basis of an objective function related to specific QoS parameters.

3.9 Quantum RADAR

The Quantum Radar process begins with a device that generates a pair of highly correlated entangled photons: an *idler* and a *signal* photon. The idler photon is kept in a quantum memory, i.e., a piece of quantum hardware able to faithfully hold the quantum state of the idler photon, while the signal photon is transmitted toward the some region of space [285]. If a target is present along the transmission path then the signal photon may be reflected back toward the Quantum Radar. At any given time, the Quantum Radar receiver may measure a reflected signal photon or a noise photon from the environment. Because there is no a priori way to distinguish signal photons from noise photons, each received photon is compared to the idler state in the quantum memory. Entanglement correlations eventually allow statistical information from signal photons to be probabilistically distinguished from the noise as the comparison process is integrated over a sequence of many detections.

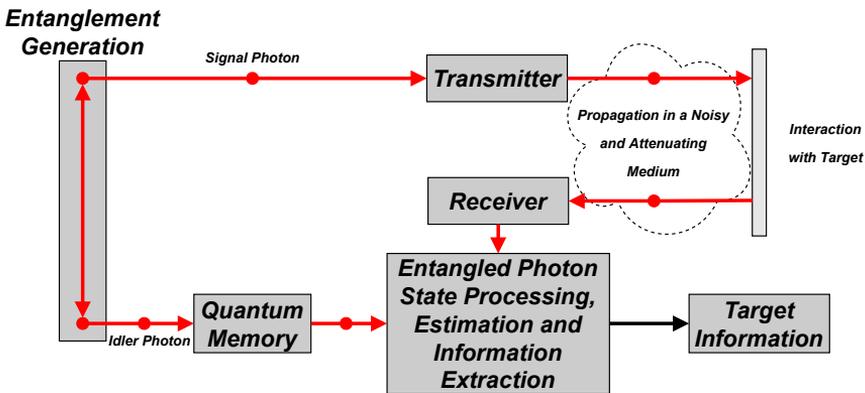


Figure 3.12: Conceptual description of an entanglement-based monostatic standoff Quantum Radar [13].

As quantum entanglement offers an advantage on the small signal-to-

noise regime (approximately from 15 to 20 dB), the applications of quantum radar may be limited to those that require the detection of targets using the minimum amount of energy that is possible. For example, *stealth sensing* for military applications or for *medical imaging* where it is desirable to keep radiation levels to a minimum. On the other hand, if no low energy sensing constraints exist, then classical radar will be preferable to quantum radar. Indeed, in the large signal-to-noise regime, the classical radar will operate with a similar detection probability as quantum radar, but without the enormous technological complexities involved with quantum hardware [13] [286].

Part II

Design and Performance
Analysis

Chapter 4

Quantum Networking

This Chapter describes QNs by considering both the hardware elements required for their operation and the protocol stack. Although the protocol stack has still to be defined, there are some papers in the literature that attempt to define some guidelines for its realization. The Chapter also provides some elements of satellite networks and discusses the possibility of realizing QSNs based on SDN technology. Therefore, the Chapter provides an overview of SDN technology.

4.1 Quantum Networks Elements

The main difference between classical and QNs consists on the services they deliver. Classical networks simply move data from a source application to one or more destination applications over a distance. QNs may likewise transport data from place to place, but they also have the peculiarity to produce distributed entangled quantum states, connecting two or more quantum applications [287] [288]. Therefore, QNs will enhance classical networks and they will require protocols that are completely different w.r.t classical networks. However, these protocol could results even more efficient. This new paradigm enables new possibilities such as distributed quantum computation, quantum secure communications, cloud computing applications, clock synchronisation, and quantum-enhanced measurement networks. These networks, could be easily integrated into existing classical networks, but they require the introduction of new elements. As a matter of fact, the creation of long distance links requires the interconnection of multiple QRs in

a chain [289].

4.1.1 Quantum and Classical Channels

In order to establish communication between two quantum devices, two links are required:

- Quantum links: a link which can be used to generate an entangled pair between two directly connected QRs. It may include a dedicated classical channel that is to be used solely for the purpose of coordinating the entanglement generation on this quantum link.
- Classical links: a link between any node in the network that is capable of carrying classical network traffic.

Indeed, classical communication is still relevant in quantum communications, and in fact the classical channel has the following roles:

- Communicate classical bits of information as part of entanglement swapping and teleportation.
- Communicate control informations. This includes background protocols such as path selection as well as signalling protocols to set up E2E entanglement generation [79].

4.1.2 Quantum Repeaters

QRs are used to transmit quantum information over long distances. These devices are equipped with quantum memories [290]. A network of QRs supports distributed quantum computation by creating high-fidelity E2E Bell pairs. Furthermore, the created entangled pairs can also be used to teleport application data [291].

There are three primary operations that are necessary to create long-range entangled states and are performed by QRs. These operations consist on:

- Entanglement distribution: this operation consists on the creation of entangled links between adjacent nodes.
- Entanglement purification: considering that the created entangled states may not be perfect, this operation allows the creation of entangled states with very high quality.

- Entanglement swapping: the process in which a Bell-state measurement is performed within a node on two qubits which are halves of separate Bell states. The Bell measurement allows the creation of entanglement over distances at which direct transmission is infeasible connecting adjacent repeater nodes [77].

However, a QR will have to do more than just entanglement swapping in a functional quantum network. Specifically, a QR participate in the management of the network such as *path selection* [179].

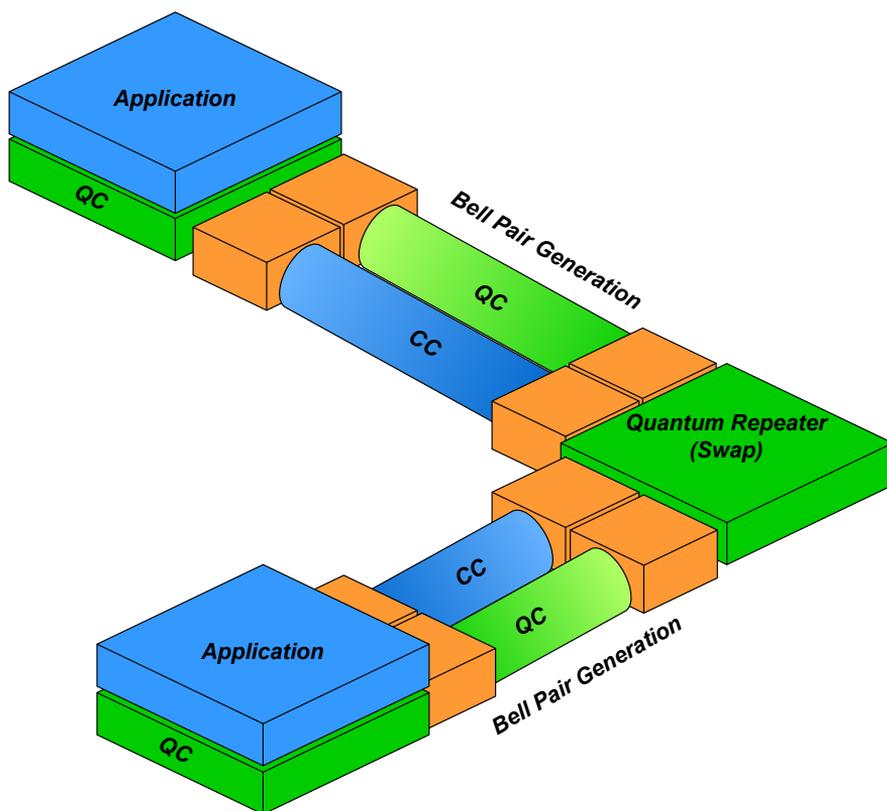


Figure 4.1: A representation of a QN. Two quantum computers are interconnected through a QR. Each device is equipped with a classical and a quantum interface.

4.2 The Quantum Internet Protocol Stack

The QI protocol stack has not been defined yet. However, some examples exist in the literature, such as the one described in [14] and depicted in Fig. 4.2.

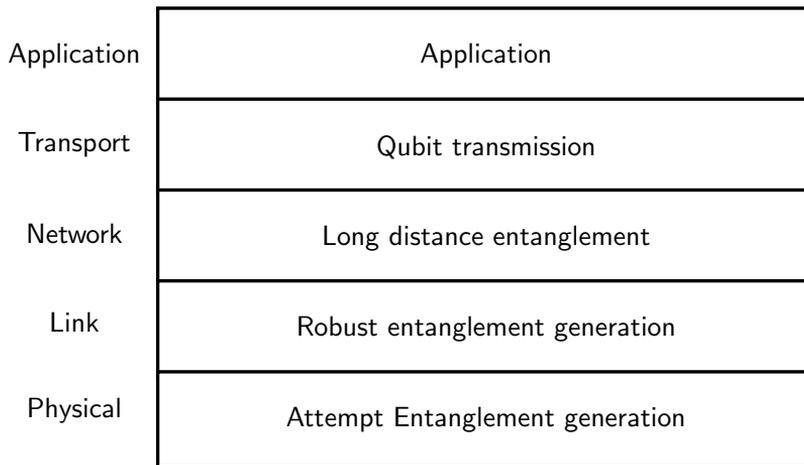


Figure 4.2: A representation of the protocol stack defined in [14].

As can be seen from Fig. 4.2, the number of layers is the same as that of the classical protocol stack, but they have different features. The layers and their functionalities are described as follows.

4.2.1 Physical Layer

The Physical layer corresponds to the actual quantum hardware devices and physical connections. The physical layer keeps no state related to entanglement production, produced entanglement probabilistically, and has no decision making capabilities. The hardware is solely responsible for tasks such as time synchronisation, photon emission, laser phase stabilisation, and so on, that are required to actually produce entangled Bell pairs.

4.2.2 Link Layer

The main task of the link-layer is to utilise the physical layer's ability to produce entanglement between neighbouring nodes reliably. It also integrates the *quantum and classical data planes* providing sufficient information for higher level protocols and network management.

4.2.3 Network Layer

Similar to a network layer in classical networking, the task of the network layer is to enable the generation of entanglement between network nodes which are not directly connected. A protocol to achieve this would utilise the link layer to produce entanglement between neighbouring nodes followed by entanglement swaps to create long distance links.

4.2.4 Transport Layer

The transport layer could provide the additional service of transmitting qubits to the application layer. This could be realised by, for example, pre-generating entangled pairs of qubits using the network layer, followed by teleportation to ensure reliable E2E delivery of qubit [14].

4.2.5 Application Layer

The application may be a sensor network, or a numeric computation or decision algorithm based on shared state. The application will determine if E2E entanglement is required, or if our quantum states can be measured on a pay-as-you-go basis. Some applications may also desire quantum states other than Bell pairs, including any of several common forms of three-party or larger states. Of course, the application is driven by a classical program, presumably using a *socket-like* data structure [292].

4.3 Quantum Satellite Systems

This Section discusses the technological principles for the creation of QSNs. In particular, in addition to explaining the reasons that lead to the use of satellite links, are shown the operations of the basic components and the reasons that lead to the use of SDN technology for the design of these networks.

4.3.1 Motivations

The probability of success in generating entanglement between two adjacent nodes that are at a distance d decreases with an exponential trend:

$$p_s(d) = \frac{1}{2}(p_g\eta_h\eta_t)^2 e^{-\frac{d}{L_a}} \quad (4.1)$$

where p_g is the entangled photons generation probability, while η_h and η_t are the detector efficiencies at herald and telecom wavelength. The first factor $\frac{1}{2}$ means that only two of the four Bell states can be unambiguously identified performing a BSM [293] [66]. L_a is the electric field attenuation length which is the distance at which the electric field is attenuated by a factor of $\frac{1}{e}$ [294].

In order to overcome the distance limit, it is necessary to deploy multiple QRs on the path between transmitter and receiver. Differently from conventional repeaters used in classical communication, QRs cannot clone quantum signals [295]. These devices are equipped with quantum memories, where a quantum state of light is mapped onto an ensemble of atoms and then recovered in its original shape [296].

Considering the results in [66], which show a significant decrease in the rate at the increasing of the distance on paths consisting of optical fibers, deploying a terrestrial QN would require a high number of QRs. Nevertheless, to further increase the distance between two QRs, free-space quantum links have been investigated in recent years, considering that photons experience negligible losses space vacuum. In fact, as shown in [20] despite the strong decay in terms of entanglement rate between two satellite repeaters the distances reached are much more significant compared to fiber optics.

4.3.2 Possible Orbits and Constellations

As described in [297], the path of the satellites is determined by the altitude and the shape of the orbit. In particular, the parameters which define an orbit are eccentricity and inclination [298]. Thus, it is possible to consider the deployment of objects that perform the QR task at different orbits and altitudes.

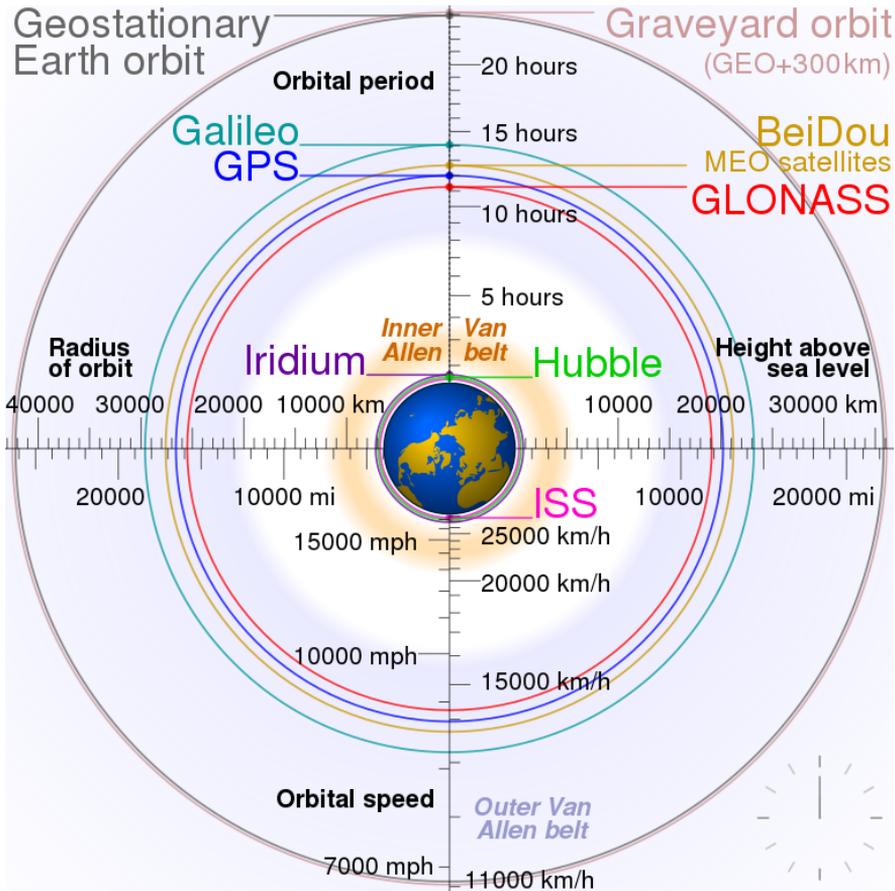


Figure 4.3: Comparison of geostationary Earth orbit with GPS, GLONASS, Galileo and Compass (MEO) satellite navigation system orbits with the International Space Station, Hubble Space Telescope and Iridium constellation orbits, and the nominal size of the Earth. “File:Comparison satellite navigation orbits.svg” by cmglee <https://commons.wikimedia.org/w/index.php?curid=16891766> is licensed under CC BY-SA 3.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/3.0/>

The possible orbits to which satellites can be deployed are described in the following:

- high-Earth orbit satellites, reaching about 36000 km of altitude [299]. The satellites in this orbit are characterized by an orbital period equal

to the sidereal day of Earth following a Geosynchronous Orbit (GSO) and do not necessarily always maintain the same position in the sky. If a GSO satellite is positioned above the Equator (zero inclination), it is referred to as a GEO satellite, and it appears in a fixed position, providing coverage to a specific ground area [297]. A GEO satellite can cover about one third of the surface of Earth, with the exception of the polar regions [300].

- The MEO is located between 2000 and 36000 *km*. This orbit includes satellites for communication, geodetic and space environmental science, and navigation, among which are the GNSS [301].
- The Low Earth Orbit (LEO) is generally considered below 2000 *km* [302]. Considering their proximity to the surface of Earth these objects move at very high speeds between 5 to 10 *km/s* [95] [96], with an orbital period between 90 and 110 [*min*] [303].
- The Highly Elliptical Orbit (HEO) has a perigee below the altitude of 1000 *km* and an apogee which can be above 35000 *km*. HEO orbits are primarily used to provide satellite services to high latitude regions of the Earth, which are difficult to cover with a satellite placed on a GEO orbit [297] [304].

Recently, intermediate layers of communications systems between terrestrial and traditional satellite segments have emerged considering the technological advance of the aerial and miniaturized satellite platforms. These platforms can also be classified according to their operating altitude [300]:

- Very Low Earth Orbit (VLEO) operate at altitudes below 450 *km* [305]. However operating in lower layers of the atmosphere these objects are subjected to much higher aerodynamic forces and therefore a VLEO constellation would require more maintenance [306].
- High Altitude Platforms (HAP) objects can provide communications services at a regional scale. HAPs are typically deployed at an altitude between 18 and 20 *km* and can ensure coverage of a specific area for long periods of time [307]. This operating altitude is chosen because in most regions of the world this represents a layer of relatively mild wind and turbulence above the jet stream [308]. The communication channel of these architectures requires a more in-depth study, even in the classical field [309].

- Low Altitude Platforms (LAP) operate at very low altitudes ranging from tens to hundreds of meters [310]. The LAPs are more economically affordable and can be deployed much more quickly than the HAPs. Furthermore, these objects allow to create multi-tier heterogeneous aerial networks in order to expand the coverage for 5G terrestrial networks and to increase their capacity [311].

In the case of quantum communications, many of these configurations are

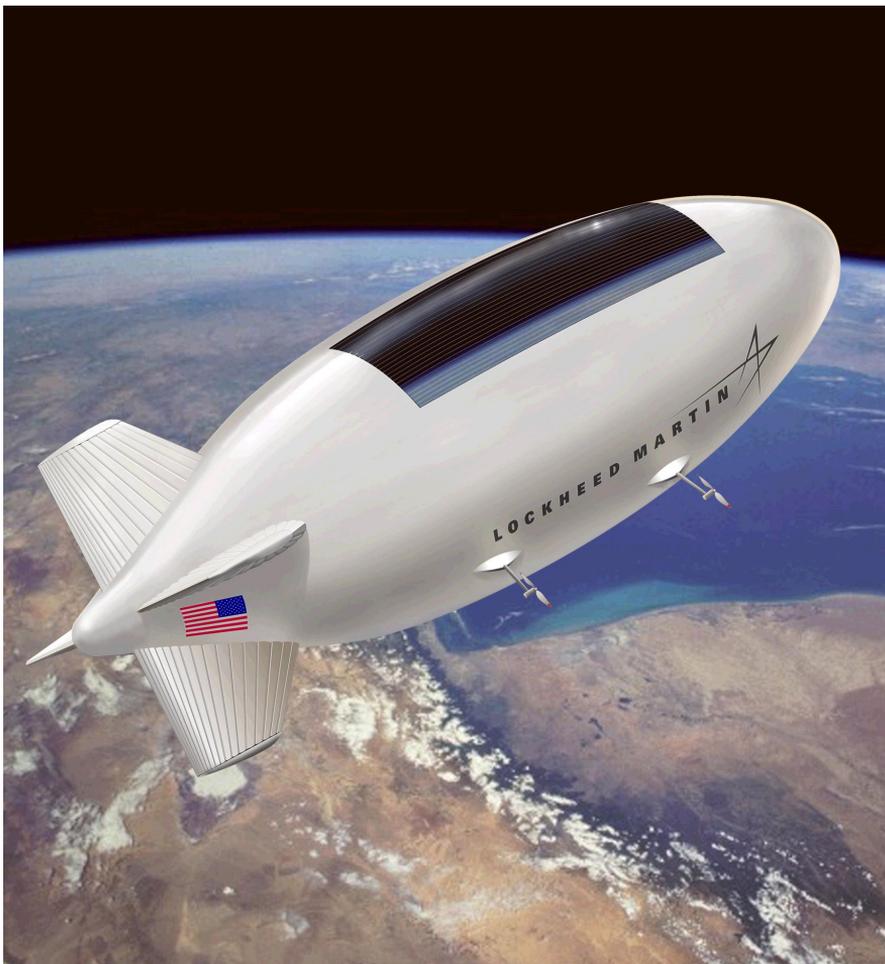


Figure 4.4: High-altitude airship used as HAPs carrier.

still to be studied and need further investigation. However, some studies have already been conducted. In particular in [312], this research group has investigated the use of THz frequencies in order to establish a quantum communication within a constellation of LEO satellites. Furthermore, in [21], which is described in more detail in Section 3.3, the performance of three different constellations, one positioned in MEO orbit and two in LEO orbit, have been analyzed. In this study [313], an estimation of the link budget is carried out considering stratospheric HAPs, and a comparison of the link budget between the various constellations considered in the current Section must also be made, particularly those at very low altitudes. Specifically, in order to ensure the best possible performance on the entire path, it is necessary to investigate the characteristics of the inter-VLEO, inter-HAP, and inter-LAP links, also considering mixed cases.

4.3.3 Device and Components

As explained in [314], in general, a QR must be equipped with two interfaces, an interface for quantum communication in order to exchange Bell pairs and a classic interface dedicated to the traffic exchanged on the classic channel. In [63] it is represented a scheme of a quantum communication system. Specifically, a quantum device consists of a quantum light source and a quantum light detector, both driven by a hardware device driver that is controlled by a general-purpose processor. The quantum light source and detectors are specific semiconductor devices for the generation of entangled photons, which can be realized with different technologies, as discussed in [315]. Therefore, a distributed QC network requires a specific set of memory capabilities: mapping of the light state onto memory, storage and operations on the memory state, and retrieval of the memory state back onto light for further processing [71].

In order to generate the entanglement among multiple devices, there are three schemes, which are described in [316] and [79]. The entanglement generation schemes are depicted in Figs 4.5, 4.6, 4.7 and are described in the following part:

- At mid-point: an entangled photon source is positioned between the two nodes to which it sends the pair of entangled particles.
- At source: in this scheme one of the two nodes sends to the other one a photon, which is entangled with one of the qubits of its memory.

- At both end-points: in this approach both nodes send a photon, which is entangled with one of the qubits of its memory. A detector performs a measurement on the two qubits. In this manner, the remote qubits are projected in an entangled quantum state.

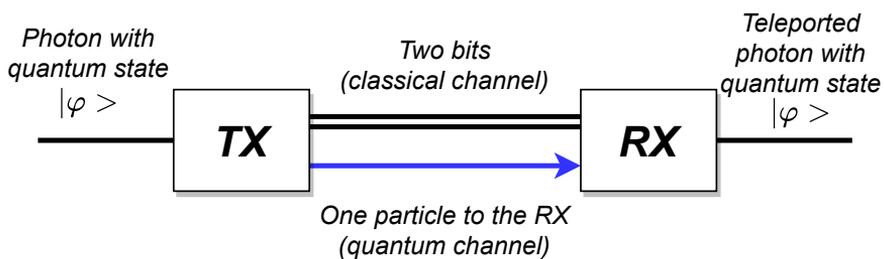


Figure 4.5: At-source strategy. The entangled photon source is integrated into the devices.

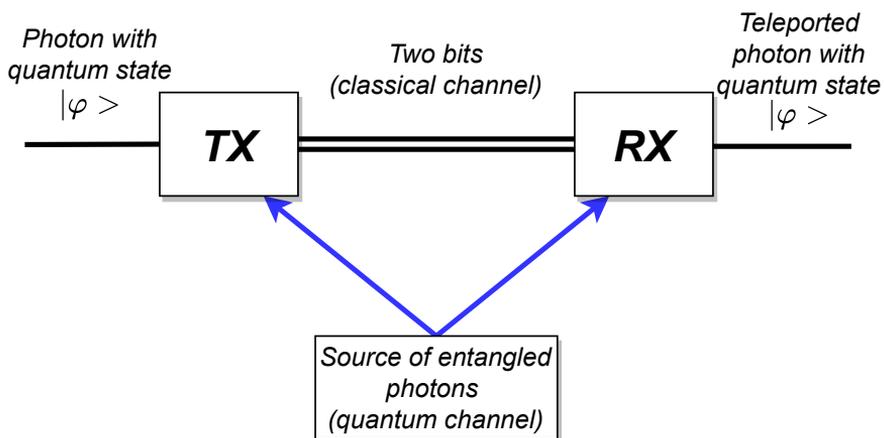


Figure 4.6: At-midpoint strategy. A specific device generates pairs of entangled particles and delivers them to devices that will perform teleportation.

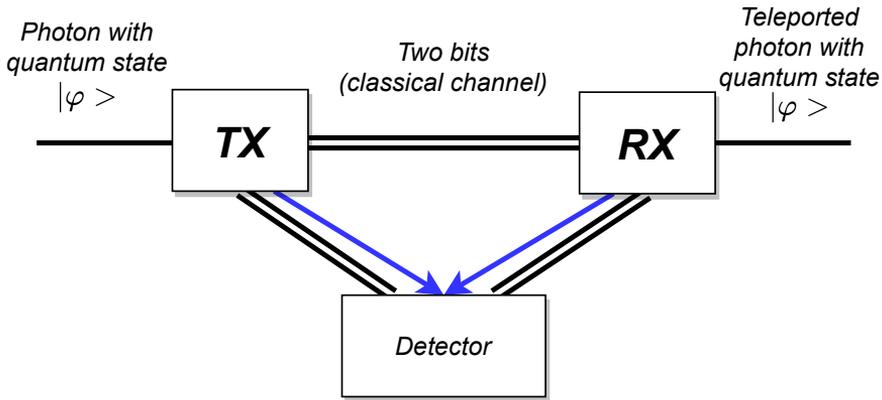


Figure 4.7: At-both-endpoints strategy. A third device performs the measurement of the particles, and entanglement is generated between the involved devices

The strategies At-source and At-midpoint, shown in the Fig. 4.5 and 4.6, are commonly used in the schemes involving the implementation of the E91 protocol [317].

The quantum fidelity describes how close two given quantum states are [180]. Therefore, the quantum fidelity can be used to characterize drastic changes in quantum states when systems undergo QPTs [181] [318]. The decrease in the fidelity of the entangled link means information present in the state has been lost, and when this situation occurs there is not a simple way to recover it [77]. In a QR protocol there are three primary operations required to create the long-range Bell state that can be used for quantum communication tasks such as QKD or teleportation.

- Entanglement distribution: the process through which the entangled links are created between network nodes.
- Entanglement purification: the process through which it is possible to create more highly entangled state from a number of lower quality ones [319] [320].
- Entanglement swapping: the process in which a Bell-state measurement is performed within a node on two qubits which are halves of separate Bell states. The Bell measurement allows us to provide a longer entangled link connecting adjacent repeater nodes.

Considering that the entangled states that result from transmission through a noisy channel are not pure, the Bell pairs must be purified in order to be converted to almost perfectly entangled states. Measurements and local unitary operations are performed on the shared entangled pairs by the two actors, exchanging some classical messages in order to coordinate their actions, and sacrificing some of the entangled pairs to increase the purity of the remaining ones [321]. The resulted Bell pairs are almost perfectly pure and can be used together with classical messages in order to perform the teleportation of the unknown quantum states maintaining high fidelity [319] [322]. In fact, as explained in [323], the deployment of a quantum QR along the path can significantly augment the quantum teleportation fidelity.

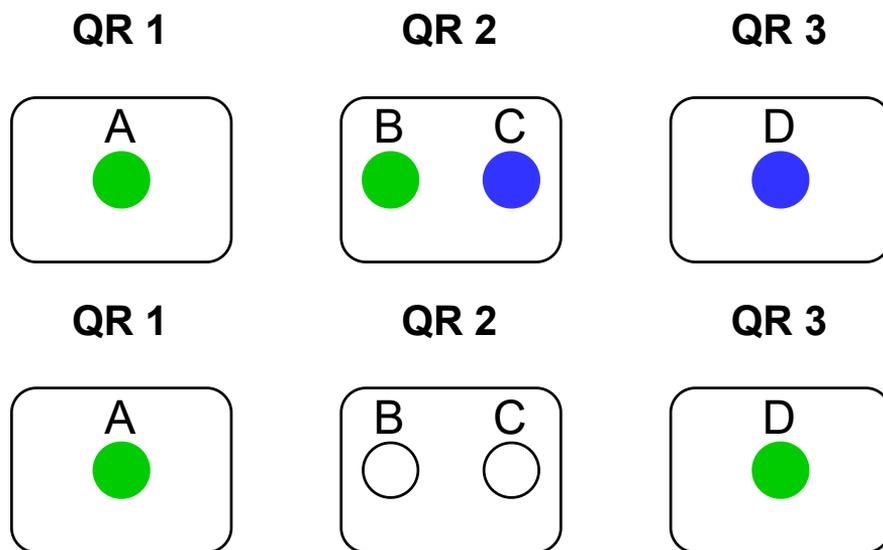


Figure 4.8: Entanglement swapping.

The entanglement swapping operation allows to increase the distance of a quantum communication [324]. As shown in Fig. 4.8, QR 1 and QR 2 share a Bell pair, whereas QR 2 and QR 3 share a different Bell pair. The QR 2 performs a projective measurement on his two particles in the Bell basis and communicates the result to QR 3. This is the teleportation protocol described in Section 2.2.4 with QR 2's first particle, the one entangled with QR 1's particle, as the state to be teleported. When QR 3 finishes the

protocol it now has a particle with the teleported state, that is an entangled state with QR 1's particle. Thus, although QR 1 and QR 3 never interacted with each other, after the swapping operation, their particles result entangled [325] [326]. The operation of entanglement swapping can also be applied to a chain consisting of multiple QRs.

As described in Fig. 4.9, the entanglement generation is performed first between pairs of quantum memories of adjacent nodes via the transmission of photons entangled with the memories [327] [208]. The entanglement swapping is performed at a node that has confirmed the existence of entanglement with other repeater nodes by receiving heralding signals from different repeater nodes at long distances. Then, the involved device selects pairs to teleport and performs a BSM on one qubit of each Bell pair [328] [329]. Hence, quantum memories must be entangled with photons for entanglement generation, and they must preserve the entanglement at least until they receive heralding signals for entanglement swapping from remote nodes [295] [147].

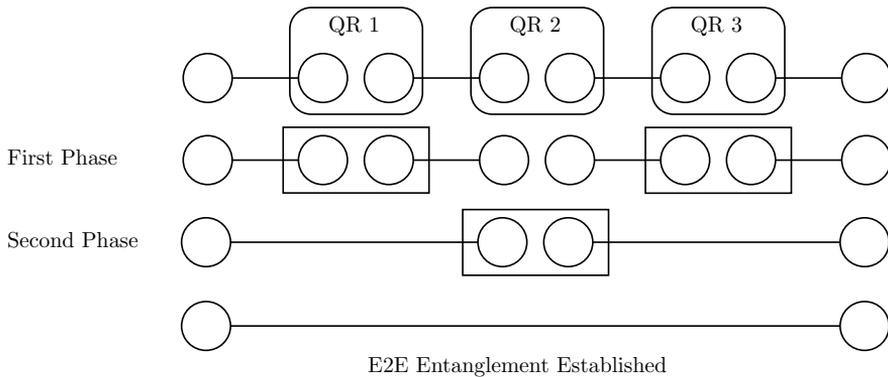
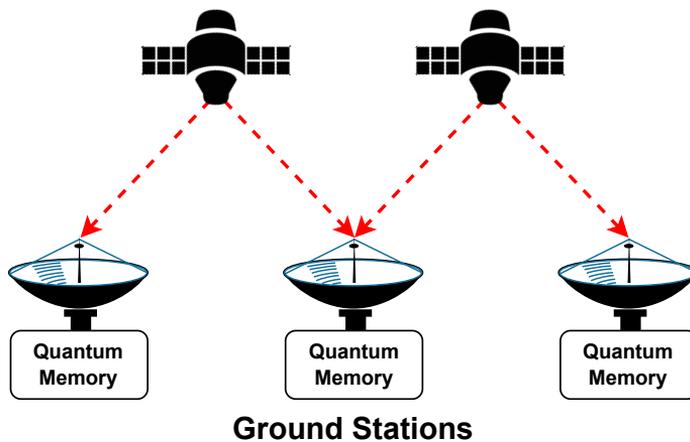


Figure 4.9: The E2E entanglement generation procedure starts with the entanglement generation through transmitting photons between adjacent repeater nodes. Afterward, the entanglement swapping is applied recursively until the E2E entanglement is generated.

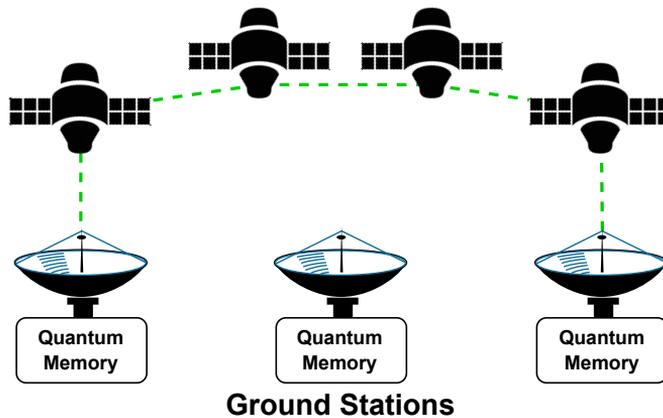
4.3.4 Quantum Repeaters in Space

As explained in Section 4.3.3, QRs are fundamental elements for the interconnection of multiple QCs over large distances. As explained in [14], QR chains have been created by interposing devices at short distances to form so-called trusted repeater or trusted node network [330]. Nevertheless, as

confirmed by [66], in which an attempt to optimize the network is made by proposing a routing algorithm suitably designed for QNs, the performance of optical fibers are acceptable only at distances of a few hundred kilometers. For this reason, satellite quantum communications have been considered.



(a)



(b)

Figure 4.10: In 4.10a each satellite is entangled photon pair source, whereas in 4.10b entanglement sources and QRs are placed on board of satellites [15] [16].

The studies that have been conducted using single satellites show that it is possible to establish a satellite quantum link with better performance than fiber optics. Furthermore, as explained in [331], a satellite-to-satellite link allows to cover larger distances, and it is necessary to perform further experiments.

Considering this, in order to create a global QN is necessary to combine satellite links for very long distances with fiber links for short and intermediate distances [251]. In [15] are examined two schemes, depicted in Fig. 4.10 for the realization of QSNs, which have been considered in the various experiments that are described in this thesis.

4.3.4.1 Free Space Optics

As explained in [332], this type of communication can be performed using FSO technology. The optical radiations can be classified into five categories:

- Near-Infrared (NIR) ranging from 750 to 1450 nm which is a low attenuation window and mainly used for fiber optics.
- Short-Infrared (SIR) ranging from 1400 to 3000 nm out of which 1530–1560 nm is a dominant spectral range for long-distance communication.
- Mid-Infrared (MIR) ranging from 3000 to 8000 nm which is used in military applications for guiding missiles.
- Long-Infrared (LIR) ranging from 8000 nm to 15 μm which is used in thermal imaging.
- Far-Infrared (FIR) which is ranging from 15 μm to 1 mm .

The commercially available FSO systems use NIR and SIR wavelength, which are already used in fiber-optic communications. In particular, using these wavelengths, it is possible to create systems with a high data rate [333].

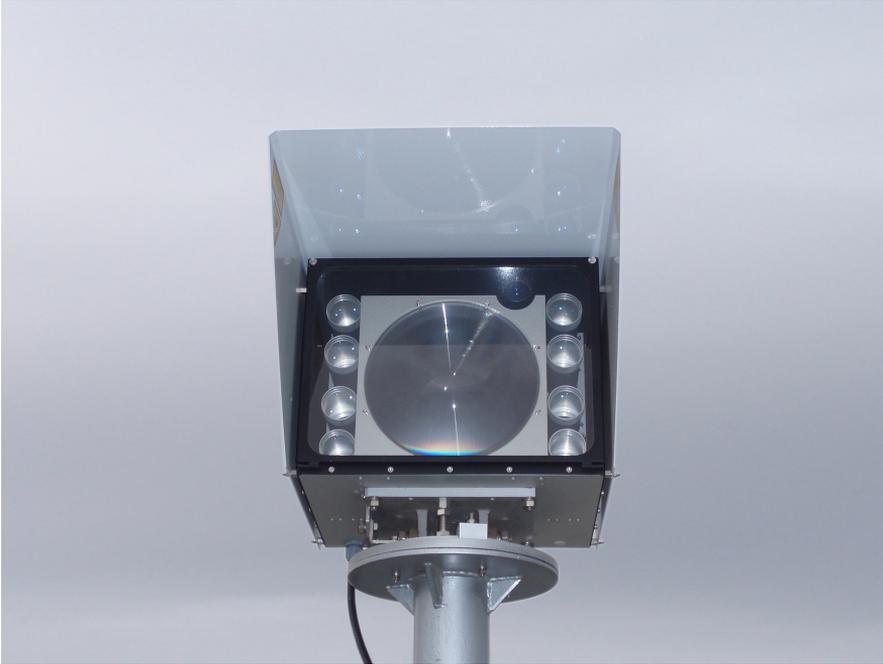


Figure 4.11: An 8-beam free-space optics laser link. The receptor is the large lens in the middle, the transmitters the smaller ones. At the top right corner is a monocular for assisting the alignment of the two heads. “File:FSO-gigabit-laser-link-0a.jpg” by Adamantios <https://commons.wikimedia.org/w/index.php?curid=4792467> is licensed under CC BY-SA 3.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by-sa/3.0/>.

The FSO technology has already been considered for use on CubeSats deployed in LEO orbit [334] and also for communication towards other celestial bodies [335] [336]. Furthermore, the deployment of CubeSats equipped with FSO technology has also been considered in Low Lunar Orbit (LLO) [337]. These satellites may employ specific transmitters that operate at the 1550 nm wavelength [338], which is also ideal for quantum satellite communications [265] [74] [339]. In particular, in [74] [340] wavelengths in the NIR and SIR range equal to 850 nm and 1550 nm respectively for the quantum and classical channels have been considered, given their high efficiency. Moreover, in [341] it has been shown that it is possible to generate a quantum-secure key with a CubeSat of just 4 kg . This result is significant since it indicates

the possibility to deploy QSNs with a small number of launches, significantly limiting costs.

Many experiments have been performed by connecting GSs with single satellites. However, some frameworks for the analysis of satellite constellations have also been developed. In particular, the use of SDN technology for constellation control and management of entanglement generation and swapping operations has also been considered. Furthermore, SDN technology has already been considered for the management of constellations composed of CubeSats [342].

4.4 Software-Defined Networking

Several trends are pushing network providers and users to reassess traditional approaches to network architecture. These tendencies can be categorized into demand, supply, and traffic.

4.4.1 Demand

The load on the Internet is increasing significantly for several reasons. Many of them are the following:

- **Mobile traffic:** Employees are increasingly accessing enterprise network resources via mobile personal devices, such as smartphones, tablets, and notebooks. These devices support sophisticated apps that can consume and generate image and video traffic, placing new burdens on the enterprise network.
- **The IoT:** Many devices in the IoT generate modest traffic, although there are exceptions, such as surveillance video cameras. However, the sheer number of such devices for some enterprises results in a significant load on the enterprise network.
- **Cloud computing:** There has been a dramatic shift by enterprises to both public and private cloud services.
- **Big data:** The processing of huge data sets requires massive parallel processing on thousands of servers, all of which require a degree of interconnection to each other. Therefore, there is a large and constantly growing demand for network capacity within the data center.

4.4.2 Supply

With the increasing demand for networks, the capacity of network technologies to absorb rising loads also increases. The increase in the capacity of network communication technologies has been coupled by an increase in the performance of network devices, such as LAN switches, routers, firewalls, Intrusion Detection System/Intrusion Prevention Systems (IDS/IPS), and network monitoring and management systems. These devices have increased performance during time, such as faster memories, greater buffer capacity, faster buffer access, and faster processor speeds.

4.4.3 Traffic Patterns

If it were simply a matter of supply and demand, it would seem that the existing networks should be able to deal with today's data traffic. However, as traffic patterns have changed and become more complex, traditional enterprise network architectures are increasingly unsuitable for demand. Until today, the typical enterprise network architecture consisted of a local or campus-wide tree structure of Ethernet switches with routers connecting large Ethernet LANs and connecting to the Internet and WAN facilities. This architecture is well adapted to the client/server IT model which was at one point dominant in the enterprise environment. With this model, the interaction, and thus the traffic, took place mainly between a client and a server. In such an environment, networks could be set up and configured with relatively static client and server locations and relatively foreseeable volumes of traffic between clients and servers. Several developments led to significantly more dynamic and complex traffic patterns within enterprise data centers, local and regional corporate networks, and carrier networks. These include the following:

- The currently common practice of virtualization of application and database servers has considerably increased the number of hosts that require high-volume network access and results in an ever-changing physical location of server resources.
- The network convergence of data, voice, and video traffic creates unpredictable traffic patterns, usually of large multimedia data transfers.
- Client/server applications usually access several databases and servers that need to communicate with each other, generating horizontal traffic

between servers and vertical traffic between servers and clients.

- The widespread use of public clouds has shifted a significant amount of what previously had been local traffic onto WANs for many enterprises, resulting in increased and often very unpredictable loads on enterprise routers.
- Unified Communications (UC) strategies involve intensive use of applications that enable access to multiple servers.
- Extensive use of mobile devices, including Bring Your Own Device (BYOD) policies, enables users to access corporate content and applications from any device at any time. The traffic generated by mobile devices is becoming an increasingly significant fraction of enterprise network traffic [343].

4.4.4 SDN Architectural Elements

SDN is a paradigm where a central software program, which is called Controller, determines the overall network behavior. As a matter of fact, the Controller is portable software that can run on commodity servers and is capable of programming the forwarding devices based on a centralized view of the network. In SDN, the network devices that compose the DP are simple packet forwarding devices, while the CP is implemented in a centralized Controller [56] or set of coordinated centralized Controllers. The DP devices can also report network status measures when requested by network applications. Northbound interfaces bind applications in Application plane to the Network Operating Systems (NOS) in the CP, while southbound interfaces provision the control channel for data exchange between NOS and DP devices [344]. The SDN allows overcoming some of the limitations that occur in current network infrastructures. The programmability of an SDN Controller offers network operators and customers comprehensive programming interfaces that can abstract all infrastructure low-level details [345]. Therefore, SDN allows simplifying the enforcement of network forwarding behavior and policies through more expressive high-level policy languages instead of using vendor-specific command sets or proprietary protocols [344]. Specifically, SDN separates the routing and forwarding decisions of networking elements, e.g., routers, switches, and access points, from the DP. Therefore,

the network administration and management procedures are simplified, considering that the CP only manages the information related to logical network topology. The DP orchestrates the network traffic according to the established configuration in the CP. The control operations are centralized in a Controller that manages the network policies [346] [347] and performs direct control over the state in the DP elements through dedicated Application Programming Interface (API) [346], as depicted in Fig. 4.12.

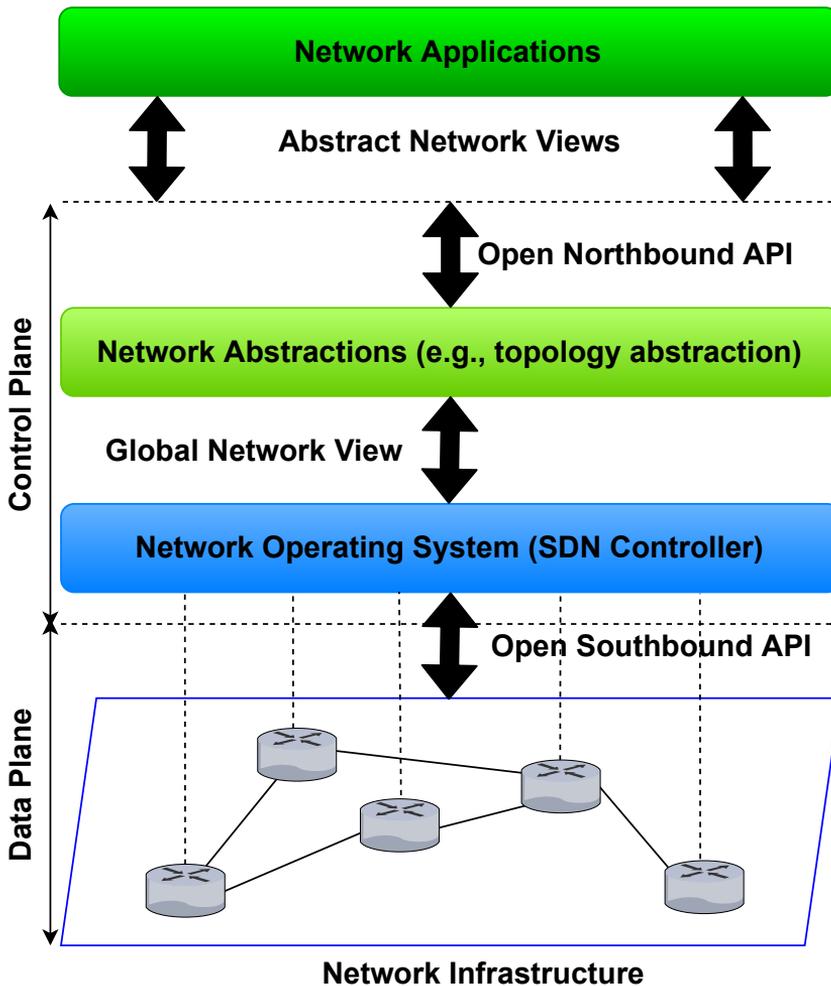


Figure 4.12: Typical representation of an SDN-based architecture.

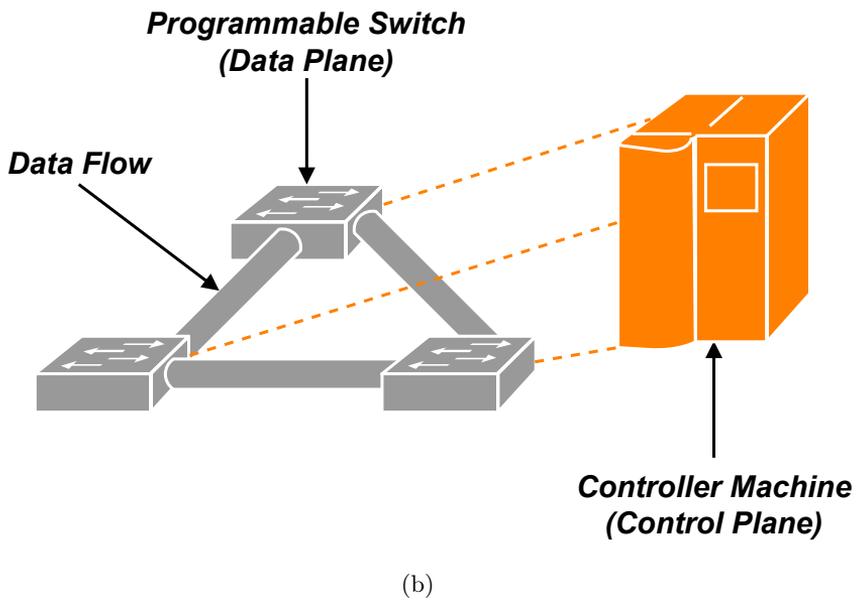
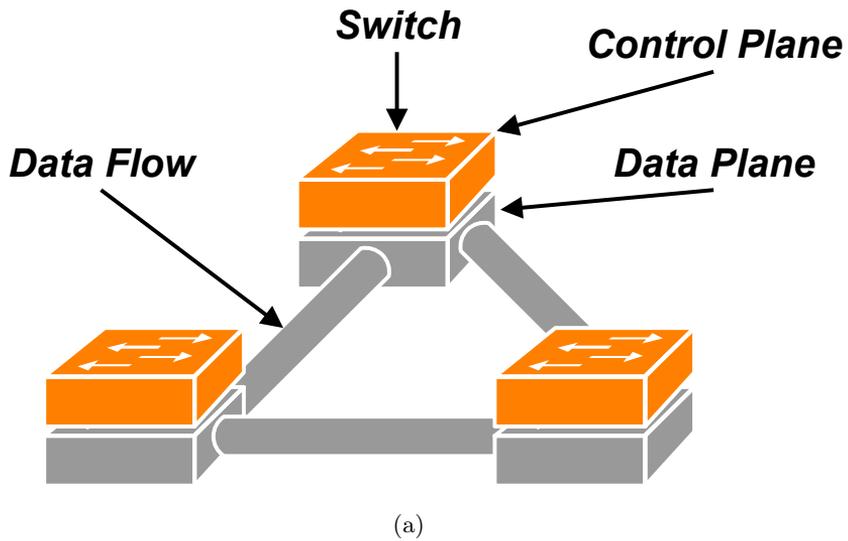


Figure 4.13: In 4.13a is represented the traditional networking paradigm, whereas 4.13b represents the SDN networking paradigm [17].

The benefits that SDN can provide are the following:

- The SDN switches are considerably simpler and less expensive w.r.t. traditional devices because they need to implement fewer protocols and do not need to make complicated decisions.
- The SDN technology allows DP and CP components to evolve independently as long as they adhere to a standard interface (e.g. OpenFlow). This versatility in coupling allows individual parties to develop interoperable management applications and control logic independently.
- Network applications can be developed and deployed easily since they are placed at a higher logical level with respect to the logically centralized Controller. On the contrary, a conventional network application may need to change the control logic in a switch firmware.
- With SDN technology, vendor-specific implementation details are irrelevant, considering that they are masked behind a standard interface between the switches and the Controller.
- With the use of SDN technology, network management is considerably simplified and less error-prone compared to traditional networks. Rather than configuring and controlling each switch independently, a network administrator can program the Controller, which in turn can configure the switches according to necessities [100] [343].
- The forwarding decisions are flow-based instead of destination-based. The flow abstraction allows unifying the behavior of different kinds of network devices, including switches, routers, middleboxes, and firewalls, enabling outstanding flexibility, limited only to the capabilities of the implemented flow tables [348].

The Table 4.1 compares the characteristics of SDN with respect to traditional network architectures.

Features	Traditional architecture	SDN architecture
Complicated network control	✓	
Error-prone configuration	✓	
Centralized control		✓
Programmability		✓
Simple implementation		✓
Network resilience		✓
Efficient configuration		✓
Improved management		✓
Enhanced performance		✓

Table 4.1: Comparison of features of SDN with respect to classical networks.

SDN architecture is centralized at the logical level, however, it is important to emphasize that this model does not postulate a physically centralized system. As a matter of fact, in order to guarantee appropriate levels of scalability, performance, and reliability would preclude such a solution [349].

4.4.4.1 Control Plane

The implementation of the SDN CP can follow a centralized, hierarchical, or decentralized design. Initial SDN CP proposals focused on a centralized solution, where a single control entity has a global view of the network. While this simplifies the implementation of the control logic, it has scalability limitations as the size and dynamics of the network increase. As a matter of fact, when designing a distributed SDN CP it is important to decide not only the number but also the placement of the control entities. An important parameter to consider while doing so is the propagation delay between the Controllers and the network devices, especially in the context of large networks [350]. Furthermore, it is also necessary to consider other issues that involve control path reliability, fault tolerance, and application requirements [351]. Therefore, in order to overcome these limitations, several SDN approaches have been proposed in the literature that fall into two categories, hierarchical and fully distributed approaches. In hierarchical so-

lutions [99] [100], depicted in Fig. 4.14, distributed Controllers operate on a partitioned network view, while decisions that require network-wide knowledge are taken by a logically centralized root Controller.

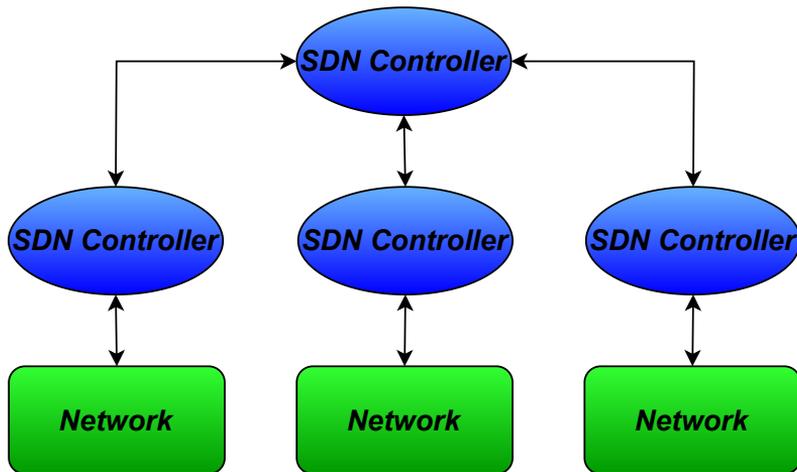


Figure 4.14: Hierarchical SDN architecture.

In distributed approaches, depicted in Fig. 4.15, Controllers operate on their local view or they may exchange synchronization messages to enhance their knowledge. Distributed solutions are more suitable for supporting adaptive SDN applications [101].

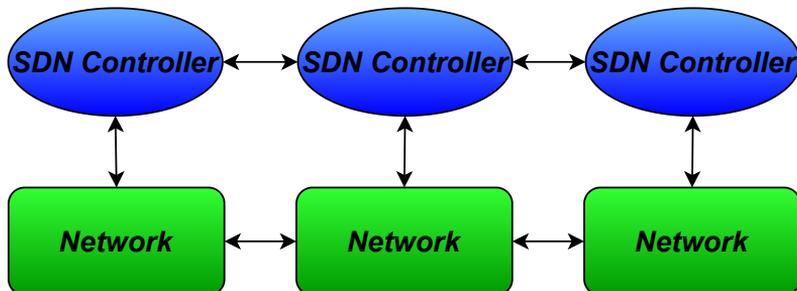


Figure 4.15: Distributed SDN architecture.

In these kinds of networks, the forwarding decisions made by the DP are flow-based, instead of destination-based. A flow is defined as a set of packet

field values acting as a match criterion and a set of specific instructions. The flow abstraction allows the classification of network traffic based on predefined matching rules, thus unifying the behavior of different types of network devices. Flow programming enables unprecedented flexibility, limited only to the capabilities of the implemented flow tables inside the forwarding devices. When a flow is generated from an entry that was previously installed in the switch, no control traffic is generated. The packets immediately pass through the switch and a much lower delivery time is experienced for these packets of the flow. When the switch receives a packet from an unknown flow, it forwards the packet to the Controller, which inspects the packet and considers the action that needs to be taken for it. Hence, the Controller instructs the switch to execute this action for all packets of this particular flow [352].

4.4.4.2 Data Plane

OpenFlow is a programmable network protocol for SDN environment, which is used for communication between OpenFlow switches and Controllers [353] [354].

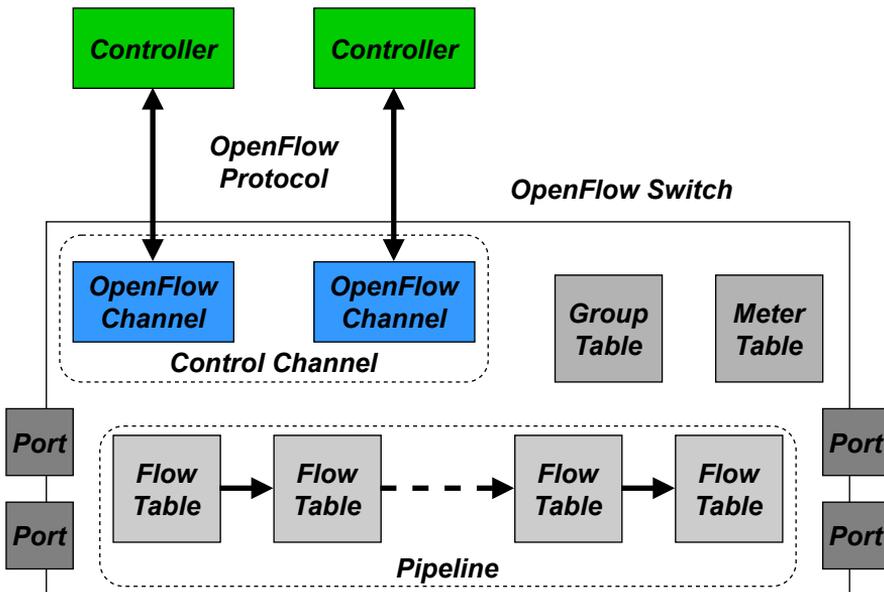


Figure 4.16: Schematic diagram of an OpenFlow Switch.

As can be seen from Fig. 4.16, the tables that compose the device have different purposes, which are explained as follows:

- **Flow Table:** a flow table matches incoming packets to a particular flow and specifies what functions are to be performed on the packets. There may be multiple flow tables that operate in a pipeline fashion, as explained subsequently.
- **Group Table:** a group table may trigger a variety of actions that affect one or more flows.
- **Meter Table:** a meter table can trigger a variety of performance-related actions on a flow [354].

Despite OpenFlow is not a protocol designed for QNs, it is logical to suppose that it can be suitably adapted to handle this type of network. For instance, on a QR flow tables could be related to the QM locations on which to perform swapping operations involving links between different QCs in the context related to a distributed quantum computation.

4.4.5 The Role of SDN in Quantum Networks

SDN technology has also been considered in order to create Next-Generation Networks (NGNs), considering that it facilitates the integration between satellite and terrestrial networks [355]. As for terrestrial networks, in the satellite context, the SDN capabilities are managed by a centralized SDN Controller with a global view of the satellite network resources [356]. Specifically, the Controller can retrieve the data about the whole constellation from a file that contains a Two-Line Element set (TLE), which is a data format encoding a list of orbital elements of an Earth-orbiting object for a given point in time, the epoch [357]. Furthermore, the Controller knows the DP resources within the satellite core network as well as proper abstractions of the resources of satellite hubs to control the offered bandwidth in the access network. In the satellite core network, including the network functions within the satellite gateway, the SDN Controller manages the appropriate flow rules, configuring the precedence and the policing as necessary. However, the case of providing flexible and on-demand bandwidth in the satellite access subsystem is more challenging due to resources constraints and their statistical multiplexing [356].

Not many experiments have been conducted on using SDN in QSNs scenario. However, considering that the positions of satellites in LEO orbit change very quickly given their high speed, it is appropriate to consider SDN technology for the realization of satellite quantum backbones. In SDN-based QSNs, a Controller is responsible for managing the global strategies for the distribution of long-distance EPR pairs. The Controller, after having managed the Link-to-Link (L2L) entanglement generation procedure manages the operations necessary to create the pairs on the E2E path by perform-

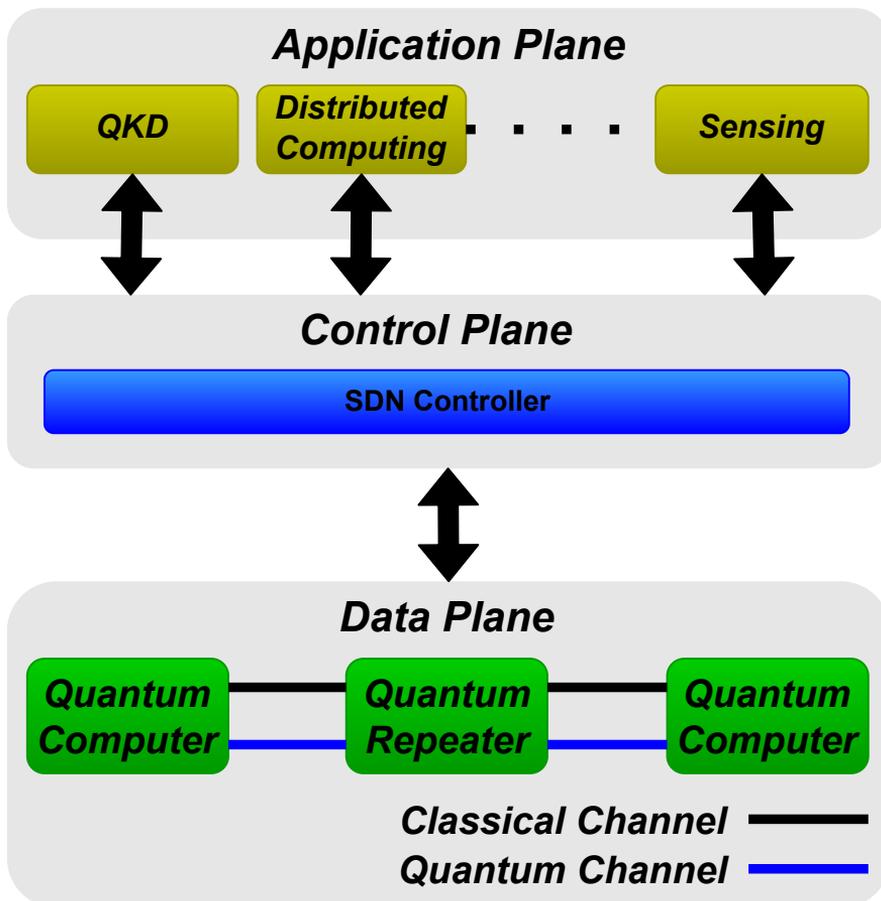


Figure 4.17: Schematic diagram of an SDN-based QN. This network can support multiple quantum applications.

ing multiple entanglement swapping [14] [358]. The control of a QN using SDN in order to manage specific quantum devices has been proposed, but however, many of the QKD protocols do not address control problems in true QNs aimed at E2E delivery of qubits, and the generation of long-lived entanglement [358]. However, some attempts related to the creation of E2E entanglement on a satellite path with specific protocols have been made and are described in Section 3.3.

Chapter 5

Satellite Architectures and Performance Analysis

This Chapter describes the proposed architectures and simulations conducted in this thesis with related results. Specifically, Section 5.1 describes some peculiarities of the simulation environment and framework adopted. In Section 5.2, an overview of possible satellite constellations and functional solutions is provided. Furthermore, Section 5.3 describes the simulations performed by applying some distributed and centralized routing algorithms on a LEO satellite network. Several simulations have been conducted also considering different constellations. The Chapter also explores the proposed solutions that integrate the SDN Controller in the constellation and provides the results of the related simulations.

5.1 Simulation Environment Features

Considering that the scenario concerns the creation of QSNs, the simulation tool can be divided into two main parts, which are (i) modelling the satellite tracklet and (ii) modelling the quantum communication system. After some investigation, the `Skyfield` Python package [359] was chosen for its many useful functions that were expected to enhance the code development. The package deploys functions to deal with time and positions, it allows to calculate sunsets and sunrises for different locations, check whether a satellite was sunlit, import ephemeris files, and it could also work with TLEs.

`Skyfield` generates a barycentric position measured from the gravitational center of the solar system. All vectors therefore originate at the gravitational center of the solar system. The package also includes the function to ask for an astrometric position relative to a specific observation location, and this position is adjusted for light-time delay.

5.1.1 Two-Line Element Set

A TLE is a data format encoding an Earth-orbiting object's list of orbital elements for a given point in time, the epoch. The state (position and velocity) at any point in the past or future can be estimated with some accuracy using a suitable prediction formula. The TLE data representation is specific to the simplified perturbations models (Simplified General Perturbations (SGP), SGP4, Simplified Deep Space Perturbations (SDP)4, SGP8, and SDP8) [360] [361], so any algorithm using a TLE as a data source must implement one of the SGP models to compute the state at a time of interest correctly.

The North American Aerospace Defense Command (NORAD) tracks all detectable objects in Earth orbit, creating a corresponding TLE for each object, and makes publicly available TLEs for many of the space objects, holding back or obfuscating data on many military or specific classified objects. Fig. 5.1 represents a typical example of a TLE that is, the one that represents the data concerning the International Space Station (ISS).

```
ISS (ZARYA)
1 25544U 98067A   08264.51782528 -.00002182  00000-0 -11606-4 0 2927
2 25544   51.6416 247.4627 0006703 130.5360 325.0288 15.72125391563537
-----
123456789012345678901234567890123456789012345678901234567890123456789
      1           2           3           4           5           6
```

Figure 5.1: Typical example of a TLE. The data represented in this figure concern the motion of the ISS.

Furthermore, the description of each parameter is stated in the following part. The first line contains the common name for the object based on information from the Satellite Catalog, while the meaning of the fields that compose the other lines are expressed in table 5.1 and table 5.2.

Line 1	
Column	Description
01	Line Number of Element Data
03-07	Satellite Number
08	Classification (U=Unclassified)
10-11	International Designator (Last two digits of launch year)
12-14	International Designator (Launch number of the year)
15-17	International Designator (Piece of the launch)
19-20	Epoch Year (Last two digits of year)
21-32	Epoch (Day of the year and fractional portion of the day)
34-43	First Time Derivative of the Mean Motion
45-52	Second Time Derivative of Mean Motion (Leading decimal point assumed)
54-61	BSTAR drag term (Leading decimal point assumed)
63	Ephemeris type
65-68	Element number
69	Checksum (Modulo 10) (Letters, blanks, periods, plus signs = 0; minus signs = 1)

Table 5.1: TLE Line 1 fields.

Line 2	
Column	Description
01	Line Number of Element Data
03-07	Satellite Number
09-16	Inclination [Degrees]
18-25	Right Ascension of the Ascending Node [Degrees]
27-33	Eccentricity (Leading decimal point assumed)
35-42	Argument of Perigee [Degrees]
44-51	Mean Anomaly [Degrees]
53-63	Mean Motion [Revs per day]
64-68	Revolution number at epoch [Revs]
69	Checksum (Modulo 10)

Table 5.2: TLE Line 2 fields.

5.1.2 Mathematical Models for the Prediction of Satellites Positions

Five mathematical models for the prediction of satellite position and velocity are available. The first of these is the SGP, which was developed in 1966 and used for near-Earth satellites [362]. This model considers the drag effect on mean motion as linear in time. This assumption dictates a quadratic variation of the mean anomaly with time. The drag effect on eccentricity has been modeled such that perigee height remains constant. The SGP4 model [363] was developed by Ken Cranford in 1970 and is used for near-Earth satellites. This model was obtained by simplification of the more extensive analytical theory of Lane and Cranford (1969) [364] which uses the solution of Brouwer (1959) [365] for its gravitational model and a power density function for its atmospheric model. The SDP4 model [366] is an extension of SGP4 to be used for deep-space satellites. The deep-space equations were developed by Hujzak (1979) and model the gravitational effects of the moon and sun as well as certain sectoral and tesseral Earth harmonics, which are of particular importance for half-day and one-day period orbits. The SGP8 model [367] is used for near-Earth satellites and is obtained by simplification of an extensive analytical theory of Hoots which uses the same gravitational and atmospheric models as in [364], but it integrates the differential equations in a much different manner.

`Skyfield` is able to predict the positions of Earth satellites by loading satellite orbital elements from TLEs files, published by organizations like CelesTrak, and running them through the SGP4 satellite propagation routine.

5.1.3 Retrieving, Importing, and Working with TLEs

TLEs are read and imported in two ways by the simulator: from a text file, or directly from CelesTrak. The user specifies which way to input the TLE by a True / False parameter. If the TLE is to be read from a file the user needs to specify further the local url to the file directory, and the name of the text file. The text file should contain the name of the satellite in the first line, then the first TLE line, and lastly the second TLE line.

The TLEs are updated continuously, and the user can choose whether to reload the latest version or to use the already fetched file in the directory. If the TLE file is to be reloaded, the progress of downloading it is indicated by a progress bar in the console.

5.1.3.1 Satellite Visibility

The observation of a satellite requires that the satellite is above the horizon. To check whether the satellite is above the horizon, the tool goes through the altitude coordinates of the satellite during the observation period. The altitude coordinate is relative to the observer, and altitude of 0 is defined as the horizontal plane. The tool, therefore, looks for any negative altitude coordinates, and if one is found, it can print a message that specifies the date and time that the satellite is below the horizon. Specifically, `Skyfield` can search between a start time and an end time for each occasion on which a

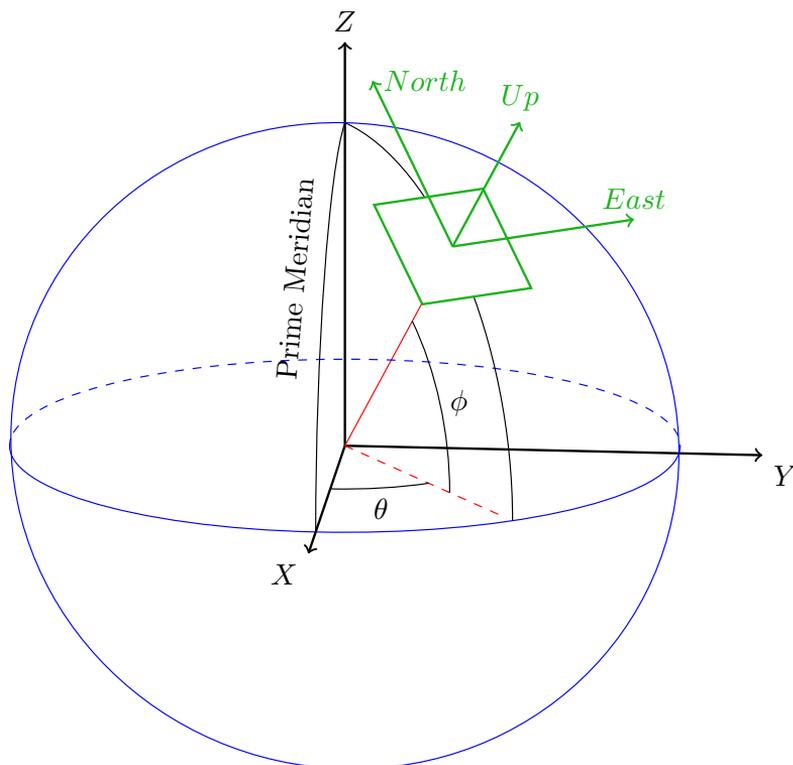


Figure 5.2: The plane of the horizon for the observer on the surface of Earth [18]. For an observer placed at the center of the coordinate system represented in green, it is not possible to see objects that set relative to its plane of the horizon (represented by the green square).

satellite's altitude exceeds a specified number of degrees above the horizon. Furthermore, it is possible to retrieve additional information regarding the position of a satellite. The simplest form in which it is possible to generate a satellite position is to call its *at()* method, which will return an (x, y, z) position relative to the Earth's center in the Geocentric Celestial Reference System (GCRS) [368], which is physically adequate to describe processes occurring in the vicinity of Earth, such as Earth's rotation and the motion of Earth's satellites.

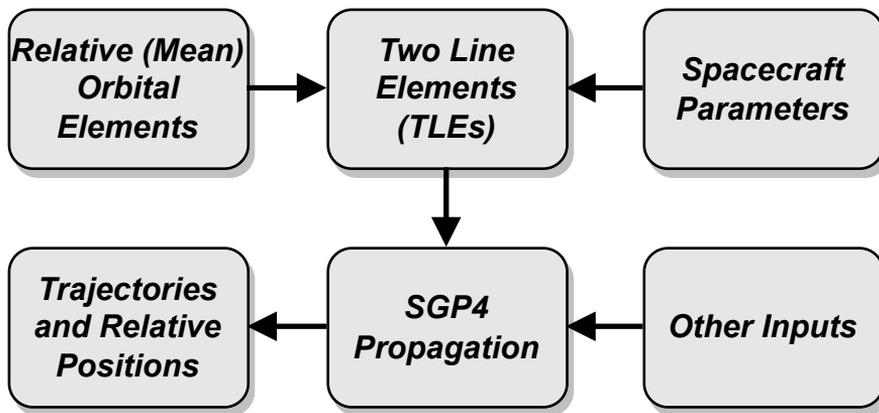


Figure 5.3: Diagram representing relevant tools for obtaining satellite trajectory data [19].

5.2 Control Plane Deployment Solutions Analysis

In the following, some of the possible SDN-based satellite architectures are outlined, analyzing their characteristics with a specific focus on the advantages, and disadvantages. Furthermore, the architectures and solutions adopted in the conducted experiments are discussed. Finally, for each proposed architecture are analyzed the results obtained in the conducted simulations.

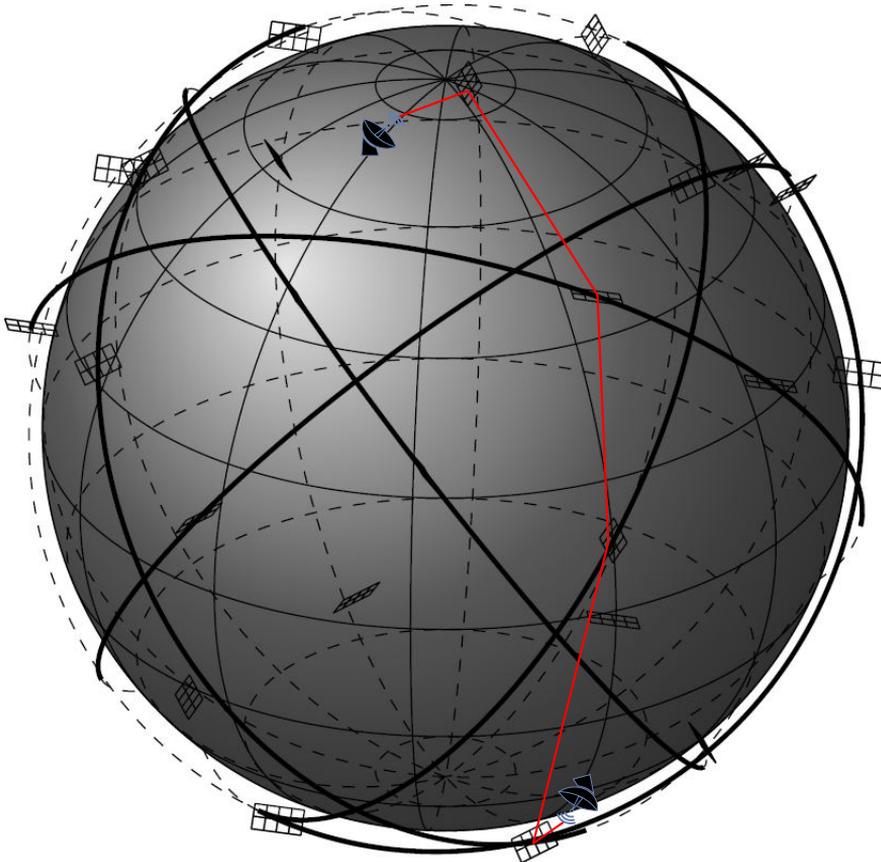


Figure 5.4: A possible connection between two GSs via multiple FSO satellite links.

5.2.1 LEO Constellation with a Single Ground Controller

In [20] an architecture consisting of a single ground Controller that manages the entire constellation has been preliminary introduced. The CP consists of a single Controller deployed in a Master Control Station (MCS), whereas the DP consists of Quantum Satellite Repeaters (QSRs). The Controller gathers the data required to build the entire satellite network state querying a database that contains the constellation adjacency matrices. Whenever

it was necessary to interconnect two GSs, the distributed application invokes the Controller best path evaluation module via the Northbound API and applies a centralized path selection algorithm. The QSRs generate and exchange entangled particles, basing on information provided by the Controller through the Southbound API. The Controller has complete control of the architecture managing the generation of L2L entanglement and the swapping operations necessary to originate E2E entanglement. This architecture, consisting of a LEO constellation managed with SDN technology is certainly appropriate, however, further improvements can be introduced, taking into account that minimizing the swapping overhead is relevant for distributed operations and, therefore, it is important to properly design the topology [11].

5.2.2 Multi Controller on GEO

Another solution is similar to the one described in [255] with a master Controller that coordinates some domain Controllers but deployed directly on GEO satellites. Since geostationary communication satellites at latitudes above about 81 are below the horizon, hence, it would be very difficult to ensure *complete* coverage for the underlying LEO constellation. Furthermore, latency becomes significant as it takes about 240 *ms* for a signal to pass from a GS on the Equator to the satellite and backwards. In addition, the inter-satellite routes between GEO satellites could be longer than the satellite to ground links, introducing even greater latencies. Therefore, an architecture consisting of several Controllers placed on geostationary satellites may not be an adequate solution, since it is not possible to achieve complete coverage of the underlying LEO constellation; moreover, the high delays could severely limit the system response time. This makes the previous solution not effective especially for applications that require distributed quantum computing.

Coverage problems can be overcome by considering an Equatorial-Polar (EP) constellation as described in [369]. MEO Polar orbit satellites could help ensure global coverage. Satellites that are part of the Polar orbit segment could be enabled at the same time as they pass over the Polar areas ensuring full control over the underlying LEO constellation. The satellite at sunset is deactivated and then reactivated when it passes over the opposite Polar area, while, when it is in transit, it can retrieve the status of the underlying LEO network. Although this kind of constellation ensures complete

global coverage, it does not solve the problem of reducing the latency. However, this type of architectures even if they are not suitable for distributed quantum processing can be used to resolve the Routing and Key Allocation (RKA) problem, as it has been proposed in [74].

5.2.3 Multi Controller on MEO

In order to get more coverage on the Earth's surface together with limit the latency problem, we could consider to place the Controllers on a MEO constellation similar to GPS. The GPS constellation operates at an altitude of 20200 *km* and each satellite thereby providing very high coverage. The lower distance of the satellite towards GSs and between the LEO satellites and the respective MEO satellites has a beneficial effect on latency. However, considering the kinematics of both constellations, this kind of architecture could be very difficult to manage, since it could require the design of appropriate *handover* procedures. In fact, a GS cannot be in LOS with respect to the same MEO satellite, and the configuration of the LEO constellation also continuously changes for the MEO one and the GSs. This architecture introduces considerable complications compared to the previous ones, then it could not be suitable neither for distributed applications nor for the resolution of the RKA problem.

5.3 Single Controller on the Ground

As explained in [74], the procedure of quantum satellite-to-ground communication consists of a quantum communication paired with a classical communication which usually uses different wavelengths multiplexed over the same laser link. The quantum satellites are able to conduct both quantum communication and classical communication using a unique integrated transponder. Typically, the quantum signal is transmitted on downlinks and the classical signal is transmitted on uplinks. The single polarized photons are sent through the quantum channel, while classical channel can be used for the measurement-basis signals and key-relay services, as well as for future data services.

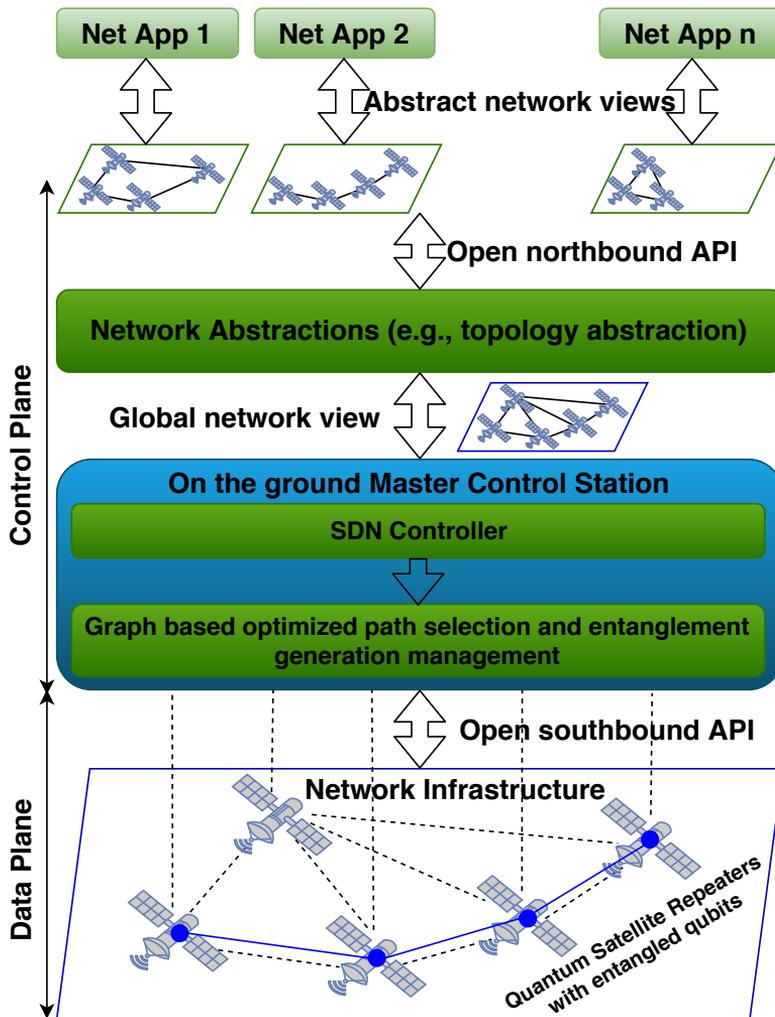


Figure 5.5: Quantum Software-Defined Internetworking architecture [20]
©2020 IEEE.

For the inter-satellite quantum channel, the FSO technology with a wavelength of 1550 nm is used due to its higher efficiency. To be compatible with classical communications, multi-beam system is used in inter-satellite communications. With the on-board multi-beam transponders, quantum signal

and data signal can be carried on different laser beams, in the same optical link.

The satellite network is similar to a terrestrial fiber optic network, considering that the GSs distributed across Earth and satellites are nodes equipped with quantum memories, as explained in [251]. In order to connect a source GS and a target GS, entanglement for quantum memories between adjacent quantum satellites is generated through the transmission of photons entangled with those memories.

A GS may have characteristics similar to those of a typical radio telescope like the Italian Sardinia Radio Telescope, which as described in [370] has an elevation of between 5 and 90 degrees. LEO satellites, which orbit in a spherical region that extends from the Earth's surface up to an altitude of 2000 *km* [371], could be an excellent alternative to fiber optic communications. Because of their low altitude, the path length traversed via the satellites between points on earth is only slightly longer than the great circle distance between the points, hence they eliminate the long propagation delay encountered by GEO satellites [372]. New LEO satellite constellations like OneWeb, Telesat, and Starlink quoted in [95] are going to be launched in the near future, but the dataset we considered is the one related to the constellation IRIDIUM NEXT made up of 75 satellites, 66 cross-linked satellites and 9 in-orbit spares operating in a LEO, at an altitude of 800 *km* [373].

As explained in Section 1, such a network could be controlled centrally following the SDN paradigm as shown in Fig. 5.5, of which we provide a brief description in the following. The entire constellation can then be controlled by one MCS on Earth like GPS, as explained in [374]. The Controller derives the data required to build the entire satellite network state. Then a centralized routing algorithm that calculates the best path can be applied. Whenever it was necessary to interconnect two GSs, the distributed application invokes the Controller best path evaluation via the northbound API. The QSRs which are the devices that make up the DP, generate and exchange entangled particles based on information provided by the Controller through the southbound API. In order for the coupling procedures to take place quickly, it is necessary to carefully choose the satellite from which to start the propagation procedure of the Bell pairs. As in the model proposed in [375] the satellite in the middle is detected by the Controller which sends it the necessary instructions to start the propagation procedure. Then the creation of the Bell Pairs starts from this satellite and propagates it to

wards both GSs. The procedure of entanglement generation on the links that compose the path can be accomplished according to the schemes described in [79] that require a coordinated action between the nodes at the two ends of the inter-satellite link and between the GSs and the connected satellite. When the entire E2E connection via Bell pairs has been established, the Controller will send the necessary messages to activate the swapping operations through the southbound API. When the Controller will be notified by the involved repeater that the swapping operations have been successfully performed and therefore the E2E entanglement has been created, it will send to the ground transmitting station an authorization notification to transmit the data packet containing the teleportation bits. The traffic needed for this process is all exchanged on the classic channel.

5.3.1 Problem Statement

A typical QN is based on the phenomenon of entanglement swapping which allows generating a pair of entangled particles at a long distance and quantum teleportation. In order to allow an exhaustive characterization of the model, we explain first the physical principles on which a quantum communication is based.

The entanglement swapping process can also be implemented in a satellite context, as it is proposed in [376]. As described in [377] and [378] the entanglement swapping procedure shown in Fig. 5.6 works as follows. Preparing two independent entangled pairs α - β and δ - γ , a joint BSM on β and δ has the effect of projecting α and γ onto an entangled state, although these two particles have never interacted nor share any common past.

In quantum teleportation described in [291] and [42], the state of a qubit is destroyed in one location and recreated in another. Initially, a pair of particles indicated as a Bell pair is distributed, one member to the source, and the other to the destination. The qubit of the QM that must be teleported is entangled with the source's member of the Bell pair. This is done performing a measure on the data qubit and source's Bell qubit. Each measurement that results in one classical bit destroys the quantum state of the qubit and these results are communicated to the destination using a classical channel. The recipient uses them to decide what quantum operations it has to perform on his Bell qubit in order to recreate the original state of the data qubit. In this manner, the *no-cloning principle* is observed and the *no faster than light communication principle* is not violated [61]. The quantum teleportation

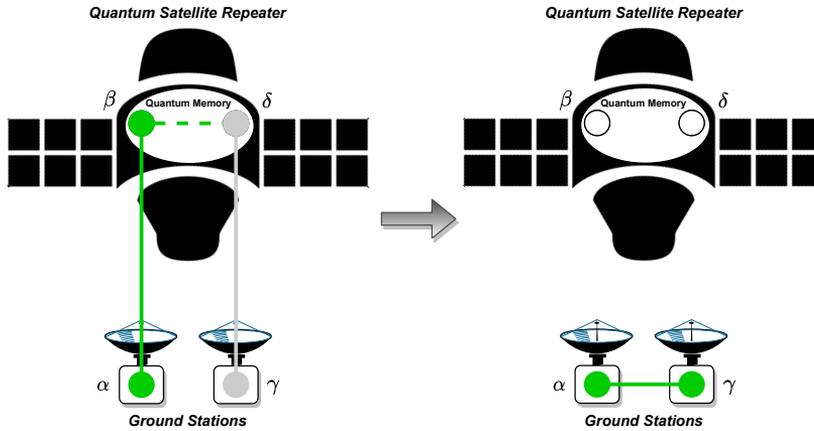


Figure 5.6: Operating principle of QSRs. Entanglement swapping is performed between two pairs of particles executing a BSM on two of them.

procedure has already been carried out in the satellite context, as described in [263]. As already specified in Section 1, repeater nodes are required to implement this mechanism, therefore the satellites of the constellation can

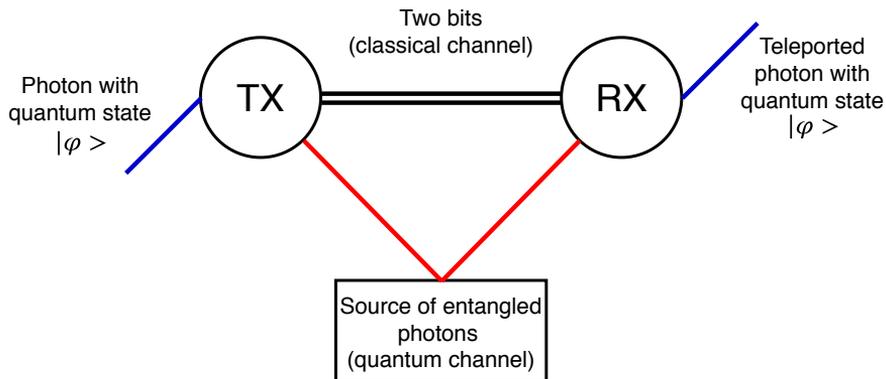


Figure 5.7: Scheme of a quantum communication based on teleportation. A particle with quantum state $|\psi\rangle$ is teleported sending two bits on the classical channel [20] ©2020 IEEE.

be considered as repeater nodes. For this reason, the model we have derived is similar to the one presented in [66], but with technological improvements in order to apply it to free space.

Specifically, it considers the *entanglement generation probability* (assumed the same for each node) as a product between the photons generation probability p_g , the heralding and entangling detector efficiency, respectively indicated with η_h and η_d :

$$p = p_g \eta_h \eta_d \quad (5.1)$$

A remote entanglement between two adjacent nodes is generated through the operation of *entanglement swapping* accomplished by carrying out an optical BSM of the two photons. In details, an heralded local entanglement is generated on each node, they are sent to the BSM and then are measured. Hence, the link entanglement generation probability between the i -th and j -th nodes is defined as:

$$p_{i,j} = \frac{1}{2} \eta_0 p^2 e^{-\frac{d_{i,j}}{L_\alpha}} \quad (5.2)$$

where η_0 is the optical BSM efficiency, $d_{i,j}$ indicates the Euclidean distance between the two nodes involved and L_α is the electric field attenuation length. As defined in [379], α is the attenuation of optical wave amplitude, which is the wave energy losses.

$$\alpha = \frac{\omega \sqrt{2\varepsilon}}{2} \left[\sqrt{1 + \left(\frac{\sigma}{\omega \varepsilon} \right)^2} - 1 \right]^{\frac{1}{2}} \quad (5.3)$$

As described in [294], L_α is defined as:

$$L_\alpha = \frac{1}{\alpha} \quad (5.4)$$

In order to calculate the attenuation length, we considered ε_r that is the resistivity and σ which is the conductivity, respectively described in [380] and [381]. The values relating to these parameters are shown in Table 5.3 of Section 5.3.3 in where the framework is described.

Moreover, respecting the specifications shown in the Section 5.3, the wavelength that we have chosen is $\lambda = 1550 \text{ nm}$. In the proposed model, $T_{i,j}$ is the average time required to generate a remote entanglement between two adjacent nodes, that is equal to:

$$T_{i,j} = \frac{\bar{p}_{i,j}T_{i,j}^f + p_{i,j}T_{i,j}^s}{p_{i,j}} \quad (5.5)$$

where $T_{i,j}^f$ is the total average time required for the failed attempt and $T_{i,j}^s$ is the average time required for the successful attempt. As shown in [382], the quantum coherence is equivalent to quantum entanglement in the sense that coherence can be correctly described as entanglement, and conversely that each entanglement measure corresponds to a coherence measure. It therefore corresponds to time within which it is possible to keep the information in order to successfully teleport qubits [66]. As stated in these studies [383] [384], it is possible to achieve a coherence time greater than 39 minutes, therefore given the technological improvements, unlike what is expressed in the reference model, we do not take this parameter into consideration.

As we specified in Section 1, the communication rate is a function of the maximum distance between two adjacent quantum repeaters, instead of the entire length of the E2E link. Therefore, the time required to generate a remote entanglement on the route is defined as:

$$T_r = \frac{\max(T_{i,j}) + \tau_a + \max(T_{i,j}^c)}{\eta_a} \quad (5.6)$$

where $T_{i,j}^c$ is the time required for ACK transmission over a classical communication link between two adjacent nodes marked with i and j , while τ_a and η_a are respectively the atomic BSM duration and efficiency. We considered η_a and η_0 values equal to 0.75 considering that in [385] are reported similar values. Finally, we define the *entanglement rate* on the same route as:

$$R \doteq \frac{1}{T_r} \quad (5.7)$$

The entanglement rate is also defined as a special kind of throughput [147] [148], or rather number of transmitted entangled states per second and is measured as Bell pairs per seconds. In [386] it is defined as the speed of variation of

the relative entropy of entanglement.

5.3.2 Proposed Forwarding Strategies

Most traditional CP processes use a distributed architecture. For instance, each router runs its own Open Shortest Path First (OSPF) routing protocol process. Those distributed CP processes use messages to communicate with each other, like OSPF protocol messages between routers. Therefore, traditional networks use a distributed CP [387]. A Delay-Tolerant Networking Architecture (DTN) like this does not expect that network links are always available or reliable [388]. In this scenario, epidemic routing could be an effective solution for an intermittently connected network. A generic node which applies the epidemic protocol works by transferring its data to each and every node it meets. As data is passed from node to node, it eventually reaches the target node. One of the advantages of an epidemic protocol is that by trying every path, it might be guaranteed to try the best path, while a disadvantage is the extensive use of resources with every node needing to carry every packet and the associated transmission costs [389].

On the other hand, a centralized CP has the logic in one place, running on a single device, or on an external server. Then the centralized procedure could have used protocol messages to learn information from the devices, but with all the processing of the information at a centralized location. A centralized application has all the data gathered into one place, hence it is easier to write than a distributed application. The SDN paradigm uses a centralized architecture, with a centralized CP, with its foundations in a service called Controller [387]. In this thesis, we have compared two distributed algorithms i.e. a Modified Random Walk (MRW) and an Ant Colony Optimization (ACO) with a centralized approach using Dijkstra's algorithm that requires the integration into an SDN-based architecture as we have defined and that is depicted in Fig. 5.5. The indicated strategies were selected because they take into consideration the problem of distance, which is crucial in QNs.

5.3.2.1 Modified Random Walk

We used as a benchmark a MRW procedure connecting satellites that are at minimum possible distance avoiding those ones that have been previously selected.

We can define as \mathcal{G} the set of satellites that are part of the constellation. If we consider as \mathcal{V} the set of visited nodes and with L_g the set of neighboring satellites of a satellite g , the algorithm proceeds only if

$$\forall g \in \mathcal{G} \exists l \in L_g \mid l \notin \mathcal{V} \quad (5.8)$$

Algorithm 1 Modified Random Walk

Output: Best path

Initialize: g as source, add g to \mathcal{V}

while g is not the destination **do**

if g is the destination **then**

return Best path

else

for every node in L_g **do**

if all the nodes in L_g are in \mathcal{V} **then**

 Restart from source node

break

else

 Consider nodes that are not in \mathcal{V} and select the closest one

 Add the selected node to \mathcal{V}

end

end

Under the hypothesis of a perfect knowledge of the distances to neighboring satellites, a satellite routes a packet to the neighbor at minimum distance. If this satellite has already been visited previously, the next one in the sorted list of neighbours is selected and so on. The information about the previously visited satellites could be included in the data field of the packet and updated as it proceeds towards the destination node. If the packet reaches the destination node it means that the path has been identified and the quantum communication can be started.

This protocol has limited signaling traffic but may require the visit of a large number of nodes and may fail to establish the connection if all the nearby nodes have been previously visited.

5.3.2.2 Ant Colony Optimization

Adaptive routing is a process where a router can forward data via a different route or given destination based on the current conditions of the system. ACO, in which information gathered by simple autonomous mobile agents is shared and exploited for problem solving, has been applied to routing in telecommunications networks [390]. This algorithm is suitable for routing because it has characteristics like capability for self-organisation, self-healing, and local decision making [391].

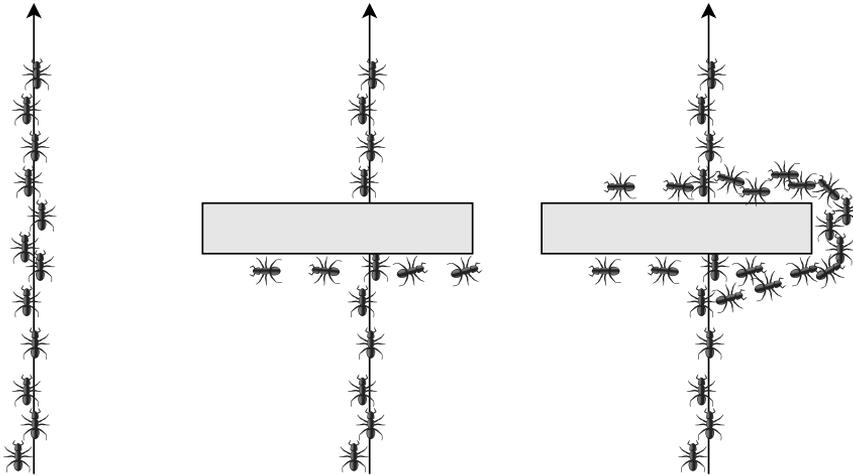


Figure 5.8: Ants follow a specific path. If an obstacle is interposed, ants can choose to go around it following one of the two different paths with equal probability. On the shorter path more pheromone is laid down.

As described in [392], social insect colonies like ants, bees, wasps or termites show sophisticated *collective* problem-solving in the face of variable constraints that emerges from relatively simple *individual* behaviors. Many of these processes are regulated by interactions between the individual agents within the colony, which will affect overall colony functioning. They use multiple modalities of communication, but the most commonly known are *pheromone* trails used to both recruit new workers to exploit the food source as well as guide these foragers to it. As shown in [393], an ant encountering a previously laid trail can detect it and decide with high probability to follow

it, thus reinforcing the trail with its own pheromone. The obtained collective behavior is a form of *autocatalytic* behavior where the more the ants following a trail, the more attractive that trail becomes for being followed.

Some definitions are given before describing the algorithm. The trail intensity is updated according to the following:

$$\varphi_{ij}(t+n) = \varepsilon\varphi_{ij}(t) + \sum_{k=1}^m \Delta\varphi_{ij}^k \quad (5.9)$$

where ε is a decay factor of the trail on the edge and $\Delta\varphi_{ij}^k$ is the quantity per unit of length of trail substance laid on edge (i, j) by the k -th ant between time t and $t+n$. If the k -th ant does not use the edge in its tour the value is zero, otherwise it is equal to:

$$\Delta\varphi_{ij}^k = \frac{Q}{\Lambda_k} \quad (5.10)$$

where Q is a constant that we set as 1 and Λ_k is the tour length of the k -th ant. The probability of going to the j -th node is:

$$p_{ij}^k(t) = \frac{|\varphi_{ij}(t)|^\beta \left| \frac{1}{d_{ij}} \right|^\gamma}{\sum_k |\varphi_{ik}(t)|^\beta \left| \frac{1}{d_{ik}} \right|^\gamma} \quad (5.11)$$

The value of $\varphi_{ij}(t)$ gives information about how many ants in the past have chosen that same edge and $\frac{1}{d_{ij}}$ says that the closer a town the more desirable it is. The other parameters β and γ act as a weight on pheromone and distance respectively. In the context of networks, an ant is a routing packet emitted by a satellite node, interspersed with the normal traffic, with a randomly chosen destination node. Pheromones represent the quality of the traversed paths and a transition rule is used to define the probability that the ant chooses to move through the edge, as explained in [390] and [394–396]. The ACO algorithm proceeds as follows. Every ant moves from satellite i to satellite j choosing the satellite to move to with a probability described in (5.11). After n iterations all ants have completed a tour. At this point for each ant k the value of Λ_k is computed and the values $\Delta\varphi_{ij}^k$ are updated according to (5.10) and the shortest path found by the ants is saved. This process is iterated until the tour counter reaches the maximum (user-defined)

number of cycles, or all ants make the same tour.

Algorithm 2 Ant Colony Optimization

Input: Number of ants, number of cycles

Output: Best path

Initialize: Pheromone values

while *number of cycles not completed* **do**

for *each ant* **do**

 Deposits a quantity of pheromones according to equation 5.10

 Ant makes a decision on what satellite to go according to the numerator of equation 5.11

end

 Multiply the pheromone matrix by decay factor

end

5.3.2.3 Dijkstra's Algorithm

The version of Dijkstra's algorithm that we used is described in [397] and [398].

Consider a directed graph G , one of whose vertices is distinguished as the source s , and each of whose edges (v, w) has a nonnegative length $l(v, w)$. The number of edges is denoted by m and the number of vertices by n . Furthermore, there is a path from s to any other vertex, therefore $m \geq n - 1$. The algorithm solves the shortest path problem using a tentative distance function d from vertices to real numbers with the following properties:

- For any vertex v such that $d(v)$ is finite, there is a path from s to v of length $d(v)$
- when the algorithm terminates, $d(v)$ is the distance from s to v .

Initially $d(s) = 0$ and $d(v) = \infty$ for $v \neq s$; afterwards, each vertex can be in a state between unlabeled, labeled, or scanned. Initially, only the source node is labeled, while all other vertices are unlabeled. The algorithm proceeds scanning each vertex until there are no labeled vertices.

Using this version of Dijkstra's algorithm a total running time equal to $O(n \log n + m)$ is obtained. This algorithm requires a centralized routing CP that is a feasible concept and is capable of simplifying routing management. It requires SDN which separates the network CP from the DP and enables a NOS which interacts with packet forwarding elements [399].

Algorithm 3 Dijkstra

Input: Directed graph G **Output:** Best path**Initialize:** A set S to store finalized vertices and a distance matrix d , where $d[v]$ represents the length of the shortest path from s to v . Let $d[s] = 0$ and $d[v] = \infty$ for v not equal to s .

```

while every vertex is in  $S$  do
    Delete the item of minimum key in heap  $h$  and put it in  $v$ 
    Declare  $v$  scanned
    for each arch( $v, w$ ) do
        if  $d(w) = \infty$  and  $d(w) = d(v) + c(v, w)$  then
             $d(w) = d(v) + c(v, w)$ 
            Insert  $x$  into heap
        else if  $d(w) < \infty$  and  $d(v) < d(v) + c(v, w)$  then
             $d(w) = d(v) + c(v, w)$ 
            Declare  $w$  labeled
    end
    Add  $v$  to  $S$ 
end

```

5.3.3 Simulations Results

In this Section, we firstly describe the framework and the adopted libraries to model and simulate the proposed approaches, whose results are then shown for different scenarios. All the trajectory data were obtained considering the TLE, which is a data format encoding a list of orbital elements of Earth-orbiting objects for a given point in time, the epoch. They allow rapid, modestly accurate propagation of space object motion [357]. The satellite topology matrix is calculated when the satellite trajectory datas are obtained from these files. In particular, we used the `Skyfield` Python package [359] in order to operate on the file containing the TLE coordinates [400] to get the necessaries data and the `pygeodesy` package in order to work with the coordinates and the routing algorithms included in the `scipy` package. Many of the values are consistent with the reference model, but for p_g, η_h, η_d denoting the photons generation probability and the heralding and entangling detector efficiencies, respectively, we considered values reported in [401–403]. Other parameters considered in the model are the speed of light c, η_0 and η_a which denotes, respectively, the optical BSM efficiency and the atomic

Parameter	Value
c	$3 \times 10^8 \frac{m}{s}$
η_0, η_a	0.75
λ	$1550 \times 10^{-9} m$
L_α	743704275.359 m
η_h, η_d	0.95
τ_h	$10 \times 10^{-6} s$
τ_t	$20 \times 10^{-6} s$
τ_0, τ_a	$10 \times 10^{-6} s$
p_g	0.9
σ	$8 \times 10^{-15} \frac{S}{m}$
ε_r	$1.000536 \frac{C^2}{Nm^2}$

Table 5.3: Values of the parameters adopted in the simulations [20] ©2020 IEEE.

BSM efficiency, while with τ_0 and τ_a we denote the optical and atomic BSM duration.

In the following, the curves in red depict the performance obtained by the MRW algorithm, in blue the ones for ACO, while in green the results obtained by applying the Dijkstra's algorithm. The simulations were carried out by connecting two terminal stations on the Earth's surface placed at the antipodes for a reference time interval of sixty minutes and capturing a sample every 500 ms.

First of all, we focus on the entanglement rate achieved over a single link, whose length has been varied between zero and 10000 km. As shown



Figure 5.9: Artistic representation of an optical ISL.

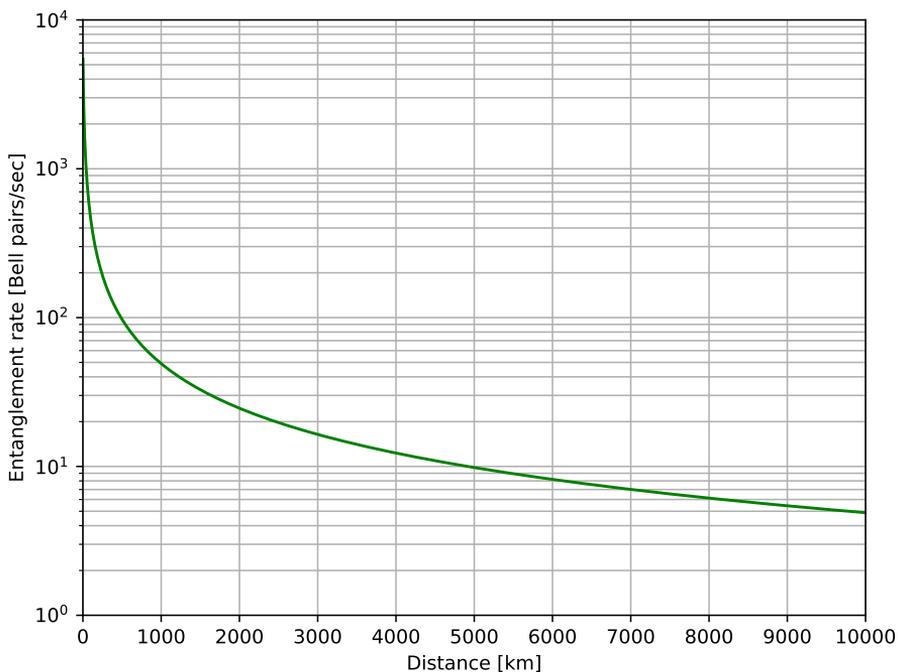


Figure 5.10: Entanglement rate for different L2L inter-distances [20] ©2020 IEEE.

in Fig. 5.10, the entanglement rate value tends to decrease with a *super-exponential* trend. Considering that we have used in the model parameters that can be traced back to the best technologies currently available, the value of the entanglement rate is higher than other works in the literature, such as in [331], in which they claim to be able to reach an entanglement rate equal to 4 *Bellpairs/s* with LEO satellites. These considerations are fundamental, especially in the design of satellite backbones in even higher orbit as proposed in [264].

Moreover, we analyze the performance with respect to the length of the E2E path and the number of hops for the three considered routing approaches. In particular, Fig. 5.11 shows the path length, while in Fig. 5.12 the maximum inter-satellite distances are shown. Furthermore, in Fig. 5.13 the number of hops are represented. Each Figure depicts the histograms of the Probability Density Functions (PDF) of the three algorithms for each considered parameter and their statistical fitting, where the value at the ori-

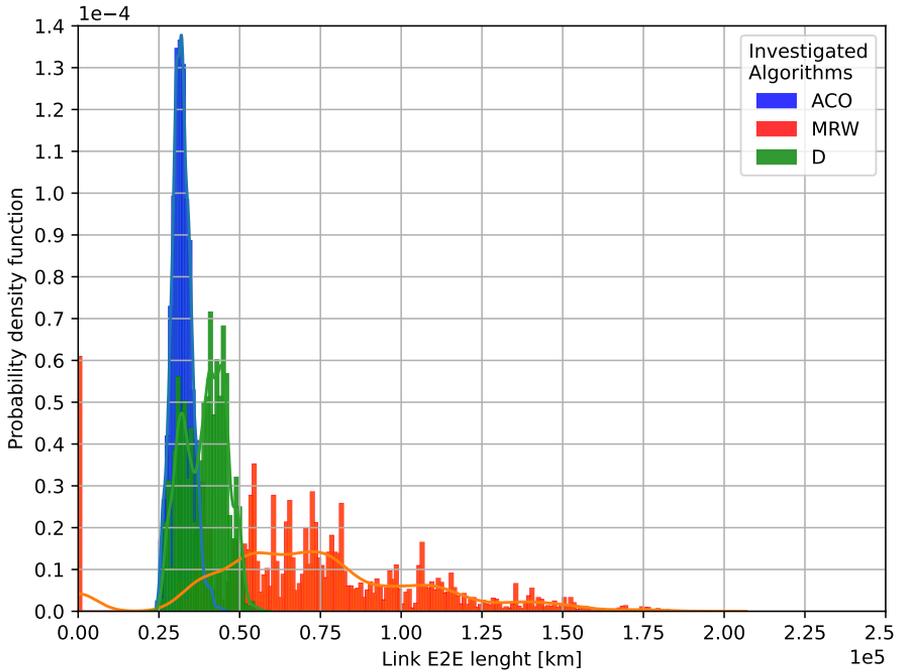


Figure 5.11: E2E path Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.

gin of the x-axis represents the failures, that only occurs when MRW fails in the generation of the E2E path.

As can be seen from Fig. 5.11 (summarized in Table 5.4 where the average values μ of the distributions and the relative standard deviations σ are presented), the length of the E2E paths achieved by the MRW protocol is greater than for the other two cases. As regards to the other two approaches, we can see that Dijkstra's algorithm creates routes that are shorter on average than MRW but longer than the ACO algorithm. Considering the results in Table 5.4, we can see that using Dijkstra's algorithm we have longer routes with a greater number of hops.

Moreover, as can be seen from Fig. 5.12, the Dijkstra's algorithm is able to guarantee a maximum inter-satellite distance lower than the others, a factor that mostly affects the distribution of entanglement rate values. Fig. 5.14 shows the PDF of the entanglement rate which represents the objective function for all the investigated schemes.

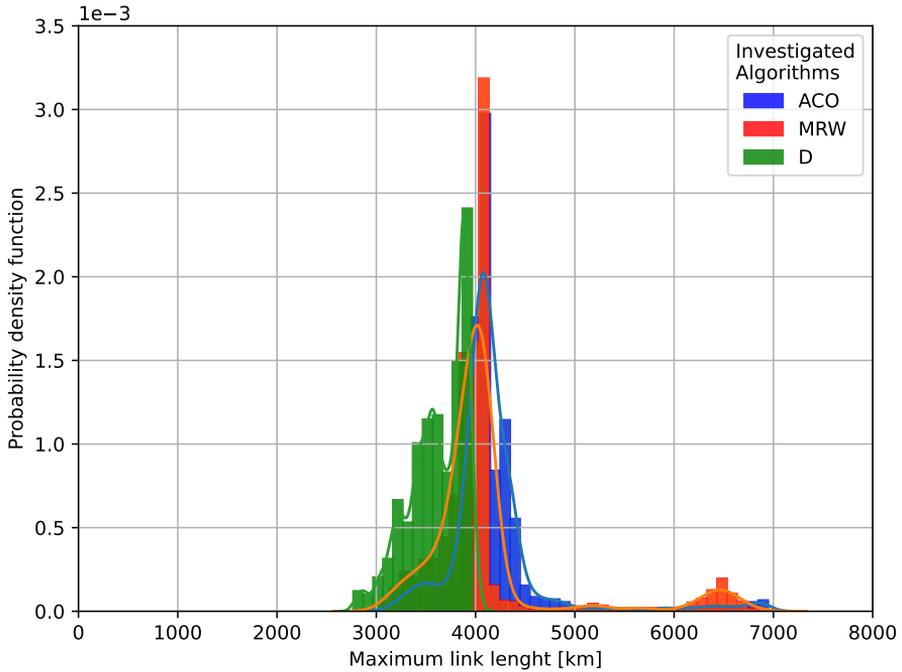


Figure 5.12: Maximum single link length Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.

Algorithm	MRW		ACO		D	
	μ	σ	μ	σ	μ	σ
End-to-end path length [km]	75610	34774	31897	2755	38965	6598
Maximum single link length [km]	4218	751	4229	564	3745	195
Number of hops	35	14	15	3	19	4
Entanglement rate [Bell pairs / s]	11.196	3.224	11.786	1.194	13.175	0.724

Table 5.4: Average and standard deviation of the evaluated parameters for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.

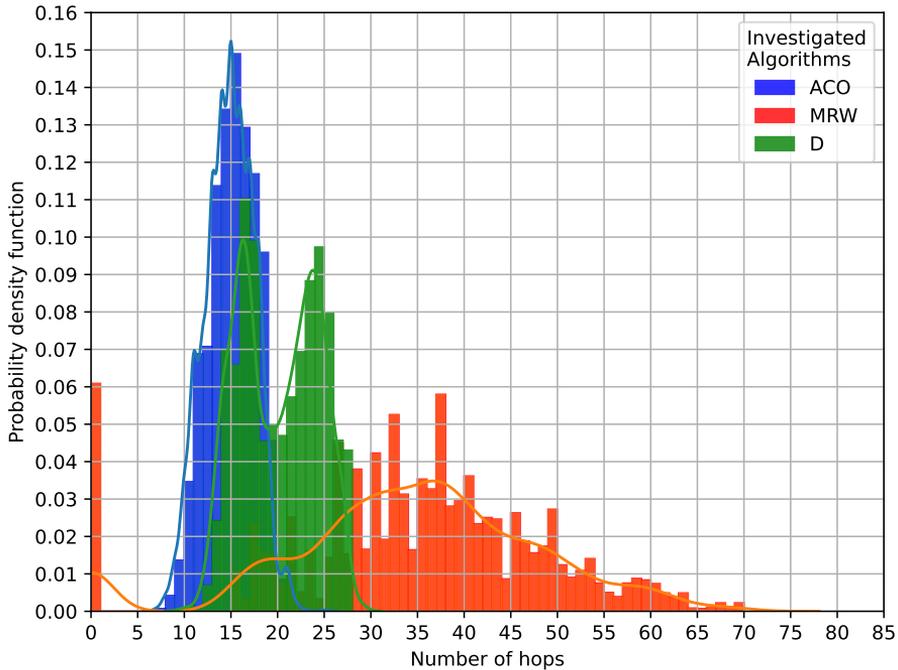


Figure 5.13: Number of hops Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.

Finally, the distance between the two GSs has been varied starting from a distance of 1000 *km* up to the antipodes with a step of 1000 *km*. As can be seen from Fig. 5.15, Dijkstra’s algorithm provides better performance than the other ones. However, ACO has a similar trend managing to achieve similar performances.

As shown in the Figures and Table 5.4, the values achieved are not very high, due to the current technological limits of the devices. The results already allow us to understand which could be the best routing policies to be adopted on entanglement based networks. The centralized solution based on Dijkstra’s algorithm allows reaching higher average entanglement rates this is because, although the E2E section is longer a greater number of nodes are also involved, which allows for shorter inter-node links. The fact of being able to obtain short inter distances increases the probability of success in the generation of Bell pairs.

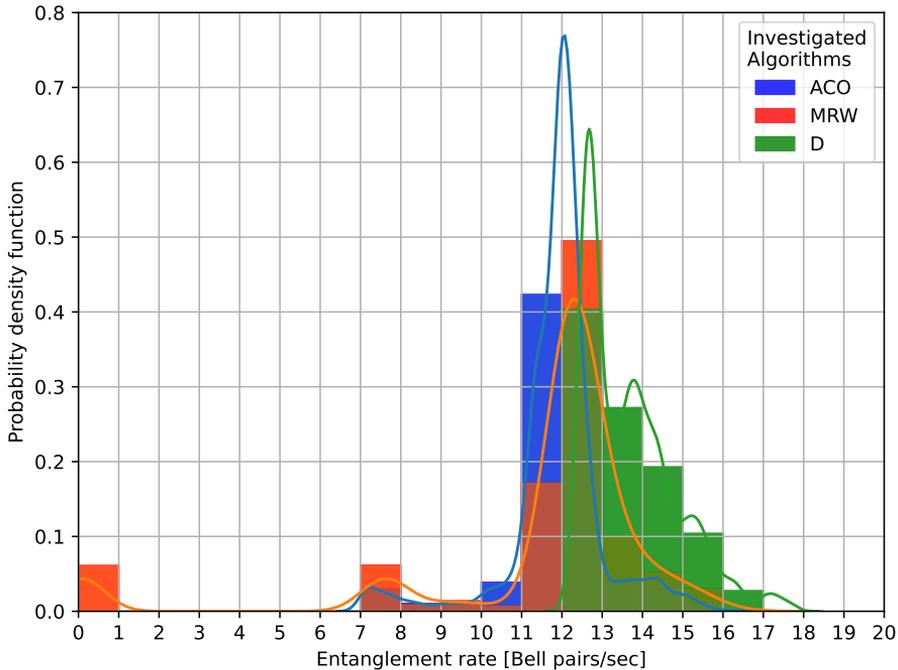


Figure 5.14: Entanglement rate Probability Density Functions for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.

Despite the application of ACO in network routing has many advantages, there are some unsolved problems when it is applied in satellite networks. The routing algorithm is limited by the mobility of satellite networks, and satellite handover could bring negative influence to the performance [404]. In particular, ACO's performances appear similar to that of Dijkstra's algorithm, but the speed of scenario variation due to the displacement of satellites in LEO orbit may require extremely high signal traffic for ACO. Moreover, as described in [405] [406], considering that the algorithm is computationally complex and has a slow converges speed, it could not be suitable for real-time business with a large volume. Therefore, an SDN-based architecture as well as higher values in terms of entanglement rate guarantees shorter convergence times in the calculation of the optimal solution and better strategies both in terms of entanglement propagation and swapping procedures management.

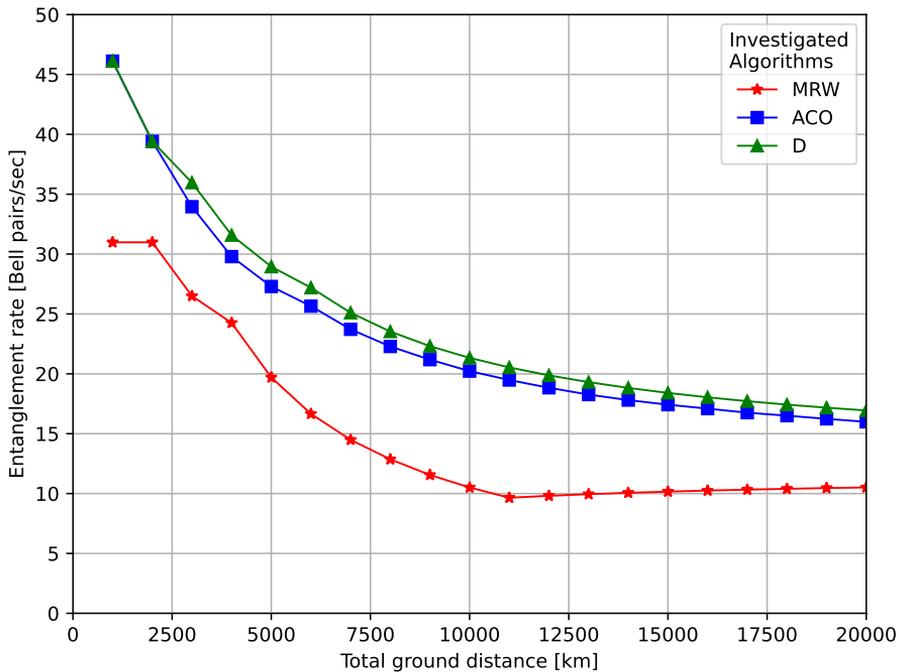


Figure 5.15: Entanglement rate as the distance between GSs varies for the considered MRW, ACO and Dijkstra protocols [20] ©2020 IEEE.

5.3.4 Satellite Constellations

Satellite systems have the advantage of global coverage and inherent broadcast capability and offer a solution for providing broadband access to the end-users. In many constellations direct Inter-Satellite Links (ISLs) provide communication paths among satellites and they can be used to carry signaling and network management traffic as well as data packets. Compared to GEO satellites, LEO and MEO satellite networks have shorter round trip delays and lower transmission power requirements [407].

Recently, the number of satellite missions has had significant growth with different aims, such as weather monitoring, disaster prevention, and space observation, involving several fields such as telecommunications, astronomy, Earth observation, and atmospheric science. Furthermore, the size of these objects has decreased significantly such that these objects are defined as micro-, nano-, and pico-satellites. The main advantages of small LEO satel-

lites reside in the much lower cost, low communication latency, high fault tolerance, and low energy consumption. Specifically, microelectronics allows decreasing satellite mass, getting power savings, and increasing flexibility as well as robustness. Currently, all electronic systems can be embedded in objects whose weight is only few kilograms instead of few tons and whose size is in the order of centimetres instead of metres. A CubeSat has to be made by one (1U) or more (nU) 10 x 10 x 10 cm cube units, with a mass of up to 1.33 *kg* per unit. The great attraction of this product is that it can be entirely built by using Commercial Off-The-Shelf (COTS) hardware components that better fulfil the target mission keeping low construction cost [408].

Moreover, these small satellites have also already been considered in the context of quantum communications. Specifically, in [409] was designed a 3U CubeSat for the implementation of the BB84 protocol.

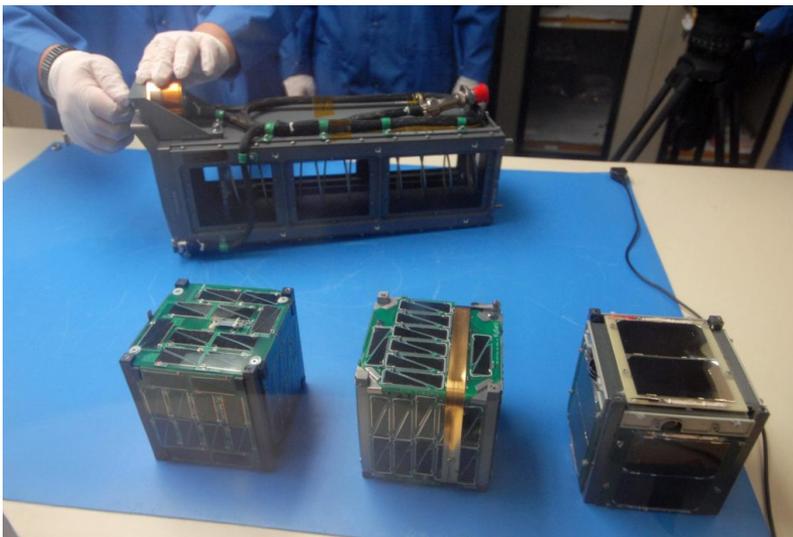


Figure 5.16: An example of Cubesats.

Therefore, this thesis investigates and compares three different constellations designed considering the flight plans of the following real constellations:

- A MEO constellation based on GPS, which consists of a nominal constellation of 24 satellites located at average altitudes of 20200 *km*.

- A LEO constellation based on Iridium-NEXT made up of 75 satellites, 66 cross-linked satellites and 9 in-orbit spares, at an altitude of 800 *km* [373].
- A constellation composed of 179 CubeSats, which are miniaturized satellites used so far for space research [410] [411] deployed in LEO orbit.

The orbits of the satellites that compose the considered constellations are depicted in the Figs.s 5.17, 5.18 and 5.19, which were extrapolated from the animations available on *CelesTrak* [412].

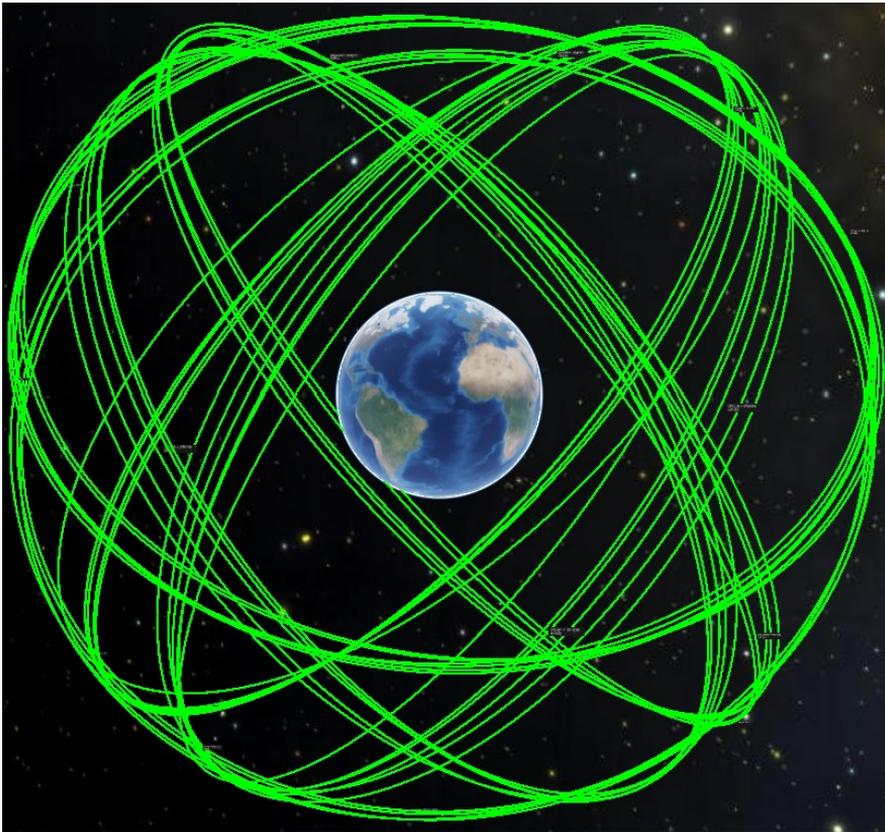


Figure 5.17: Orbits of the 24 satellites that compose the GPS constellation.

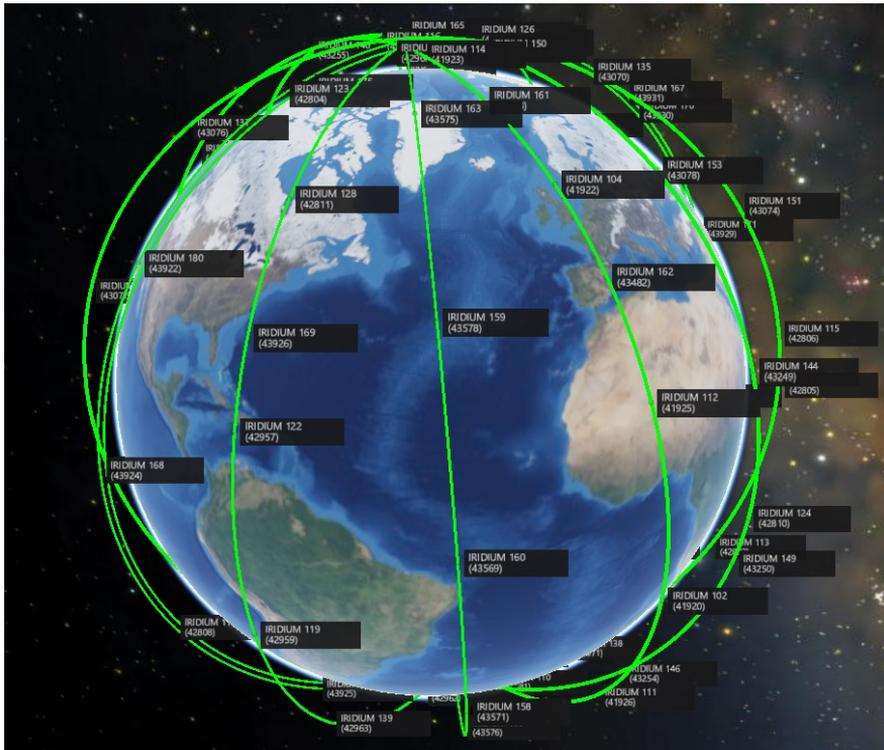


Figure 5.18: Orbits of the 24 satellites that compose the Iridium NEXT constellation.

From these Figs, it can be seen that the orbits are completely different, and also the numerosity of the constellations changes. It is important to note that despite the satellites that compose the CubeSats constellation shown in Fig. 5.19 are in LEO orbit, they operate at slightly different altitudes from each other, having been launched by many space agencies with different objectives. In addition, the distance of the satellites from the Earth's surface should also be considered. As a matter of fact, despite all three constellations providing global coverage, in designing a QNs ensuring global coverage efficiently, it is important to take into account the inter distances between QSRs. Therefore, in a satellite scenario, it is necessary to investigate which constellation ensures the best performance.

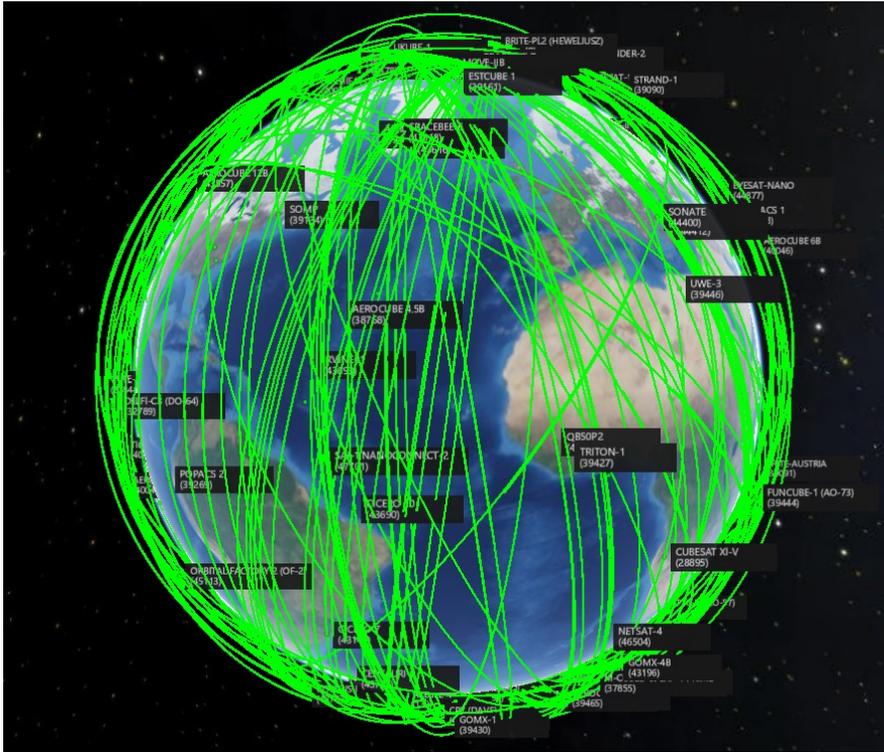


Figure 5.19: Orbits of the 179 CubeSats launched by various space agencies.

5.3.5 Simulations Results

In this Section, the performance achievable by different satellite constellations are investigated in order to set up efficient quantum E2E communications. In particular, we investigated three possible satellite backbone located at different altitudes as presented in Sec. 5.3.2 by always applying the Dijkstra's algorithm, as it represents the upper bound for assessing the path selection metrics. In order to carry out the experiment we wrote some Python scripts that considering the TLE files they produce the matrix of inter-satellite distances and they apply on it the centralized algorithm. In particular, we used the following libraries: the *Skyfield* Python package to operate on TLE files and obtain the satellites data, and the Dijkstra's algorithm included in the *scipy* package. Tests were carried out by connecting two stations placed on the Earth's surface for sixty minutes and capturing

a sample every 500 *ms*. In Fig. 5.20 the E2E entanglement rate is depicted by varying the distance between GSs with a step of 10^3 *km* until reaching antipodal coordinates. It can be firstly noticed that the MEO constellation achieves the lowest performance no matter the GSs distance was, due to the predominant Earth-to-satellite length. In addition, it can be seen that as soon as GSs are close the better choice is the Iridium-Next constellation, but in the other cases, it is preferable a constellation made up of CubeSats.

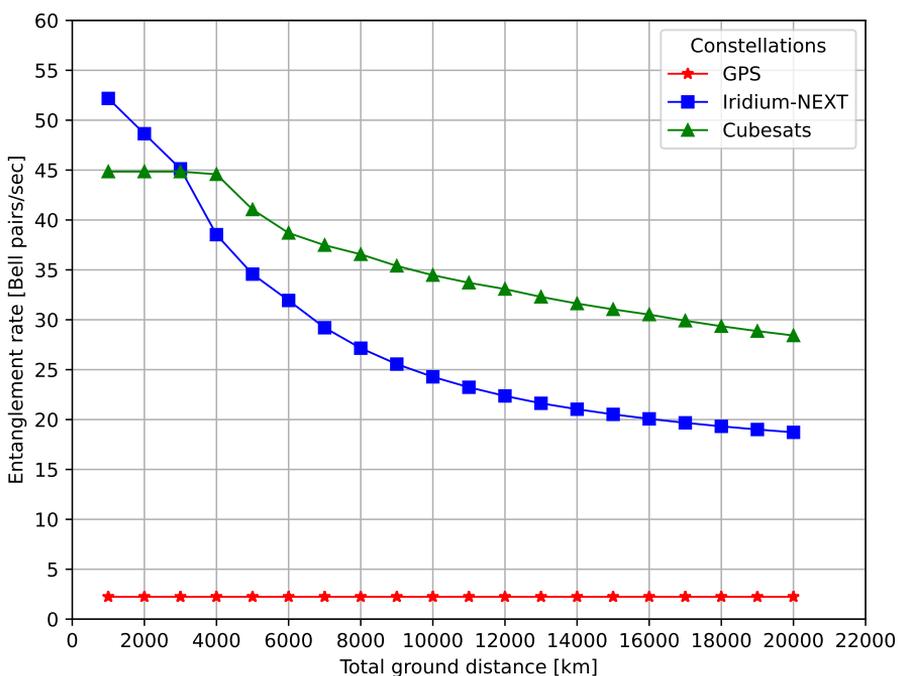


Figure 5.20: E2E entanglement rate considering different distances between GSs [21] ©2021 IEEE.

The previous considerations are corroborated by Fig. 5.21, where the maximum link length within the best E2E path is represented as a function of the distance between a couple of ground terminals. In particular, it is easy to understand the better performance of the Iridium-NEXT w.r.t. the Cubesats constellation for distances lower than $3 \cdot 10^3$ *km* as highlighted in the zoomed subfigure.

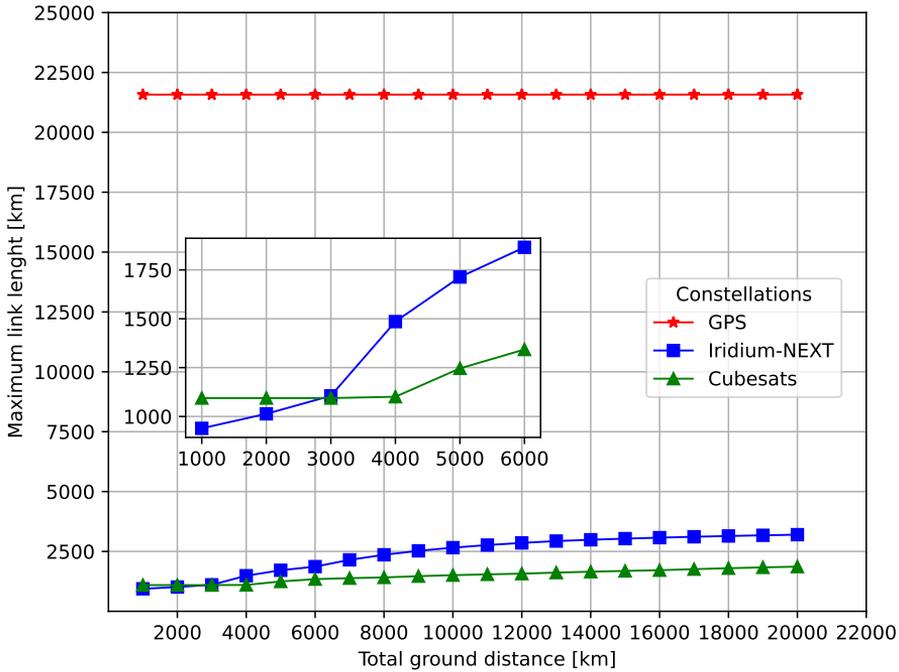


Figure 5.21: Links of Maximum link length within an optimised E2E path as a function of the distance between the GSs for different satellite constellations [21] ©2021 IEEE.

The probability density function of the achievable entanglement rate obtained by simulating 1 hour of our systems in is sketched in Fig. 5.22, that again confirms the better performance of the Cubesat constellation in terms of mean value, while again the overlapping with the Iridium-Next one is motivated by the analysis conducted in Fig. 5.21. However, the most unsuited constellation is represented by the GPS one with an average entanglement rate of approximately 1/10 with respect to the other performances.

To conclude our investigation, we evaluated the appropriateness of the *static* Dijkstra approach when applied to a time varying graph. In order to simulate the satellite system stationarity, we focused on a specific worst case scenario, where the GSs are deployed in the Earth Poles. Without lack of generality, we consider only the Iridium-Next constellation and we first evaluate the duration of the path (τ_{sbp}) selected by Dijkstra's algorithm in the initial time instant (called *static best* path), which allows to upper-

bound a typical E2E session duration. It is worth noticing that τ_{sbp} depends on the time interval in which the involved satellites QRs are in line of sight with each other. As shown in Fig. 5.23, τ_{sbp} statistical distribution is mainly concentrated over the interval $[0, 200]$ s, with mean value equal to 150 s. The estimation of this parameter value can support the SDN Controller to evaluate an effective solution to perform an entanglement, while limiting the signalling overhead.

To this purpose in Fig. 5.24, the performance of the static best path w.r.t. the second best path, in terms of E2E entanglement rate is presented. It can be pointed out that in a specific time interval of about 20 s, where the satellite inter-distances vary over time, but the QRs constituting the static best path do not, the best performance is achieved by the Dijkstra approach that could be assumed a correct solution to our problem.

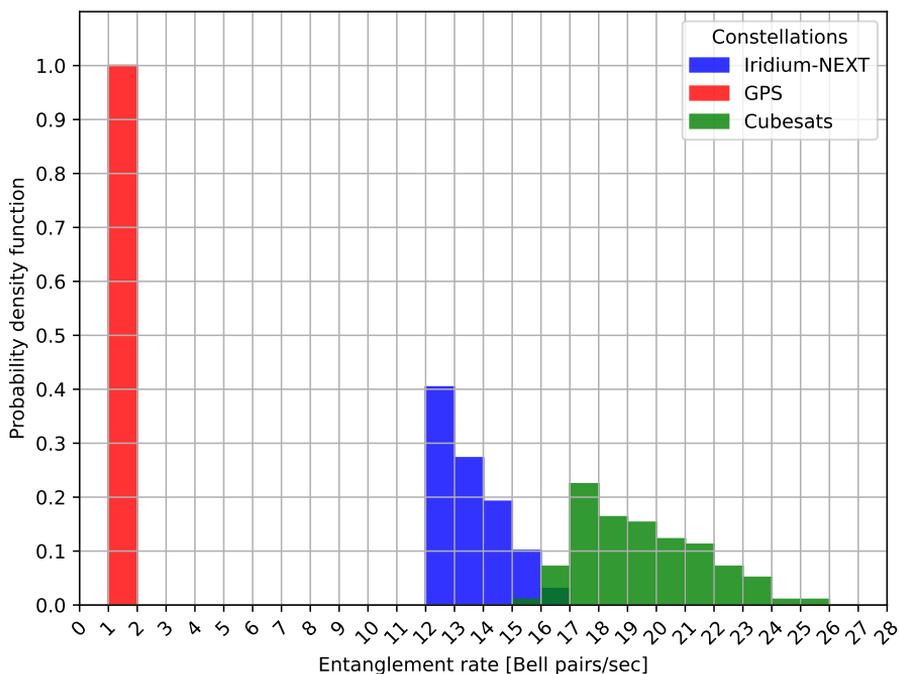


Figure 5.22: PDF of the entanglement rate achievable by the different satellite constellations [21] ©2021 IEEE.

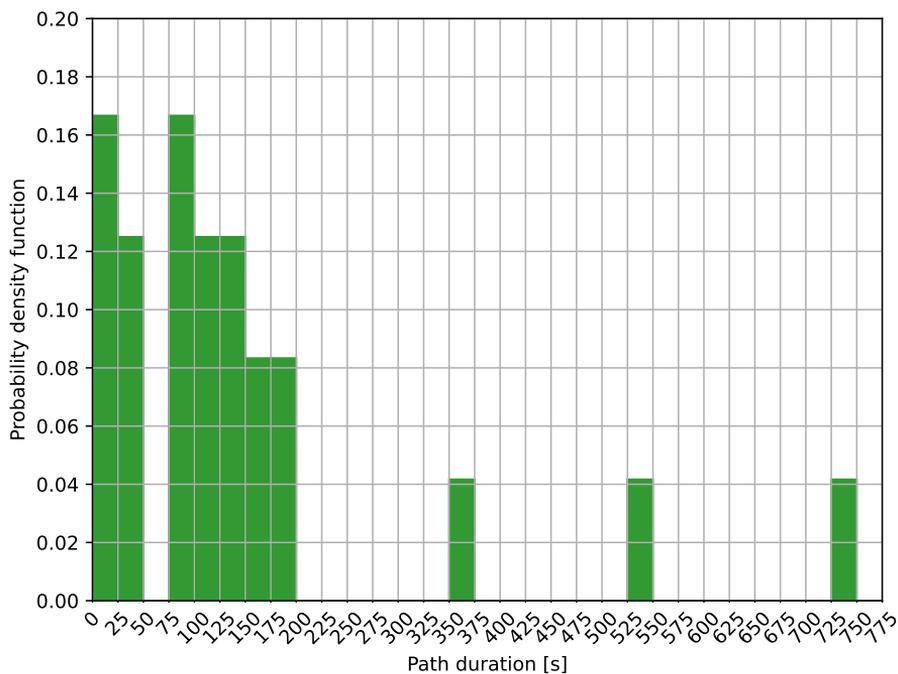


Figure 5.23: PDF of the path duration achievable on Iridium-NEXT [21] ©2021 IEEE.

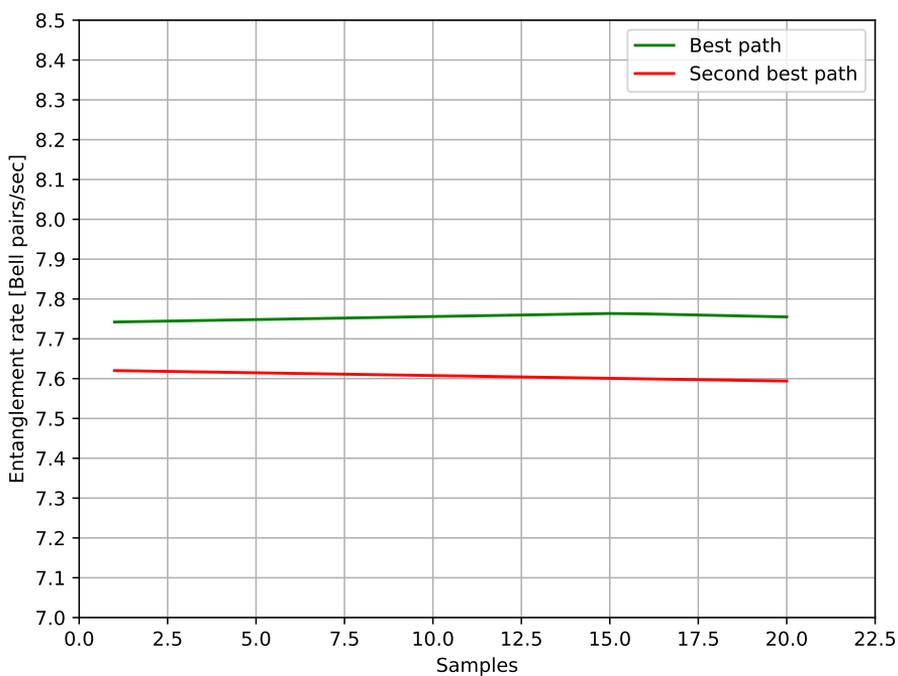


Figure 5.24: Performance of the static best path in terms of entanglement rate [21] ©2021 IEEE.

5.4 Satellite Control Plane Solutions Analysis

This Section investigates two architectures in which the SDN Controllers are integrated into the satellite constellations. The possibility of integrating CP into the DP may allow for some advantages, such as being able to perform some operations locally while reducing the overhead. Specifically, these architectures are based on the possibilities stated in Section 4.4.3, which are distributed and hierarchical solutions. The latter is a solution that considers a logically centralized root Controller which takes decisions that require network-wide knowledge.

5.4.1 Modular two-tier Control Plane

The design of an efficient quantum satellite backbone requires extremely accurate control and the SDN technology could be fundamental to achieve this goal. In order to increase the generation rate of Bell pairs on the selected path an appropriate path selection algorithm is required. These are the functions of the MCS depicted in Fig. 5.25.

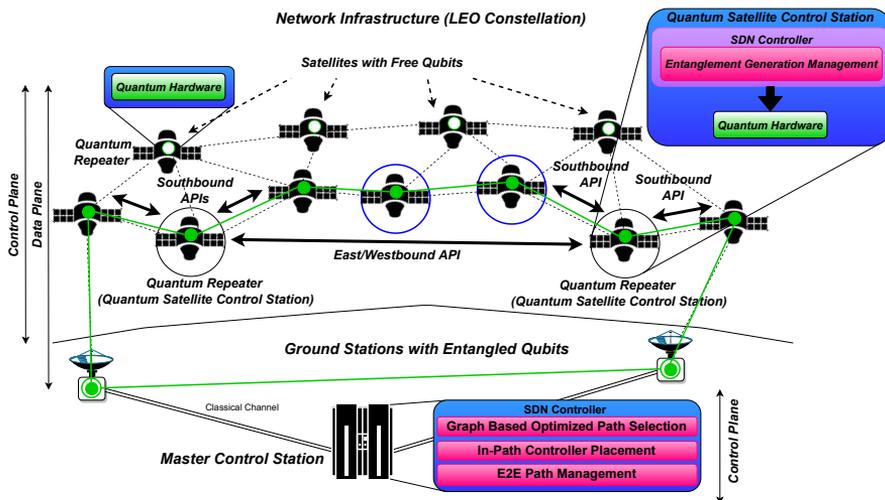


Figure 5.25: QSDN backbone architecture. A Bell pair is generated between GSs through operations driven by the Controllers embedded in the LEO constellation.

Moreover, considering that the management of swapping procedures could increase the overhead, it is relevant to minimize it especially for distributed operations [11]. This goal can be achieved by efficient management of entanglement generation and swapping operations by the CP integrated into the constellation itself.

The following Sections describe in detail the architecture together with the protocol and the related messages exchanged.

5.4.1.1 Proposed Architecture

Several satellites in low orbit are considered in the presented architecture to overcome the distance problem, as shown in Fig. 5.25 [20] [21] [66]. The use of a dense constellation close to the Earth's surface allows the distance problem to be addressed as described in [21]. In fact, as explained in [66] the probability of success in entanglement generation decreases exponentially as a function of distance and the time required to generate the entanglement between two adjacent nodes strongly depends on this probability and the characteristics of the medium. Therefore, in our paper, we considered a single LEO constellation whose all the elements can embed SDN Controllers. The elements that are part of the DP, i.e., the QSRs and the GSs, as depicted in Fig. 5.25, operate in the frequency range of FSO, described in [20]. Atmospheric factors and beam wandering limit the FSO performance significantly [222] especially regarding Earth-to-Satellite communications, but adequate performance can be achieved in fair weather conditions using the 193.415 THz frequency. Optical technology can be used not only for the quantum channel but also for the control channel. In fact, all nodes in a QN are assumed to have classical connectivity between each other in order to perform background protocols, such as path selection as well as signaling protocols to set up the E2E entanglement generation [79]. Furthermore, at the considered frequencies the space vacuum has a much higher *attenuation length* [20] w.r.t. OFs. For these reasons, we have considered the realization of a satellite backbone managed by a MCS on the ground with an SDN Controller embedded, which derives the matrices of intersatellite distances. Then, a *graph based optimized path selection algorithm* that calculates the best path is applied on the derived matrices [21]. The MCS calculates and manage the best path communicating with the satellites through the south-bound APIs. This architecture, shown in Fig. 5.25, also includes the use of multiple Controllers embedded in the constellation, whose proper placement

helps to reduce the delays between them and the satellites acting as QRs, thus making it possible to completely avoid the terrestrial routes and, in particular, the earth satellite link, which is the most critical due to atmospheric phenomena. As explained in [375], the starting point from which to start generating Bell Pairs [413] affects the speed of entanglement propagation over the entire path. A first attempt which considers the use of SDN technology to address this problem has been made in [20], in which is described an architecture wherein the satellite *in the middle* is detected by a single Controller on the ground, which sends to the selected satellites the necessary instructions to start the propagation procedure interfacing with them through the southbound APIs.

However, with the proposed architecture shown in Fig. 5.25, which uses a modular two-tier CP based on SDN, it is also always possible, thanks to the intervention of the MCS, to activate the control process on an appropriate satellite along its domain, which is composed of several satellites that compose the path. The satellites that delimit the borders between one domain and another are identified as *border QSRs* highlighted with a red circle in Fig. 5.25. The satellite Controller manage the operations of entanglement generation and swapping, reducing both the time required for the propagation of the L2L entanglement and the propagation delays of signaling packets. The placement of the Controller in the middle of the path section as depicted in Fig. 5.25 is fundamental to optimize Bell Pairs propagation and minimize packet delay to and from the Controller. Moreover, is possible to avoid the satellite to ground link which is the most critical. In the following Section, it is described in detail the functioning of the protocol and the messages that are exchanged.

5.4.1.2 Protocol

The proposed protocol is designed for the architecture defined in Fig. 5.25 and it is organized in two main phases:

1. Management of the connection request between GSs and setup of the satellite path.
2. Generation of E2E entanglement using the configured satellite path.

In order to manage these operations properly, we have defined also a specific packet format, which is depicted in Fig. 5.26. The fields that compose the defined packet are described as follows:

- **Type:** this field is composed of 4 bits and it defines the type of packet.
- **C:** this is a field composed of a single bit. It is useful in order to enable the Controller functionality on a specific satellite if the field **Type** is set on 3 or if the field **Type** is set on 8 it is used in order to notify that the inter domain teleport between two border QSRs is completed.
- **Duration:** this field contains the life time of the path. It is important in order to program the opening and closing of the connections between the satellites that compose the path.
- **Source:** this field contains the address of the source of the message that could be the MCS or a satellite Controller.
- **Destination:** this field contains the address of the destination of the message.
- **Previous:** address of the previous satellite.
- **Next:** address of the next satellite.
- **Teleportation Data:** this field contains the classic bits related to teleportation.

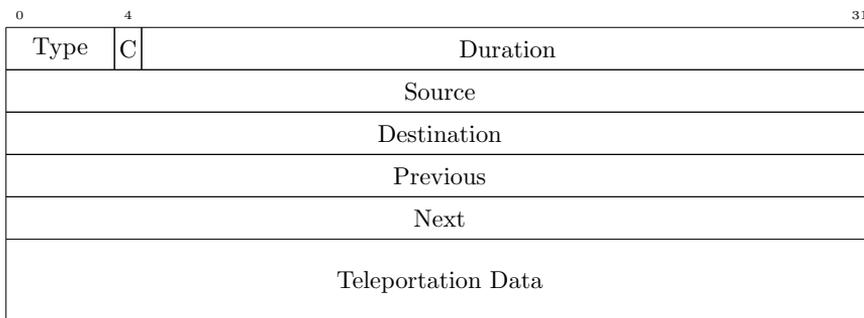


Figure 5.26: Packet format used by the protocol designed for the proposed architecture [22].

In the first phase, which is depicted in Fig. 5.27, the MCS processes the connection request from one of the GSs located on the Earth's surface. In this case, the message received by the MCS consists of the **Type** field set to

0 and the **Previous** field that contains the IP address of the GS to which it wants to connect. Thus, the Controller in the MCS calculates the best paths for all instants of time, creating a list through which it is able to obtain the duration of every best path.

At the same time, it sends the connection request to the selected QSRs and a message that has for fields the **Type**, which in this case is identified with 1 and the **Previous** field which contains the address of the station that has generated the request.

When the station affirmatively acknowledges the request, the MCS begins to perform the setup of the satellite path by sending messages of **Type 2** to each satellite that is part of the selected path indicating which is the neighboring satellite to connect to. Furthermore, the satellite recover the value of the field called **Duration**, in order to set a timer that closes the connection when the path is expired.

Once the Controller has received notification from the satellites of the selected path that all the connections have been established, the second phase of the protocol begins. As shown in Fig. 5.28, it involves the generation of entanglement on the selected satellite path and it has a duration equal to the value specified in the field **Duration**, which corresponds to the duration of the satellite path.

The MCS sends to the satellites chosen as Controller a message of **Type 3** that indicates the ability to perform certain operations on a domain that is specified in the message itself in the fields **Previous** and **Next**.

The Controller generates two pairs of particles to share with the two adjacent satellites in the path and sends a **Type 4** message to the remaining satellites, specifying the satellite to perform the entanglement with. In addition, the first Controller on the path sends a **Type 5** message to the second Controller in order to negotiate the generation of entanglement between two satellites. In this type of message, the **Previous** and **Next** fields indicate the satellites to be interconnected. When the acknowledgment is received the swapping procedure is started to generate the entanglement at level E2E.

A **Type 6** message which contains the field is sent to the satellite that has to perform a swapping operation. In this type of message, the **Previous** and **Next** fields indicate the satellites that will be interconnected after the swap operation. The internal swapping operations of each domain are performed simultaneously by the Controllers on their own domains. When a Controller has completed its operations, i.e. the creation of the E2E entanglement

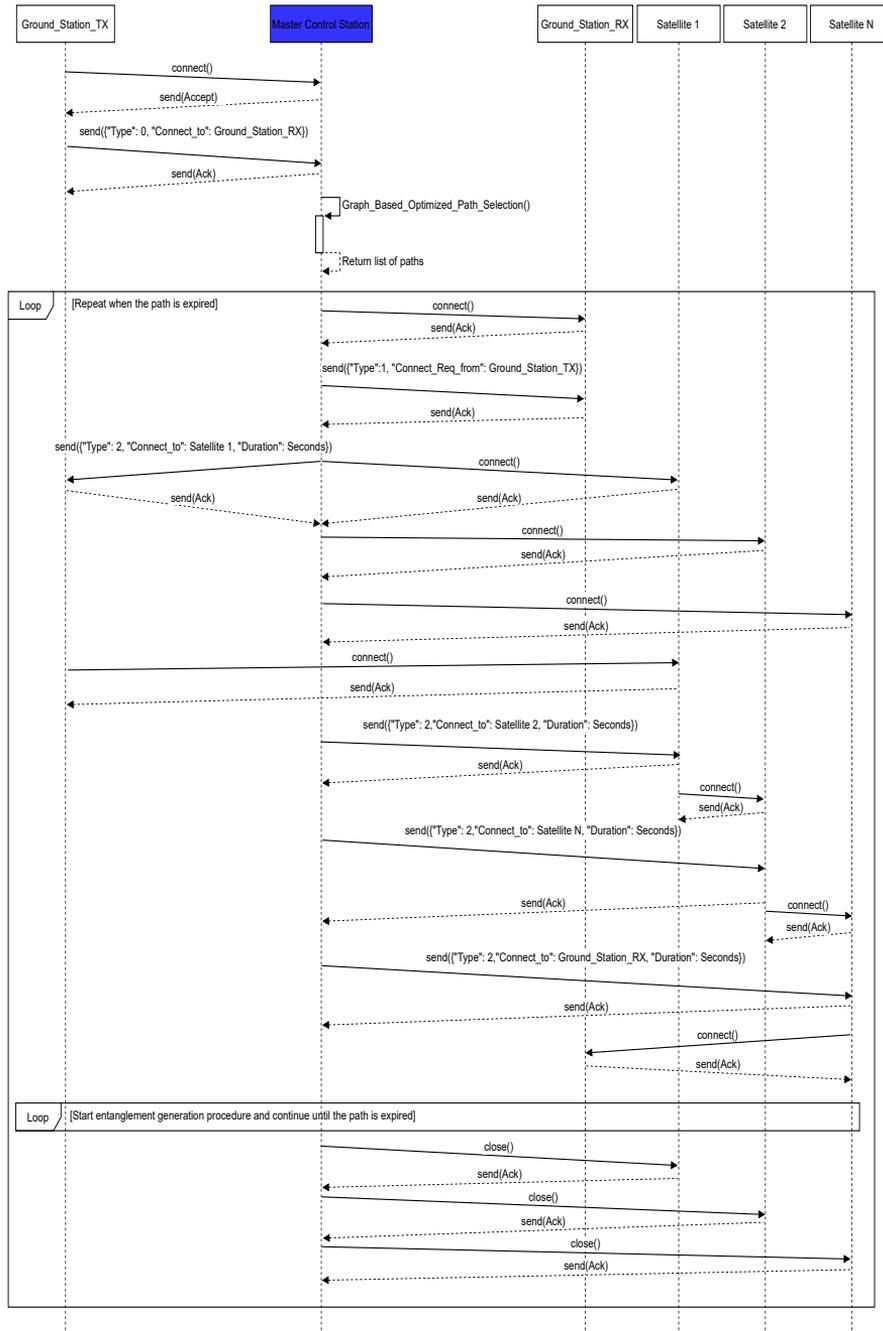


Figure 5.27: Sequence diagram of the first phase of the protocol. The MCS performs the setup operations on the selected path [22].

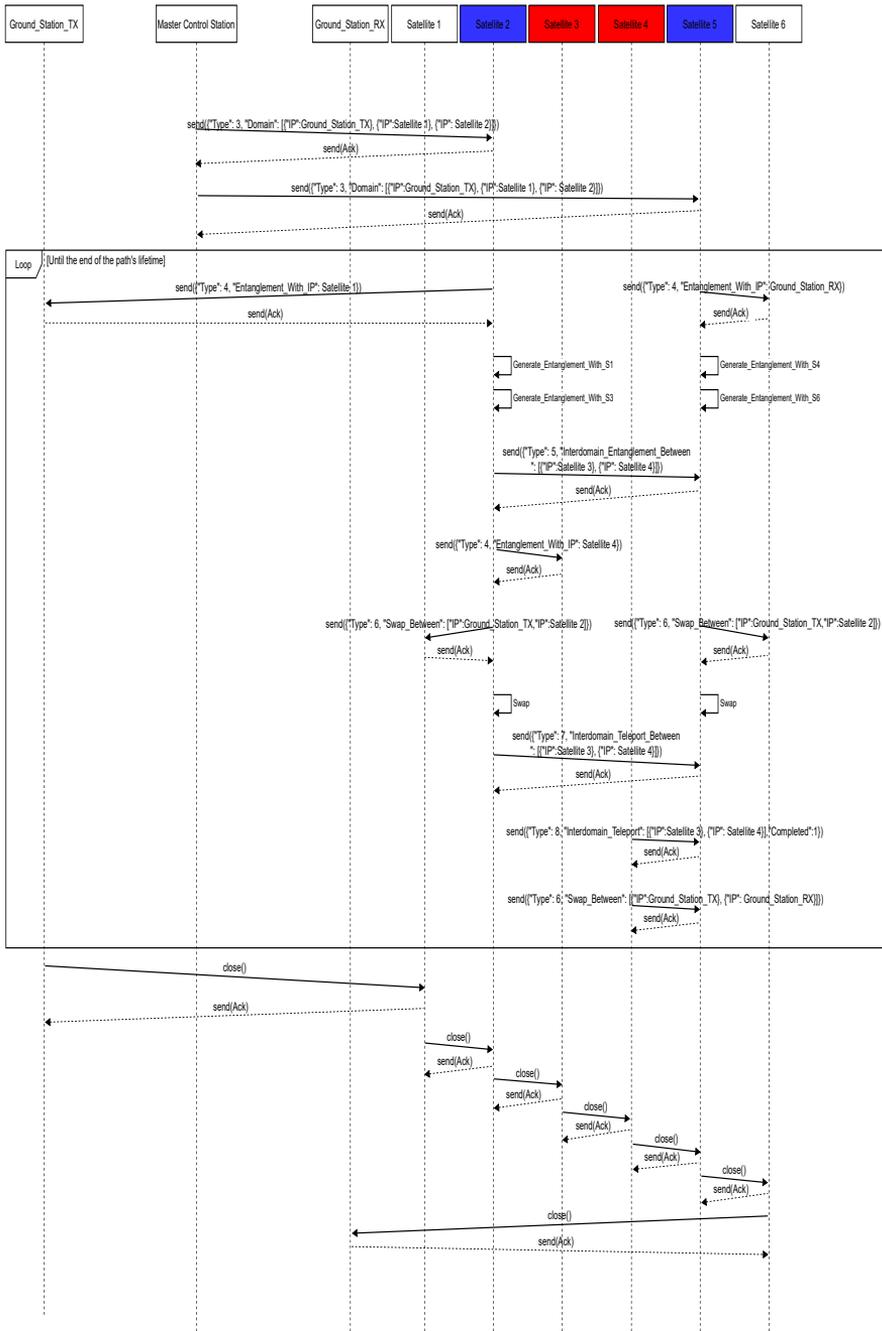


Figure 5.28: Sequence diagram related to the second phase of the protocol. The Controllers placed on the path manage the entanglement generation and swapping operations [22].

between the GS to which it is connected and the border QSRs highlighted with a red circle in Fig. 5.25, it sends a request to the other Controller with the purpose of interconnecting the border satellites.

This is done with a **Type 7** message and in this case the **Previous** and **Next** fields indicate the satellites between which to perform the teleportation operation.

When the teleportation process is completed, a **Type 8** message is sent from the border satellite that received the particle to its Controller with field **C** set to 1, indicating that the teleportation between the two border satellites has been completed. At this point, the Controller sends a **Type 6** message to its border satellite to perform the swapping operation. When this operation is completed, the entanglement E2E is established and the procedure can start again to perform the exchange of successive qubits.

When the path is not valid anymore, a condition that can be detected by checking the list of paths calculated by the Graph Based Optimized Path Selection process on the MCS, the satellites close the connections established with the others. Then, the Controller processes are deallocated and the Controller in the MCS closes the connections with the satellites involved up to that moment. Then the procedure restarts until the end of the session.

5.4.1.3 Simulations Results

In order to investigate the performance of the architecture and the protocol that we propose, we have conducted a simulation in order to verify the time required to obtain an entanglement between two GSs using a quantum satellite backbone. In order to develop the software, we used the **Skyfield** Python package to operate on the TLE [400] [357] data to calculate the inter distance matrices, as performed in the study described in Section 5.3.3, and the Dijkstra's algorithm included in the *scipy* package. In the scenario that we have simulated, we used the Iridium-NEXT constellation, composed of 75 satellites. We have considered the activation of two Controllers on the path selected by the MCS, and we performed a simulation considering a reference time interval of 1 *h* capturing a sample every second. The GSs have been located at a distance of 20000 *km* from each other. During the simulation the number of satellites that compose the best path varies from 4 to 6, then we have derived a different distribution for each case.

As can be seen from the graph depicted in Fig. 5.29 with an increase in the number of satellites involved, the time required to generate a remote

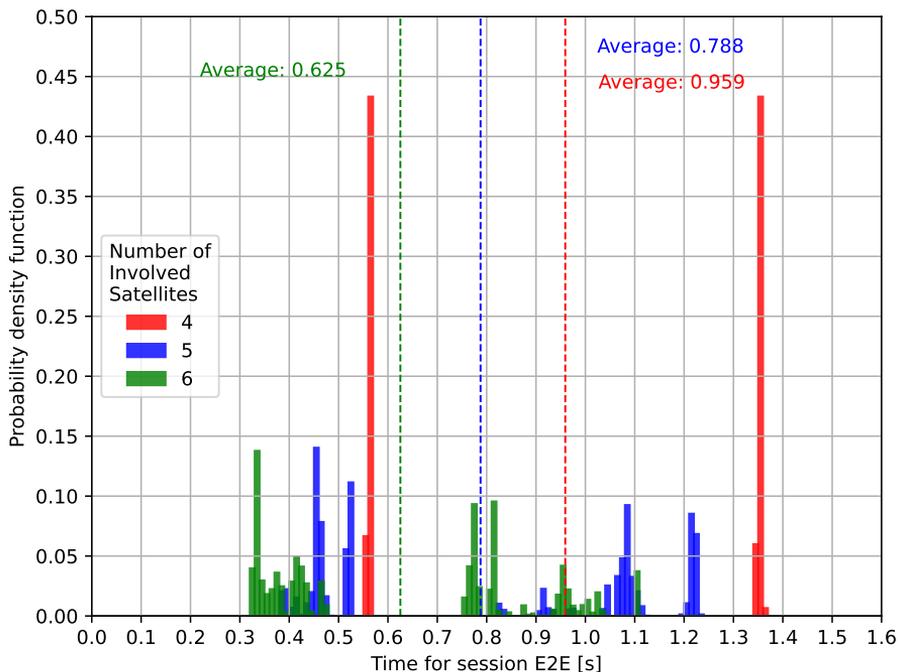


Figure 5.29: Time required to establish an entanglement E2E [22].

entanglement decreases. This fact confirms in part what has been claimed in [21] and in [20], i. e., that a larger constellation allows obtaining better results in terms of entanglement rate, defined as the number of transmitted entangled states per second, which is measured as Bell pairs per seconds [20].

From the graph in Fig. 5.29 it appears that considering the same number of Controllers within the path, performance improves as the number of satellites increases. This is because given the shorter distance the probability of success in order to obtain an entanglement increases. Since the time needed to obtain the entanglement strongly depends on this probability, the time needed to obtain it decreases.

This provides a first indication that as the number of satellites that compose the path changes, the performance of the protocol is not degraded, but the beneficial effects of the distance between the satellites that compose the domains can be seen. Further studies on scalability could provide useful indications for the realization of an intelligent architecture in which the MCS

allocates an appropriate number of Controllers inside the path in order to achieve effective quantum communications.

5.4.2 Multiple Controllers Integrated into the Constellation

Before providing a description of the architecture that we have defined it is important to describe some phenomena that are necessary to consider, to support efficient quantum communications and processing.

As explained in [66], the probability of successfully generating remote entanglement between two adjacent nodes is highly dependent on the distance and the characteristics of the propagation medium with an exponential decay. Compared to OFs, a free-space photon experiences negligible loss in vacuum [20].

When decoherence occurs, some qubits of the computation become entangled with the environment, collapsing the state of the QC. Then, once a qubit has decohered, the entire computation of the QC is corrupted, and the result of the computation is no longer be correct [414].

To obtain an over long distance entanglement QRs are then necessary. These devices perform the entanglement swapping procedure, which works as it follow. Considering two independent entangled pairs A-B and C-D, a Bell-state measurement on B and D projects A and C onto an entangled state, although these two particles have never interacted [20].

Based on the previous considerations, in order to design an efficient satellite QN backbone, some basic requirements need to be addressed. It is clear that this system requires an extremely accurate control and therefore SDN technology could be proven to be fundamental for this type of network. Besides, an appropriate path selection algorithm could help to increase the rate on E2E routes by properly selecting QRs that compose the path. Furthermore, considering that the management of swapping procedures could increase the overhead, it is relevant to minimize it especially for distributed operations [11]. These are the two main functions of the Controller depicted in Fig. 5.30.

Based on previous considerations, we proposed some guidelines through the design and dynamic placement of the CP within the constellation itself and some E2E entanglement generation strategies with the aim to identify the one that can provide the best performance for the derived architecture.

5.4.2.1 Proposed Reference Architecture

Considering that as is described in [66] and [20] distance represents a serious impairment for QNs, it may be preferable to consider a constellation consisting of a large number of satellites placed in a low orbit such as LEO, as also recommended in [21].

The QSRs and the GSs, which are the elements that compose the DP can operate in the same range of frequencies described in [20] that is, FSO. In fact, FSO is a technology that has found application in several areas of the short and long-haul space communications, for instance on inter-satellite links, and it has already been used in the realization of quantum communications on Earth [415]. The performances of FSO systems are usually limited by atmospheric factors and beam wandering [222] especially regarding Earth-satellite communication, but considering a wavelength equal to 1550 *nm* the atmospheric absorption is negligible in clear air conditions making it a favorable wavelength for FSO applications. Compared to optical fiber, the space vacuum has a much higher *attenuation length* [20] at the considered frequencies. For this reason, we have considered the realization of a satellite backbone with the Controller embedded in the constellation in order to further reduce the delays between it and the satellites acting as QRs. Besides, the control virtual process migration is crucial in this architecture. Indeed, it is always possible to deploy the control process on an appropriate satellite in the middle of the path [375] to reduce both the time required for the propagation of the L2L entanglement and the propagation delays of signaling packets.

This type of architecture provides significant advantages, considering that it allows to significantly reduce the losses related to the links between the GSs and the *first* satellite, which is the more problematic one, considering that optical communications are subject to scattering phenomena due to the presence of water particles in the atmosphere that varies according to weather conditions. These problems are related both to the quantum link and to the classical link on which the control packets are transmitted. However, with the proposed architecture, only the packets exchanged between the GSs and the *Quantum Satellite Control Stations (QSCSs)* will have to pass through these links. Moreover, fiber optic terrestrial connections between the Controller and GSs are also avoided, allowing losses to be neglected. Finally, since the distances are very high and the Controller is in charge of managing the operations between the satellites, this helps to limit the propagation delays,

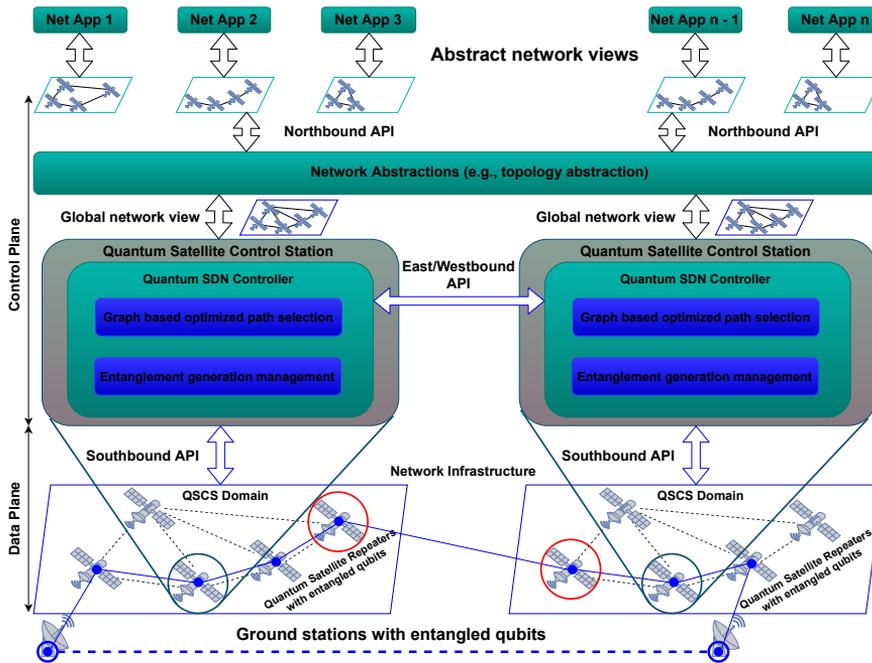


Figure 5.30: QSDN backbone architecture. A Bell pair is generated between GSs through operations driven by the Controllers embedded in the LEO constellation [23] ©2022 IEEE.

that given the very high distances, are not negligible.

The proposed architecture is depicted in Fig. 5.30 wherein the domains that could consist of clusters of satellites of the same constellation in LOS to a QSCS are highlighted. The procedure that is performed in order to create an E2E entanglement operates as follows. Once the satellites that compose the E2E path have been selected, the Controllers of the individual domains perform the operations needed to create an E2E entanglement between the GSs to which they are connected and the *border QSR* that are highlighted in red in Fig. 5.30. When the intra-domain E2E link has been established, the domain Controller communicates this to the neighboring domain Controller that has independently performed the same operations. The Controller of the first domain sends the qubit to the edge satellite of the neighboring domain once the acknowledgment from the neighboring domain Controller is received. The edge satellite receives the particle and performs a swapping

operation in order to generate an E2E link between GSs belonging to the two distinct domains. At the end of the procedure, an E2E entanglement is created between the GSs.

5.4.2.2 Entanglement Generation Strategies

A QSCS in addition to the Northbound, Southbound, and East/Westbound API typical of an SDN Controller, also includes a module for the path selection and a module dedicated to the entanglement generation management, as depicted in Fig. 5.30. Whenever it was necessary to interconnect two GSs, the distributed application invokes the Controller's best path evaluation module via the Northbound API. The QSRs, which are the devices that make up the DP, generate and exchange entangled particles based on information provided by the SDN Controller embedded in the QSCS through the Southbound API.

In order to speed up the E2E coupling procedures, it is necessary to carefully choose an appropriate scheme for generating the entanglement. There are several basic schemes for generating entanglement on a link through the coordinated action of two end nodes. In this thesis, we focused, in particular, on two of these methods:

- *at source*: in this scheme, one of the two end nodes sends a flying qubit that is entangled with one of its matter qubits. A transducer at the other end of the link will transfer the entanglement from the flying qubit to one of its matter qubits.
- *at mid-point*: in this approach, an entangled photon pair source positioned between the two nodes with matter qubits sends an entangled photon through a quantum channel to each of the nodes [79].

In the considered scenarios, the *at source* strategy, which is depicted in Fig. 5.31a, works as described in the following. The L2L Bell pairs are generated according to the policy applied by the Controller, which sends a message to the GSs and all the satellites that are part of the path. Once the Controller receives the feedback messages, it sends a message to a subset of the selected satellites in order to perform the swapping procedure. The Controller continues it sending the relative messages to the remaining satellites until the entangled E2E link is established.

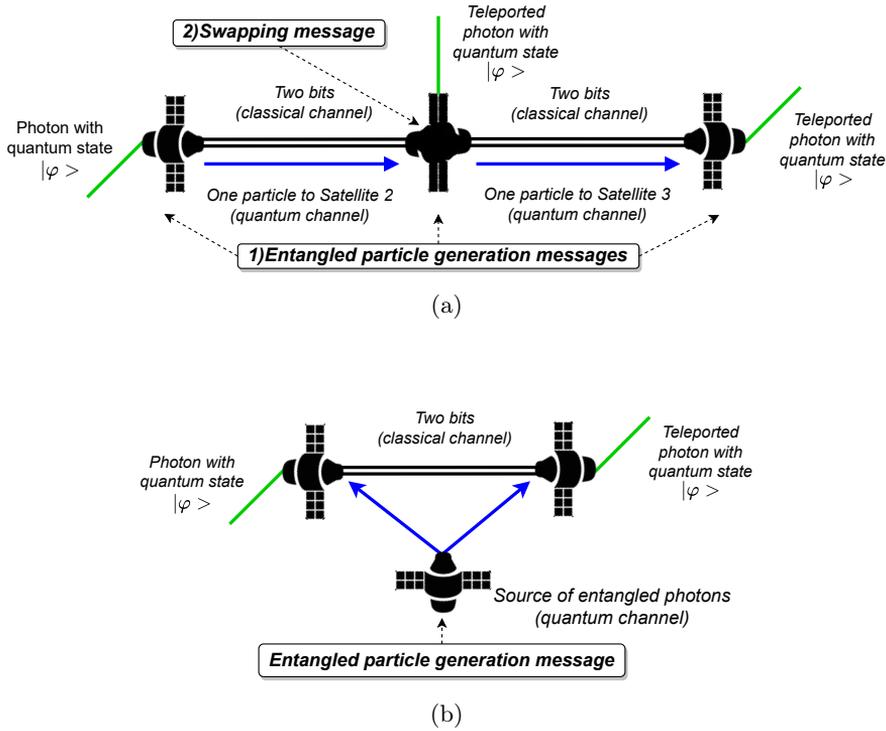


Figure 5.31: In 5.31a is represented how the *at source* strategy works, whereas in 5.31b is depicted an example of the *at mid-point* strategy.

The *at mid-point* strategy considers some satellites of the path as *generators* of Bell pairs, which sends the particles to other satellites that in turn perform the swapping operation, as shown in Fig. 5.31b. Hence, once the best path has been evaluated, QRs are assumed to have been properly selected by the Controller. With the *at mid-point* procedure, it is possible to avoid some swapping operations, considering that some satellites are only generators of Bell pairs and are, therefore, not involved in the swapping process.

5.4.2.3 Simulations Results

We have conducted a campaign of simulations with the objective of verifying the performance in terms of overhead and delay required to obtain an entanglement between two GSs using a quantum satellite backbone. According to

the considerations discussed in the previous Section, a constellation such as Iridium-NEXT, consisting of 75 satellites, has been considered in the simulated scenarios. As a first case, we considered a single Controller located on a satellite in a continental scale scenario and we performed a simulation considering a reference time interval of 60 *min* and capturing a sample every second. The GSs have been located at a distance of 10000 *km* from each other. We measured both the number of packets exchanged to generate a Bell pair between the GSs exploiting the satellite path and the latency required to achieve this E2E coupling. A comparison of the two strategies illustrated in Section 5.4.2.2 was performed and it shows that the strategy named *at source* results the more appropriate one, as can be seen from the graphs in Fig. 5.32 and Fig. 5.33. This is because the probability of success in generating an entangled particle pair with the *at mid-point* method is lower considering that both particles have to pass through the free space, hence, the total entanglement generation probability is given by the product of the probability of success on both the links.

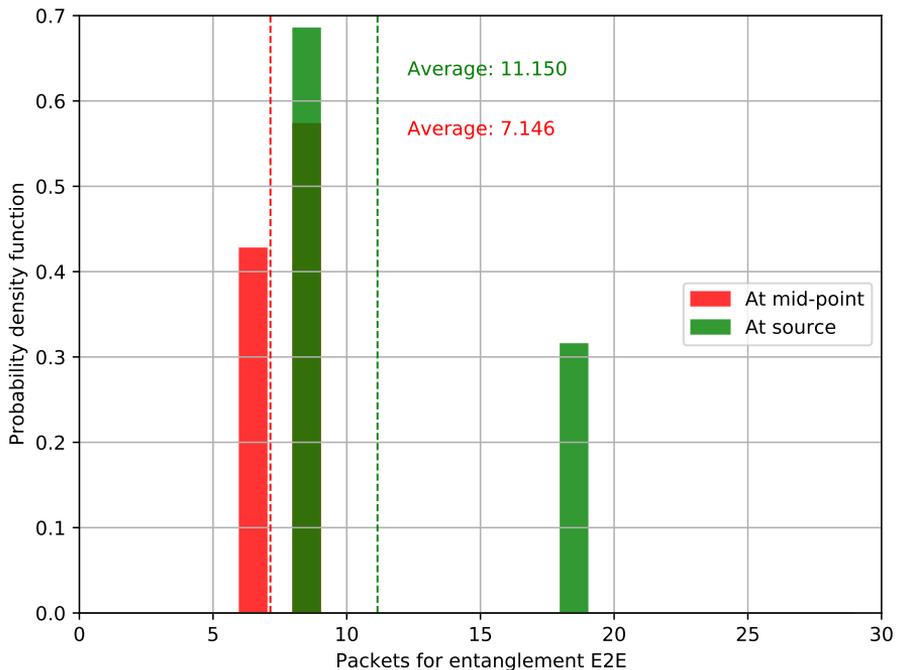


Figure 5.32: Packets exchanged for a single session using both strategies [23]
©2022 IEEE.

Having identified the best strategy we extended the scenario by placing the stations at the maximum distance possible that is at the Earth antipodes. We then compared two different architectures considering a single Controller positioned on the ground at 10000 km from the GSs and one controlled by two Controllers belonging to the constellation. As can be seen from Fig. 5.34 and Fig. 5.35, the scenario with multiple mobile Controllers allows achieving higher performance in terms of the overhead and the generation time of Bell pairs. The control protocol overhead is represented in Fig. 5.34, where it is possible to notice that the distribution of operations between two domains requires fewer packets to perform the total amount of operations. The improvement w.r.t. the architecture with a single Controller on the ground depends on the fact that part of the operations of entanglement generation and entanglement swapping are locally performed, without the need to send additional control messages considering that the CP is integrated into the DP.

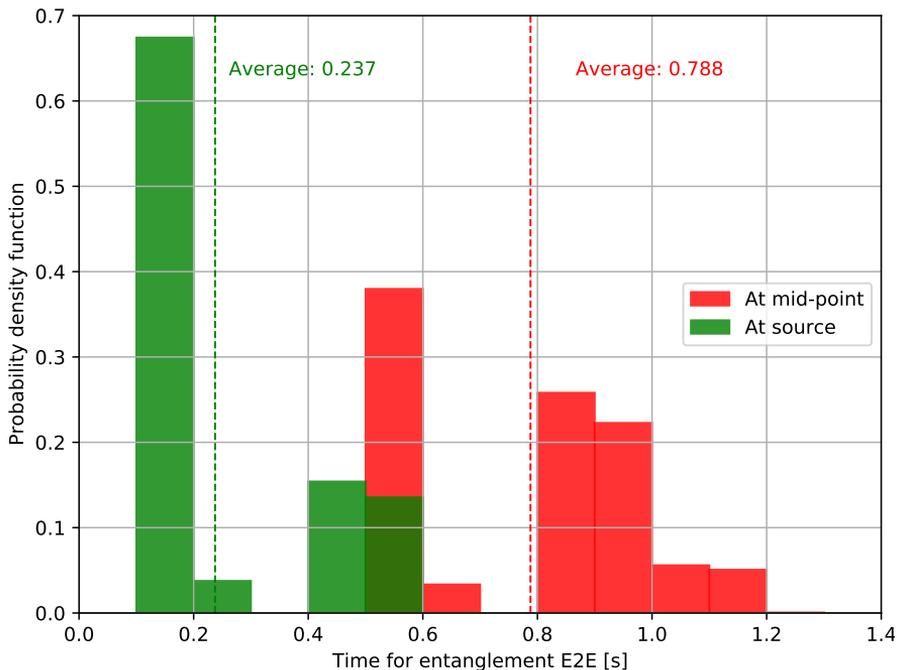


Figure 5.33: Time required to establish an entanglement E2E [23] ©2022 IEEE.

The number of packets exchanged also depends on the number of satellites that are part of the E2E path, which in the considered time interval varies between 4 and 6. In Fig. 5.35, we considered a realistic packet loss probability for infrastructure with a single Controller on the ground. Indeed, all the traffics from the Controller to the satellites and the respective acknowledgments use the link between the GSs and the directly connected satellite, which is the most critical link. In addition, traffic to and from the ground Controller also uses a fiber optic link. The packet flow between the GSs and the Controllers has been also considered in our architecture, but deploying the Controllers that manage the operations to be performed on the satellites of the selected path directly to the satellites mitigates the losses, which we considered negligible. The improvement in terms of latency required to establish an E2E entanglement compared to the case with a single Controller on the ground depends on that some entanglement generation and

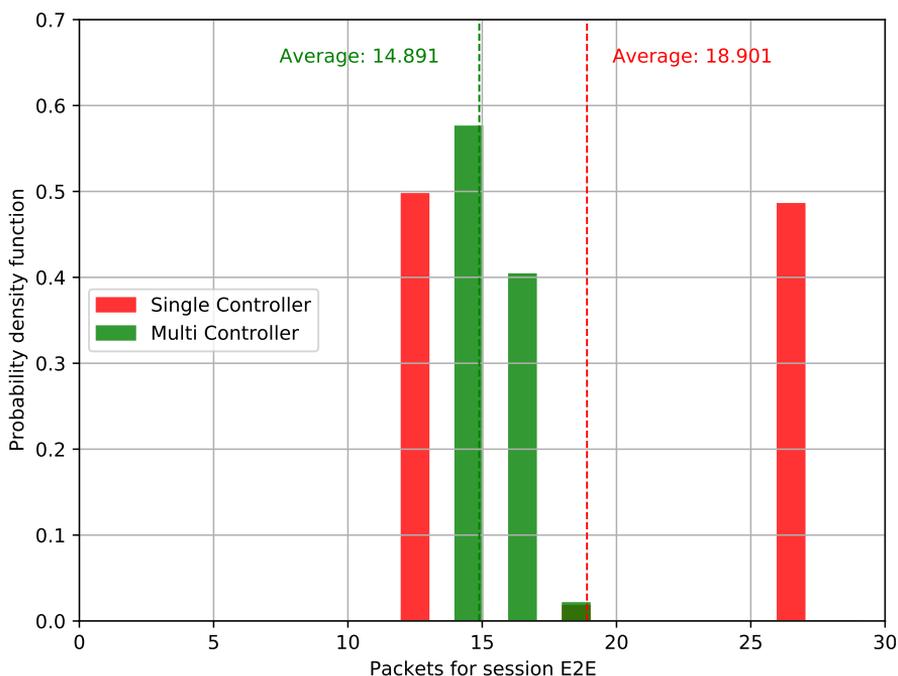


Figure 5.34: Packets exchanged during a single session using a single Controller on the ground and the multi Controller architecture [23] ©2022 IEEE.

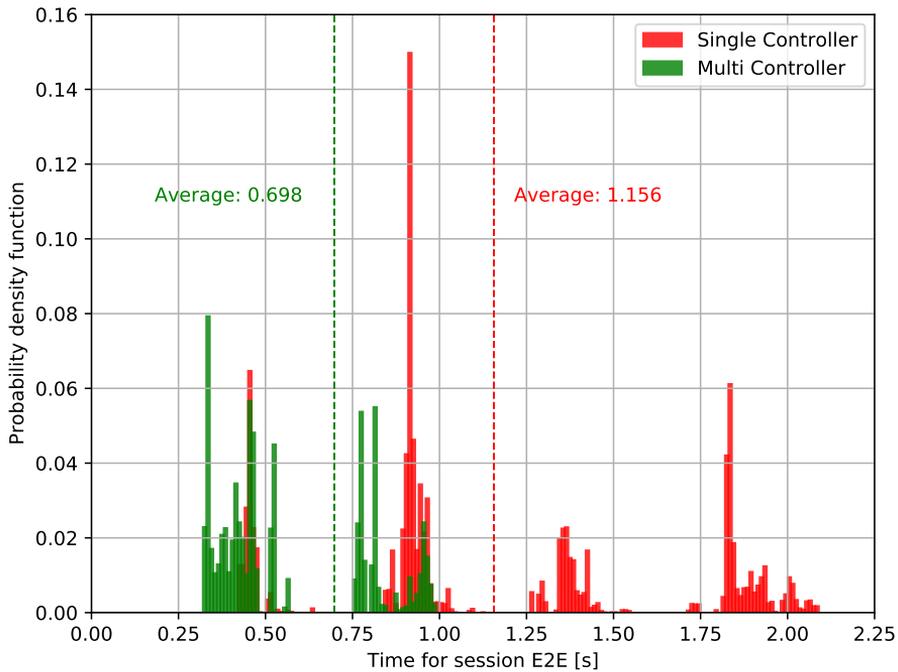


Figure 5.35: Time required to establish an entanglement E2E [23] ©2022 IEEE.

swapping operations can be performed on the device that has the Controller process embedded, while avoiding the sending of some messages, and, thus saving time.

Chapter 6

Drones Network Architecture and Performance Analysis

Drones are considered essential for the development of future QNs. Many experiments have already been conducted, as reported in Section 3.8, however, they involve just single drones. For this reason, a specific SDN-based architecture capable of managing multiple drones is defined in this Chapter. Specifically, this architecture integrates an SDN Controller into the swarm itself. The performance was evaluated in terms of the fidelity, the entanglement rate, and the overhead of the proposed protocol considering different meteorological conditions.

6.1 Motivations

The deployment of multiple drones, indeed, allows delivering cellular and Internet services to remote regions or areas, where a massive number of users are temporarily gathered or where terrestrial infrastructure is unavailable or difficult to deploy. Furthermore, drones can be *on-demand* disposed above the desired area in order to assist communications at any given time and according to their dynamic requirements [102]. In the 5G and 6G networks, one of the main objectives is the creation of a fully integrated heterogeneous network [122] [123] following the SOA paradigm [119]. Moreover, considering that a good level of miniaturization has been achieved regarding QDs it is logical to infer that swarms of drones can be equipped with these devices. As a matter of fact, in [24] is presented a 19-inch rack quantum computing

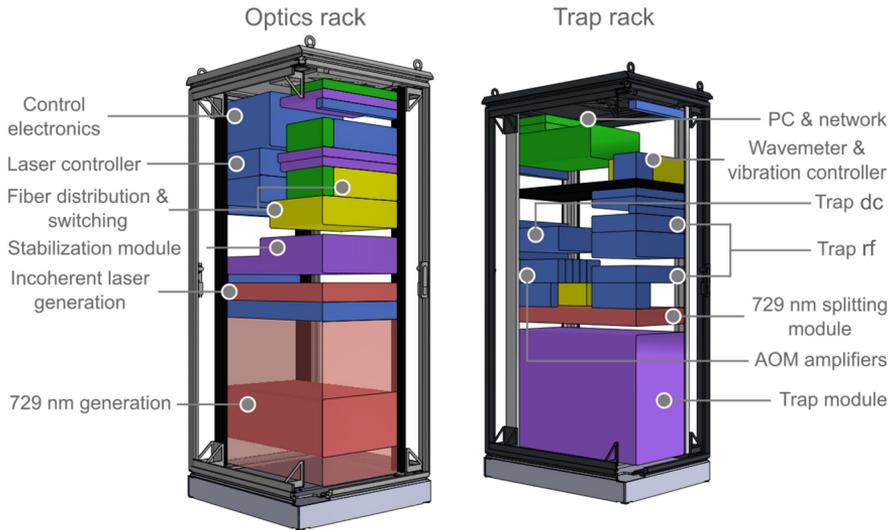


Figure 6.1: Scheme of the quantum computing demonstrator housed in two 19-inch racks [24]. By Pogorelov, I. *et al.* <https://journals.aps.org/prxquantum/abstract/10.1103/PRXQuantum.2.020343> is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>

demonstrator based on 40Ca^+ optical qubits in a linear Paul trap [416], which is depicted in Fig. 6.1. In addition, as reported in [417] [418] from the point of view of energy consumption, a fully quantum or hybrid network can also be very efficient. Therefore, the realization of a QN composed of drones is not expected to be problematic from the energy point of view.

The quality of the FSO link can be severely impacted by the change of drones' position and orientation due to their random fluctuations [104]. Specifically, pointing errors and atmospheric turbulence contribute to increased losses [105]. These effects are known as *beam wandering* and can significantly deteriorate the communications performance [106], which depends on the fraction of power that falls onto the photo-detector. Despite the circuitry onboard the drone could contribute to mitigating these effects [107], they cannot be completely neglected.

Given all the previous considerations, the swarm of drones can be taken into account to create efficient ad hoc MQDNs for critical missions. Further-

more, considering that the SDN is a suitable technology for the management of mobile QNs [20–23, 64], in this Chapter is examined an SDN oriented architecture that can be used to manage and control a MQDN and to adapt it to possible quantum applications. Specifically, in a MQDN, the SDN Controller can set up the E2E drones' path by sending control messages on a particular classical control channel [79]. Furthermore, with the SDN technology, it is possible to further mitigate pointing errors by compensating the trim changes due to atmospheric agents [110].

The architecture presented in this Chapter could be devoted to distributed quantum computing, which allows creating *Quantum Cloud* with an unprecedented computational capacity [11, 111, 112], and quantum cryptography, that makes quantum communication extremely secure [113]. However, many of the QKD protocols applied so far do not involve multiple drones as considered in this thesis, and only a few studies concern the implementation of entanglement-based protocols [115] [92]. The proposed architecture allows the creation of a network of drones acting as QRs, which can share Bell pairs on a L2L basis. Through teleportation and entanglement swapping operations between the drones, the objective is to create E2E-based entangled states which can be used both for distributed quantum computing and as the basis for entangled-based QKD protocols such as E91.

Moreover, the proposed architecture provides accurate mission planning and control also allowing to reduce the effects due to quantum *decoherence* [116] that remarkably affects both quantum communication and quantum computation. As a matter of fact, decoherence leads the qubits that compose the Bell pair to lose the entanglement as time passed [23]. Specifically, several parameters, e.g., temperature or magnetic fields, constitute an uncontrollable source of noise in the system, which influences the quality of the generated entangled state [79]. Nevertheless, as explained in [66], by positioning the QRs equidistant, it is possible to mitigate the effect of decoherence. Therefore, the drones that compose the swarm must be positioned as equidistant as possible. Through accurate layer positioning operations that can involve, e.g., the use of pseudospectral optimal control [419].

Despite the several efforts that have been dedicated to performing quantum communications through *couple* of drones, it is still unclear how the E2E paths between two GSs can be optimally configured. As a consequence, the aim of the thesis is to provide some guidelines to dispose and manage a QDN optimally, to create an efficient ad hoc MQDN for specific missions,



Figure 6.2: A quadcopter can be stationed for a relatively long time in a fixed position [25] [26]. In this manner, it is straightforward to interconnect and maintain them as equidistant as possible in an optimal position, facilitating quantum communication.

i.e., whenever a terrestrial connection is unavailable or difficult to set up or whether the performance achievable through OF is not sufficient. On the proposed architecture, the following metrics are analyzed: (i) the *fidelity* [79] [420], which indicates the quality of the generated entangled pairs, (ii) the *entanglement rate* [20] that is the number of generated entangled pairs per second, and (iii) the *overhead* of the proposed SDN-based protocol.

6.2 Simulation Environment

This Section describes the Python library used to perform the simulations described in Section 6.4. Moreover, the final part of the Section compares the chosen environment with other simulation environments highlighting the pros and cons.

6.2.1 NetSquid Simulator

The Network Simulator for Quantum Information using Discrete events (NetSquid) [421] is a software tool for the modelling and simulation of scalable QNs developed at QuTech. The goal of NetSquid is to enable scientists and engineers to design the future QI as well as modular quantum computing architectures. One of NetSquid's key features is its ability to easily and accurately model the effects of time on the performance of QNs and QCSs. This forms an essential ingredient in developing scalable systems which require a design that can mitigate the limited lifetime of quantum bits processed by QDs. Specifically, the main features of NetSquid are the following:

- It has a discrete event simulation engine to accurately track quantum decoherence across a network in time.
- A quantum computation library focused on localised qubit operations and optimized for repeated random sampling using memorization.
- Seamless support for representing quantum states as ket vector states, stabiliser states and DMs, providing trade-offs in performance, scalability and versatility.
- A library of modular and composable component base classes with which to physically model QNs hardware.
- An easy to use Python package that uses optimised C and Cython code under the hood.
- An intuitive asynchronous framework to program QNs protocols and the classical CP above it.

6.2.2 NetSquid Simulation Engine

To track the time evolution of qubit quantum states and account for communication and processing delays in a network a discrete event simulation engine is used. Specifically, the simulator schedules events at specific times on a timeline, and progresses time by chronologically stepping through these events, as depicted in Fig. 6.3. Simulation entities can listen for and react to these events, and optionally schedule future events in the process.

The simulation package `PyDynAA` defines a handful of classes that represent its key concepts. These classes are the entities of a simulation, events

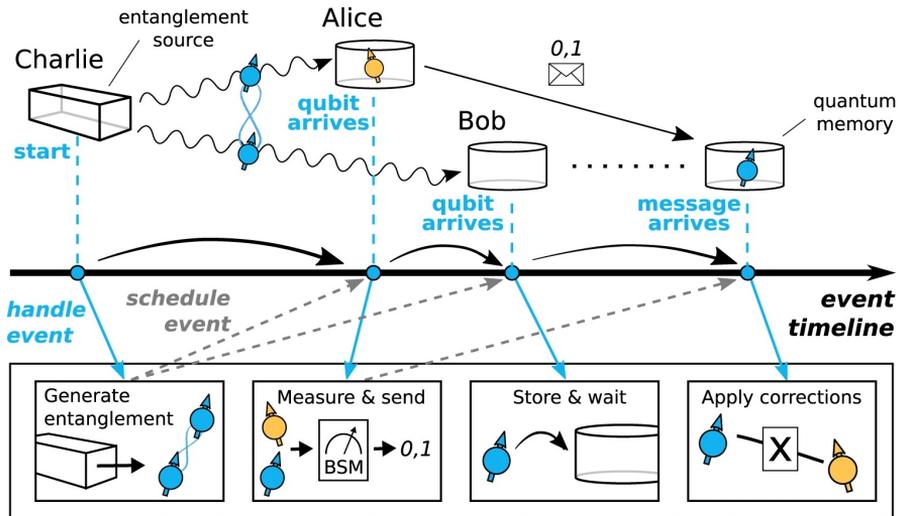


Figure 6.3: Timeline of the discrete event simulation engine of NetSquid. "Abstract example of simulating a quantum protocol with discrete events" by Tim Coopmans *et al.* <https://www.nature.com/articles/s42005-021-00647-8/figures/2> is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>.

of a specific type that occur at scheduled times during a simulation run, event expressions that can be used to describe logical event combinations, handlers objects that respond to triggered events, and the simulation engine that manages the event scheduling and handler registration. Simulation entities are anything in the simulation world that can generate or respond to events. The Entity base class, which should always be sub-classed, provides methods for scheduling events and waiting for them. Scheduled events will occur at given instances on the simulation timeline. The simulation engine runs by stepping sequentially from event to event in a discrete fashion. An entity can respond to events by registering an event handler object with a callback function to wait for events with specified or unspecified type, source, and id to be triggered.

The entire software architecture of NetSquid is represented in Fig. 6.4. The sub-packages that make up the NetSquid package are shown stacked in relation to each other and the PyDynAA package dependency. The main classes in each (sub-)package are highlighted, and their relationships in terms

of inheritance, composition and aggregation are shown. Fig. 6.4 also represents the key modules users interact with.

Specifically, QNs can be modeled and set up in NetSquid by linking the provided component base classes together. Components in NetSquid are simulation entities that model the hardware of the network physically. They can be composed of functional models that characterise their behaviour, IO ports for communication, and, in the case of composite components, other subcomponents. Specifically, the main components adopted in this thesis are quantum channels to transmit the qubit in both directions.

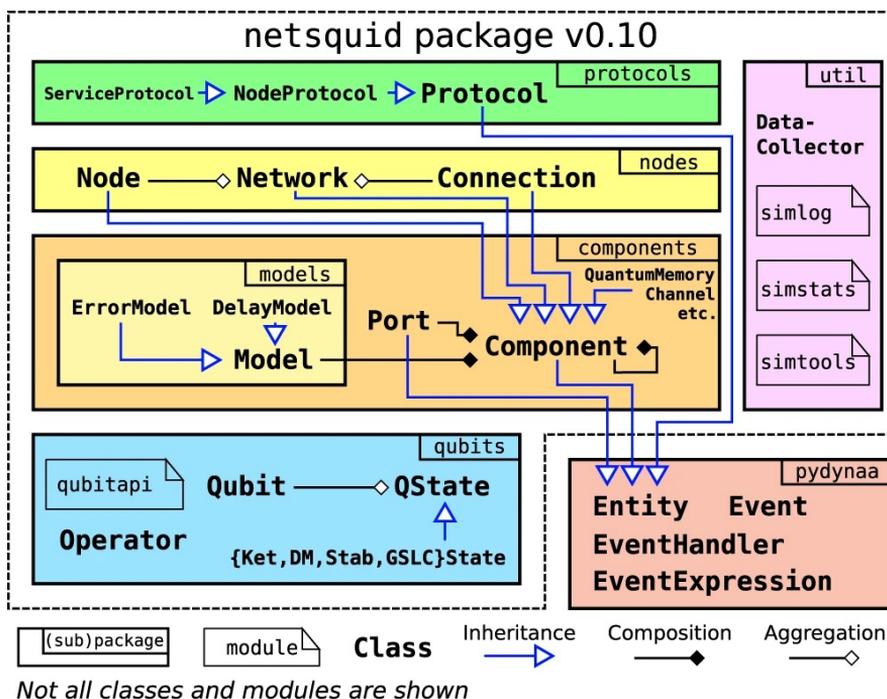


Figure 6.4: NetSquid’s software architecture. ”Overview of NetSquid’s software architecture” by Tim Coopmans *et al.* <https://www.nature.com/articles/s42005-021-00647-8/figures/10> is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>.

6.2.3 NetSquid Quantum Network Elements

An illustrative example of a NetSquid use case is reported in Fig. 6.5, where each sub-figure explains part of the modelling and simulation process. For the sake of clarity, the figures are not based on actual simulation data. The scenario shown is a QR utilising entanglement distillation. In (a), the setup of a QNs using node and connection components is represented. Sub-figure (b) represents a zoom-in related to the subcomponents of the entangling connection component. The quantum channels are characterised using fibre delay and loss models. The quantum source samples from an entangled bipartite state sampler when externally triggered by the classical channel. Sub-figure (c) is a zoom-in of the QM positions within a quantum processor illustrating their physical gate topology. The physical single-qubit instructions possible on each memory in this example are the Pauli (X, Y, Z), Hadamard (H), and X-rotation (RX) gates, and measurement. The blue-dashed arrows show the positions and control direction (where applicable) for which the two-qubit instructions controlled-X (CNOT) and swap are possible. Noise and error models for the memories and gates are also assigned. Sub-figure (d) is an il-

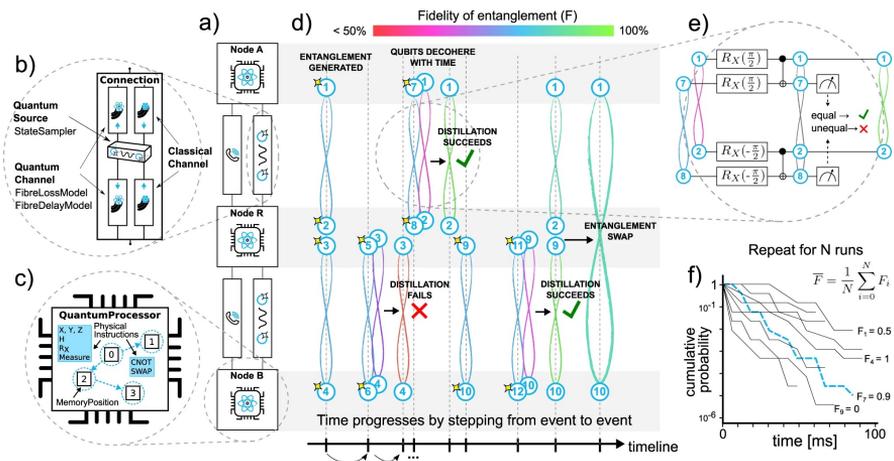


Figure 6.5: Modelling and simulation process adopted in NetSquid. "Illustrative example of a NetSquid use case" by Tim Coopmans *et al.* <https://www.nature.com/articles/s42005-021-00647-8/figures/1> is licensed under CC BY 4.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>.

lustration of a single simulation run. Time progresses by discretely stepping from event to event, with new events generated as the simulation proceeds. Qubits are represented by circles, which are numbered according to the order they were generated. A star shows the moment of generation. The curved lines between qubits denote their entanglement with the colour indicating fidelity. The state of each qubit is updated as it is accessed during the simulation, for instance to apply time-dependent noise from waiting in memory. Moreover, (e) is a zoom-in of the distillation protocol. The shared quantum states of the qubits are combined in an entangling step, which then shrinks as two of the qubits are measured. The output is randomly sampled, causing the simulation to choose one of two paths by announcing success or failure. Finally, (f) is a plot illustrating the stochastic paths followed by multiple independent simulation runs over time, labelled by their final E2E fidelity F_i . The blue dashed line corresponds to the run shown in (d). The runs are typically executed in parallel. Their results are statistically analysed to produce performance metrics such as the average outcome fidelity and run duration.

6.2.4 Other Simulation Environments

In addition to NetSquid, other simulators have been recently developed, however, they have not yet reached its level of development. First, SimulaQron [422] and Quantum Network Simulator (QuNetSim) [423] are two simulators that do not aim at realistic physical models of channels and devices, or timing control. Instead, SimulaQron's main purpose is application development. It is meant to be run in a distributed fashion on physically-distinct classical computers. QuNetSim focuses on simplifying the development and implementation of QNs protocols. In contrast with SimulaQron and QuNetSim, the Simulator for Quantum Networks and Channels (SQUANCH) [424] allows for QNs simulation with configurable error models at the physical layer. However, SQUANCH, similar to SimulaQron and QuNetSim, does not use a simulation engine that can accurately track time. Accurate tracking is crucial for e.g. studying time-dependent noise such as memory decoherence. Other than NetSquid, there now exist three discrete-event quantum simulators: the Quantum Internet Simulation Package (QuISP) [425] [426], qkdX [427] and Simulator of QUantum Network Communication (SeQUeNCe) [428] simulators. With these simulators it is possible to accurately characterise complex timing behaviour, however they

differ in goals and scope. Similarly to NetSquid, QuISP aims to support the investigation of large networks that consist of too many entangled qubits for full quantum-state tracking. In contrast to NetSquid, which achieves this by managing the size of the state space, and providing the stabiliser representation as one of its quantum state formalisms, QuISP's approach is to track an error model of the qubits in a network instead of their quantum state. qkdX, on the other hand, captures the physics more closely through models of the QDs but is restricted to the simulation of QKD protocols. Lastly, SeQUeNCe, similar to NetSquid, aims at simulation at the level of hardware, CP or application. It has a fixed control layer consisting of reprogrammable modules. In contrast, NetSquid's modularity is not tied to a particular network stack design. Furthermore, it is unclear how performant SeQUeNCe's quantum simulation engine is: currently, at most a 9-node network has been simulated, whereas NetSquid's flexibility to choose a quantum state representation enables scalability to simulation of networks of up to 1000 nodes.

6.3 System Model

This Section describes the proposed system model and the architectural criteria proposed to perform quantum communications and processing. Specifically, the considered scenario consists of two GSs interconnected through a swarm of drones equipped with quantum hardware. In order to organize the mission properly, the correct number of drones needs to be selected and dynamically controlled during the mission.

One of the phenomena to be taken in consideration is decoherence, which concerns the interaction between qubits and the surrounding environment. To prevent that a qubit becomes entangled with the environment, the system must be kept as possible isolated, otherwise, the processing and the communication process can result altered [23]. In the considered scenarios, we arranged the drones in an equidistant configuration, as shown in Fig. 6.11. The choice is due to the fact that, with this configuration, it is possible to minimize the coherence time required to successfully achieve entanglement [66], mitigating the negative effects due to decoherence not requiring higher-performance technologies with additional costs.

In order to obtain an E2E-based entanglement over a long distance, the involved QDs operate as QRs [103]. The quantum operations that a QR performs are *quantum teleportation* and *entanglement swapping*, which are

explained in the following.

In quantum teleportation, the state of a qubit is destroyed in one location and recreated in another [79]. The process of entanglement swapping uses teleportation *consuming* two Bell pairs covering adjacent short distances into one pair, which covers the corresponding longer distance [292]. The entanglement swapping procedure is depicted in Fig. 6.6 and works as follows: after preparing two independent entangled pairs α - β and δ - γ , a Bell state measurement on β and δ projects α and γ onto an entangled state, even though these two particles have never shared any common past [21]. Therefore, the entanglement swapping procedure can also be defined as an extension of teleportation [257].

To reduce the impact of channel losses, several QRs have to be deployed along the E2E path [20] [429] [430] and the performance can be further improved with the use of FSO technology. However, despite the previously described phenomena limiting the performance of FSO significantly, as reported in [22] adequate performance can be achieved in clear air conditions using the 1550 *nm* wavelength. In order to model the atmospheric links, several models [90] [91] allow calculating the specific optical attenuation considering a wavelength-dependent relation that regards the *atmospheric visibility* and the *drop size distribution*. As a matter of fact, some models show that in favorable meteorological conditions, reduced attenuation values can be obtained, even lower than those obtainable with OFs [91] [90]. This

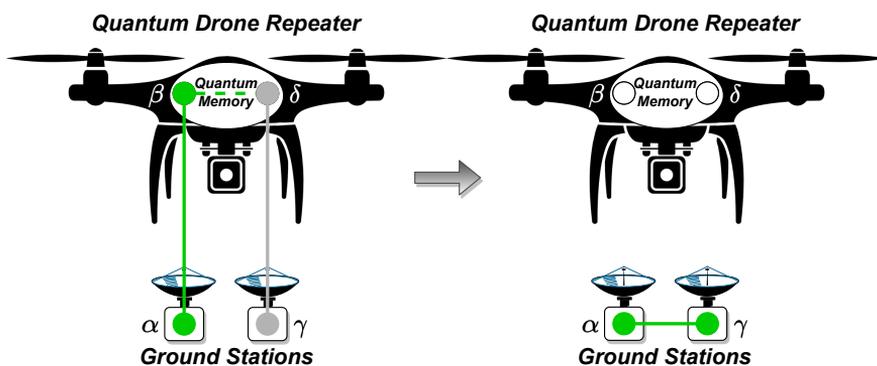


Figure 6.6: Operating principle of a drone acting as QR. Entanglement swapping is performed between two pairs of particles executing a Bell state measurement on two of them [27] ©2022 IEEE.

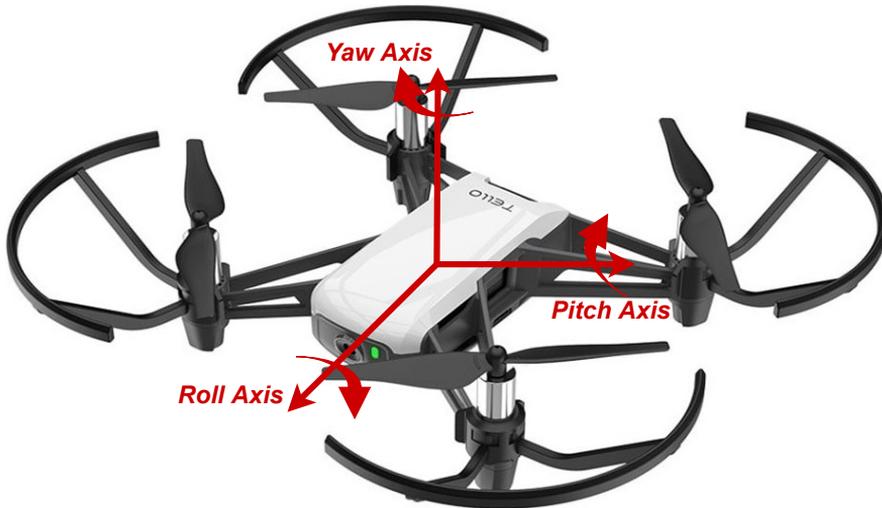


Figure 6.7: Oscillations that typically affect a flying object. "DJI Tello Micro-Drone" by Dennis Sylvester Hurd <https://www.flickr.com/photos/dennisylvesterhurd/49238096152> is licensed under CC BY 2.0. To view a copy of this license, visit <https://creativecommons.org/licenses/by/2.0>. The picture has been modified within the terms of the license by inserting the coordinate system [27] ©2022 IEEE.

results in a significant reduction of losses due to the scattering phenomenon and allows to reduce the number of required QRs.

Nevertheless, as explained in [106] the quality of the FSO link can be degraded due to the random fluctuations of the drones w.r.t their position and orientation. As a matter of fact, aerial objects, including drones, are subject to phenomena such as pitch, roll, and yaw, which are variations in position with respect to all three axes, as shown in Fig. 6.7. Specifically, the axes and the related motions are described as follows:

- Yaw axis: is defined to be perpendicular to the plane of the wings with its origin at the center of gravity. Motion about this axis is called yaw.
- Pitch axis: an axis parallel to the wings of a winged aircraft. Motion about this axis is called pitch.
- Roll axis: an axis drawn through the body of the aircraft, with its origin at the center of gravity and parallel to the normal direction of

flight. Motion about this axis is called roll [431] [432].

On a drone, these variations can be measured by an *Inertial Measurement Unit (IMU)* on board the drone [432–435] and mitigated by the *Flight Controller*, which provides the following features:

- Kinesthetics of drone flight.
- Automatic thrust/angle control.
- Maintains position and orientation [107].

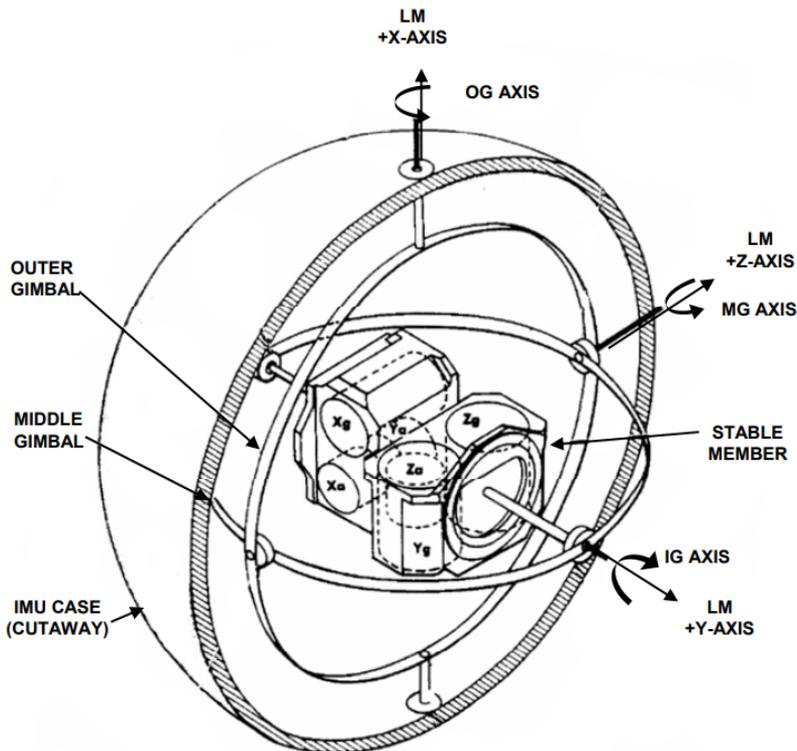


Figure 6.8: Representation of an IMU. "Apollo Guidance, Navigation, and Control (GNC) Hardware Overview" by NASA <https://ntrs.nasa.gov/api/citations/20090016290/downloads/20090016290.pdf>.

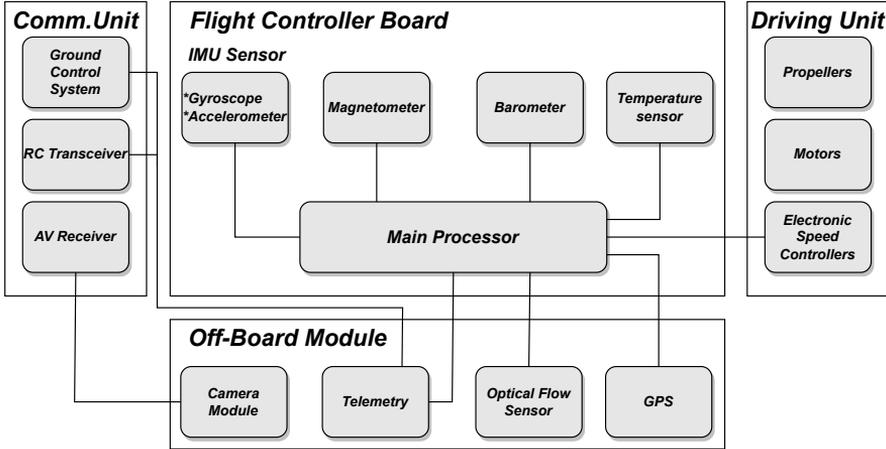


Figure 6.9: Scheme of the modules that compose a typical drone [28].

However, despite the flight Controller onboard the drone could contribute to mitigating these effects [107], the consequences introduced by this phenomenon cannot be completely neglected. Specifically, these losses depend on whether the optical receiver can capture only the fraction of power that falls onto the photo-detector. Furthermore, pointing errors contribute to increased losses. These effects are known as *beam wandering*. Considering that the beam may experience random displacements both along with the horizontal and vertical axis, the misalignment errors of the photo-detector are modeled as independent Gaussian random variables, where μ_x and μ_y denote the

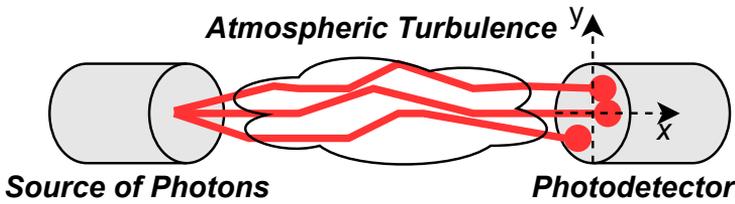


Figure 6.10: Representation of beam wandering due to atmospheric turbulence [27] ©2022 IEEE.

averages and σ_x^2 and σ_y^2 the variances, expressed as follows [105] [106] [436]:

$$x \sim \mathcal{N}(\mu_x, \sigma_x^2) \quad (6.1)$$

$$y \sim \mathcal{N}(\mu_y, \sigma_y^2) \quad (6.2)$$

Moreover, as the number of drones increases, the error becomes progressively more significant, whereas every drone is affected by such phenomena [437].

In the proposed architecture, depicted in Fig. 6.11, the mission is loaded by a classical server that optimizes and schedules the mission according to the user's request. Specifically, drones must be programmed by providing them the GPS coordinates calculated according to the optimization procedure, and the SDN Controller is installed on the drone that is supposed to occupy the central position. Therefore, the mission can start, and the drones position themselves at the specified coordinates. During the second phase, the SDN Controller, which is installed in the drone that is located in a central position, starts managing the operations of entanglement generation and swapping to enhance the process. Furthermore, the Flight Controller mitigates pointing errors compensating the trim changes due to atmospheric agents relying on the position control given by the on-board GPS receiver and IMU [434]. In case one or more drones deviate excessively from their position or in case of failure, the SDN Controller could reorganize the traffic on the path by reprogramming the devices that compose it via Southbound messages, in order to operate without the missing drones. According to the design specifications of QNs stated in [79], the Controller messages are sent over a dedicated classical control channel. The SDN-based protocol shown in Fig. 6.12 is structured in two phases described as follows.

1. The SDN Controller sends entanglement generation messages to the drones that compose the left and right sub-sets of the swarm to interconnect GSs and drones, including itself, on a L2L basis.
2. The SDN Controller sends messages to the drones to perform the entanglement swapping in order to create the E2E entanglement.

Naturally, considering that the SDN Controller is on board one of the drones,

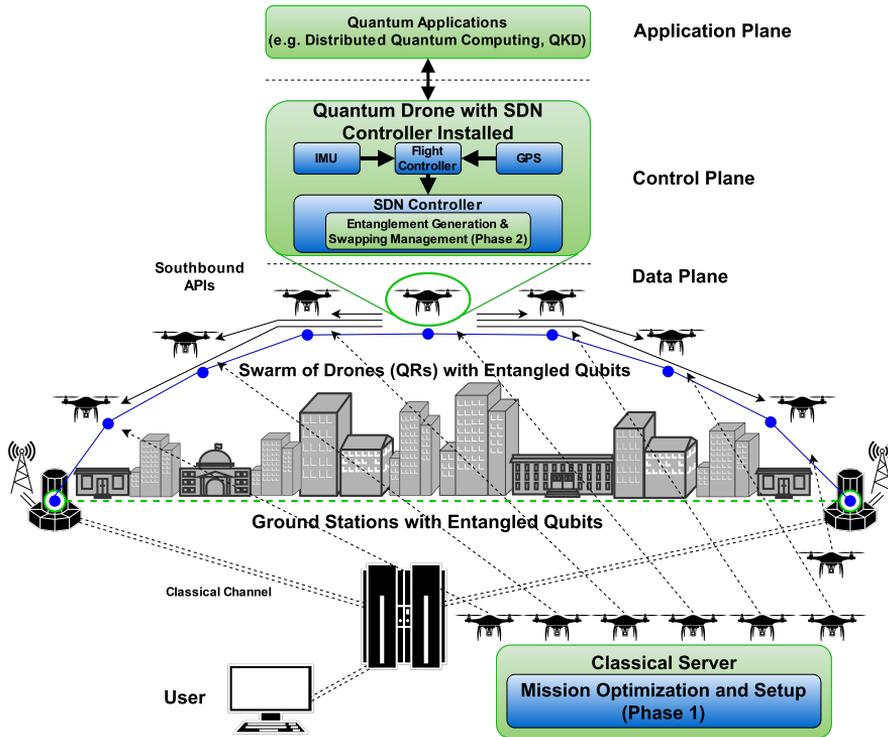


Figure 6.11: Quantum metropolitan SDN drone network. In the first phase, the mission is configured properly by calculating the coordinates of the drones according to the result of the optimization. During the second phase, the Bell pairs are generated between the GSs through operations driven by the Controller embedded in the swarm of drones [27] ©2022 IEEE.

in order to perform the swapping operation on itself, no message has to be sent, thereby limiting overhead and packet losses.

The proposed architecture can be used for distributed quantum computing and for entanglement-based QKD applications. As explained in [243] [79], the entangled particles can be prepared by both the users sharing the key or by a third entity, and are distributed in a way that both the users have one photon of each pair. As depicted in Fig. 6.11, the SDN Controller positioned in the barycenter of the created E2E path is the entity that manages the E2E entanglement generation between the GSs properly, managing the L2L entanglement generation and swapping operations performed by the other

QDs, according to the protocol explained in Fig. 6.12. Therefore, the Controller allows the creation of remote entangled states between two QCs if required by a distributed quantum algorithm [23] operating in a Quantum Cloud context or provides to create the Bell pairs that compose the key in the case of communications performed using QKD entanglement-based protocols [243].

Furthermore, as explained in [317], an architecture that uses multiple QRs can be considered secure. As a matter of fact, the advantage of QRs is that the final key between the GSs is independent of the knowledge of the repeaters and even if a repeater is controlled by an adversary, it cannot infer the final secret key.

Since drones operate in the lowest layers of the atmosphere, scattering of optical wavelengths by aerosol particulates and fog have a significant impact on communication, and it is necessary to adopt specific models [438]. Moreover, considering that, as explained in [439], the effect of turbulence on quantum states is similar to the effect on classical vector modes, we have considered the Kruse model [440], which provides a wavelength-dependent relation between the *atmospheric visibility* V and the *extinction coefficient* ξ . In particular, it allows to calculate the specific optical attenuation as follows [440] [91]:

$$A = 10(\log_{10} e)\xi \quad (6.3)$$

where ξ is defined as:

$$\xi \doteq \frac{-\ln 0.02}{V} \left(\frac{\lambda}{550} \right)^{-\eta} \quad (6.4)$$

The term V present in (6.4) is the atmospheric visibility, defined as a distance where a 550 nm collimated light beam is attenuated to a fraction of 5% or 2% of original power. The η coefficient depends on experimental data about the drop size distribution [441] and is related to visibility:

$$\eta = \begin{cases} 0.585V^{\frac{1}{3}} & \text{if } V < 6 \text{ km} \\ 1.3 & \text{if } 6 \text{ km} < V < 50 \text{ km} \\ 1.6 & \text{if } V > 50 \text{ km} \end{cases} \quad (6.5)$$

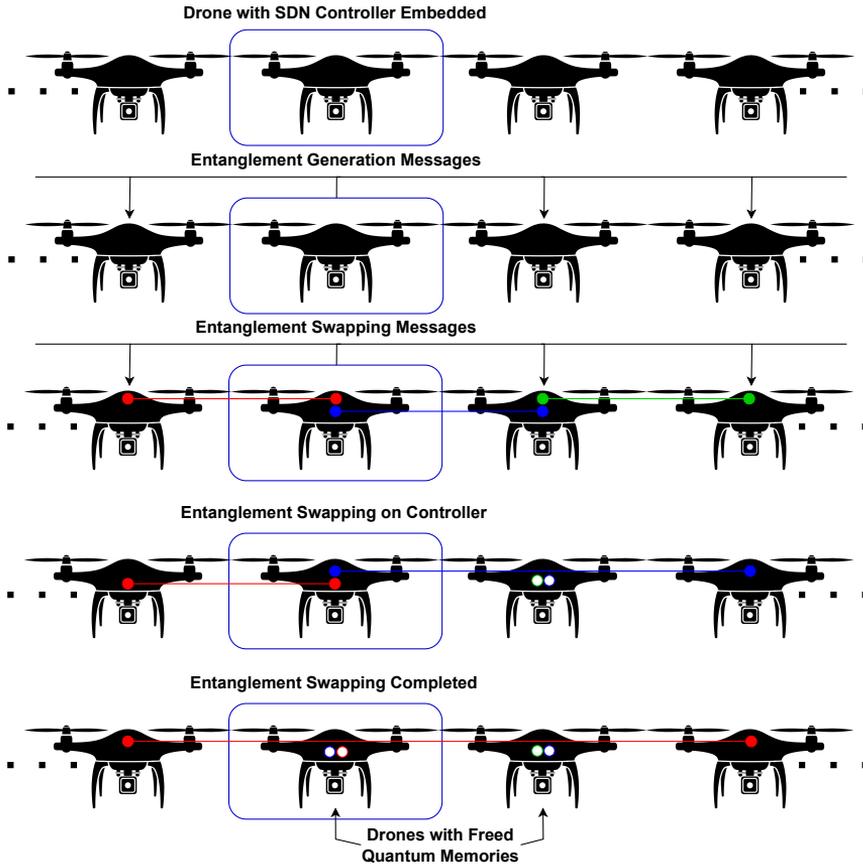


Figure 6.12: Entanglement generation and swapping protocol performed by the SDN Controller. Note that the swapping operation on the drone with the Controller embedded does not require the transmission of messages [27] ©2022 IEEE.

To address the quality of the supported applications, several parameters can be considered, among which the fidelity that is a parameter that characterizes the quality of teleportation. Specifically, the fidelity between a pure state $|\psi\rangle$ and an arbitrary state ρ , is defined as follows [38] [442] [443]:

$$F(|\psi\rangle, \rho) \doteq \text{Tr} \sqrt{\langle \psi | \rho | \psi \rangle |\psi\rangle \langle \psi|} = \sqrt{\langle \psi | \rho | \psi \rangle} \quad (6.6)$$

The fidelity is a number between 0 and 1, which is equal to 0 if and only if $|\psi\rangle$ and ρ have orthogonal support, and it is equal to 1 if and only if $|\psi\rangle = \rho$ [38]. Therefore, the fidelity is a probability that describes how *close* two quantum states are, and the closer it is to 1, the more the created state is similar to the desired one. It can be used to characterize drastic changes in quantum states in the presence of QPTs. If the fidelity value is below 0.5, the created state is unreliable, and it cannot be used for computing purposes [79]. However, the fidelity of a quantum state can be enhanced by the proper use of QRs [77] [70].

Moreover, we evaluated the entanglement rate R , which is defined as the number of created entangled states per second and is measured as Bell pairs per seconds [20] [147]. In QNs the entanglement rate is also defined as throughput, or the speed of variation of the relative entropy of entanglement [148] [386]. The entanglement is generated between the two GSs upon completion of entanglement swapping operations [21] driven by the Controller and performed by the drones involved in the E2E path.

Considering that the SDN Controller is centrally placed, the times required for the completion of operations on the left and right sides of the E2E path are respectively τ_l and τ_r . Furthermore, the time required to generate a L2L entanglement between drone i and drone $i + 1$ can be defined as $\tau_{e_{i,i+1}}$ and the time required to perform the entanglement swapping operation on a specific drone j as τ_{s_j} . However, despite the swapping operations related to the drone on which the Controller is installed do not require messages to be sent, it is necessary to consider the time required for the state measurement to perform the swapping operation, which is then given as τ_{s_0} . For instance, if we consider the path as consisting of an odd number of drones equal to N the left and right sections consist of a number of drones equal to $\frac{N-1}{2}$, the times required to complete the operations on the left and right sides are:

$$\tau_l = \sum_{i=-\left(\frac{N+1}{2}\right)}^{-1} \tau_{e_{i,i+1}} + \sum_{j=-\left(\frac{N-1}{2}\right)}^{-1} \tau_{s_j} \quad (6.7)$$

$$\tau_r = \sum_{i=0}^{\frac{N-1}{2}} \tau_{e_{i,i+1}} + \sum_{j=1}^{\frac{N-1}{2}} \tau_{s_j} \quad (6.8)$$

Considering that the time required to complete operations on the entire path

is determined by the longer time interval, the time required to obtain an E2E entanglement is equal to:

$$T = \max\{\tau_l, \tau_r\} + \tau s_0 \quad (6.9)$$

Therefore, the entanglement rate on the entire path can be effectively expressed as:

$$R \doteq \frac{1}{T} \quad (6.10)$$

where T is the time required to generate a remote entanglement over the entire E2E path [66] [21] [20] [27].

In order to maximize the overall quantum processing capability, we introduce an objective function combining the two considered metrics. Since [79], quantum applications require that the fidelity is above some application-specific threshold F^* , the objective function can be consequently expressed as follows:

$$\begin{aligned} \max_N \quad & R(V, d, \lambda, N) \\ \text{s.t.} \quad & F > F^* \end{aligned} \quad (6.11)$$

The objective function expressed in (6.11) depends on the atmospheric visibility V , the distance d between the GSs, the wavelength λ and the number of drones N . Specifically, the solution of this optimization problem yields the optimum number of QRs that provide the best performance in terms of R , while guaranteeing $F > F^*$. This optimization is calculated by mission control during Phase 1, which is shown in Fig. 6.11.

Finally, we evaluated the overhead. As explained in [23], the overhead due to entanglement generation and swapping operations has to be minimized, especially for distributed quantum computing applications where the distributed quantum compiler must optimize the circuit so that the number of remote operations is minimized to limit the decoherence effects and to reduce the overhead arising with the swapping operations. In fact, when decoherence occurs, some qubits become entangled with the environment, and the entire computation of a single QC or a distributed computation performed by multiple QCs interconnected through QRs in a QN results corrupted [414] [116]. Specifically, the overhead minimization can be achieved by the efficient management of entanglement generation and swapping operations by the Controller. Furthermore, the integration of the CP into the drone swarm contributes to limiting overhead considering that some op-

erations can be performed locally and do not require sending messages as clarified in Fig. 6.12.

6.4 Simulations Results

Considering that different wavelengths are typically used in communications using FSO technology [444], we evaluated the attenuation for several wavelengths by varying the meteorological conditions and using the Kruse model defined in (6.3). Moreover, we characterized the phenomenon of beam wandering by modeling the pointing error on the photo-detector as two independent Gaussian random variables. Specifically, with an aperture of radius 10 cm, as in [106], we assumed a pointing error with a standard deviation of $\sigma = 7.5$ cm with respect to both the x-axis and y-axis of the photodetector shown in Fig. 6.10. We supposed a significant value for the standard deviation considering that, although the effects of the beam wandering can be mitigated, it can be complicated for drones to accurately maintain the position and therefore the impact of degradation cannot be neglected. Some of the parameter values used in the following simulations are given in Table 6.1.

As it can be seen from Fig. 6.13, in specific visibility conditions, the attenuation values are lower than those ones of the OFs, which have been considered only for comparison purposes. As a matter of fact, at 1550 nm, the OFs present an attenuation of 0.2 dB/km [445] depicted as a dotted line in Fig. 6.13. Specifically, under the same visibility conditions, the use of this wavelength ensures the lowest attenuation w.r.t the other ones considered. Furthermore, Fig. 6.13 shows that if we consider as reference values the attenuation of 0.2 dB/km of OFs, for the FSO case, this attenuation can be obtained at $\lambda = 1550$ nm with $V = 22.1$ km, i.e., in sub-optimal meteorolog-

Parameter	Value
Aperture Radius	10 cm
σ	7.5 cm
FSO Wavelengths	650, 850 and 1550 nm
OF Attenuation	0.2 dB/km

Table 6.1: Values of the parameters adopted in the simulations [27] ©2022 IEEE.

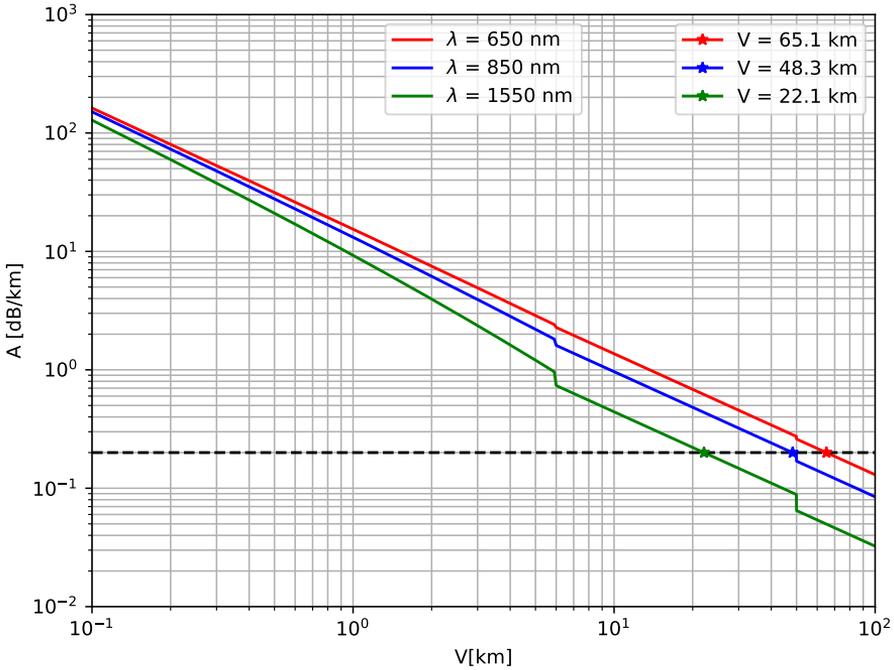


Figure 6.13: Attenuation for different wavelengths at varying meteorological conditions considering the Kruse model [27] ©2022 IEEE.

ical conditions. Therefore, it is appropriate to endow the network of drones with 1550 *nm* communications technology. These considerations are confirmed from the simulation performed on a scenario that considers a swarm of drones used to connect two GSs located at a distance of 10 *km* typical of a metropolitan area. Table 6.2 shows the values used in the simulations reported in Fig. 6.14, in which the achievable fidelity w.r.t. the number of

λ [nm]	Atmospheric visibility [km]	Attenuation [dB/km]
650	30	0.456
850	30	0.322
1550	30	0.147

Table 6.2: Attenuation values for the wavelengths employed in the simulations reported in Fig. 6.14 [27] ©2022 IEEE.

involved drones for different wavelengths and considering atmospheric visibility of 30 km in free space has been evaluated and compared with OFs. In Fig. 6.14 the maximum values of the obtained plots are also reported.

In particular, it can be inferred that under specific meteorological conditions it is possible to achieve performance comparable to OFs with a reduced number of QRs.

Furthermore, we have performed a simulation by varying the visibility conditions to verify the maximum fidelity values obtainable on the same scenario. Table 6.3 shows the parameters used in the simulations reported in Fig. 6.15, which also shows the achieved maximum fidelity values. From this evidence, it emerges that in specific meteorological conditions, it is possible to obtain very high fidelity values, even with a limited number of drones.

In addition, we investigate the fidelity varying the distance between GSs as a function of the number of drones considering visibility of 50 km . The

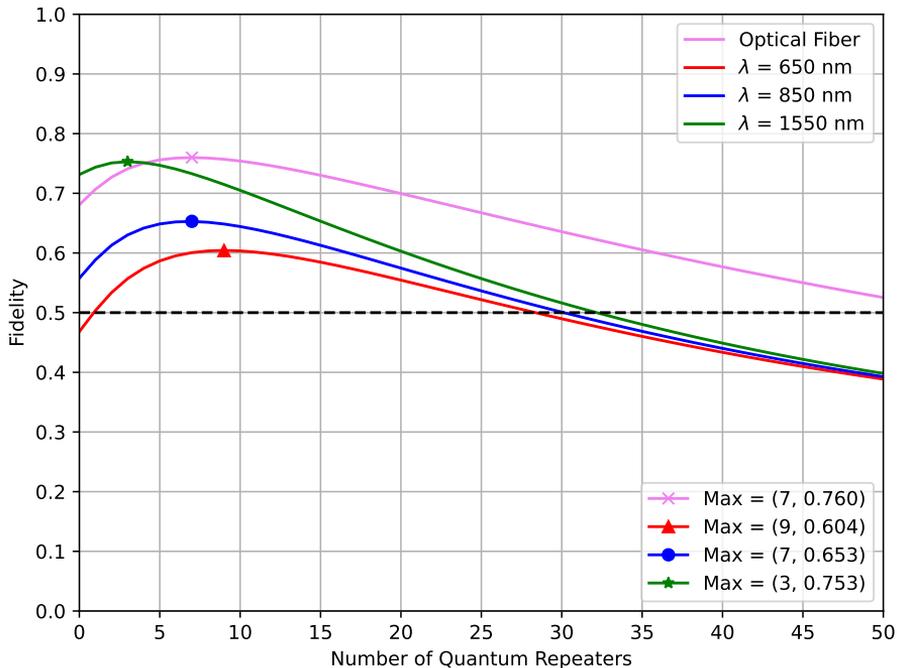


Figure 6.14: Fidelity for different wavelengths considering a visibility of 30 km [27] ©2022 IEEE.

λ [nm]	Atmospheric visibility [km]	Attenuation [dB/km]
1550	5	1.205
1550	10	0.442
1550	25	0.177
1550	50	0.065
1550	75	0.043
1550	100	0.032

Table 6.3: Parameters concerning the attenuation w.r.t. different atmospheric conditions considered in the simulations reported in Fig. 6.15 [27] ©2022 IEEE.

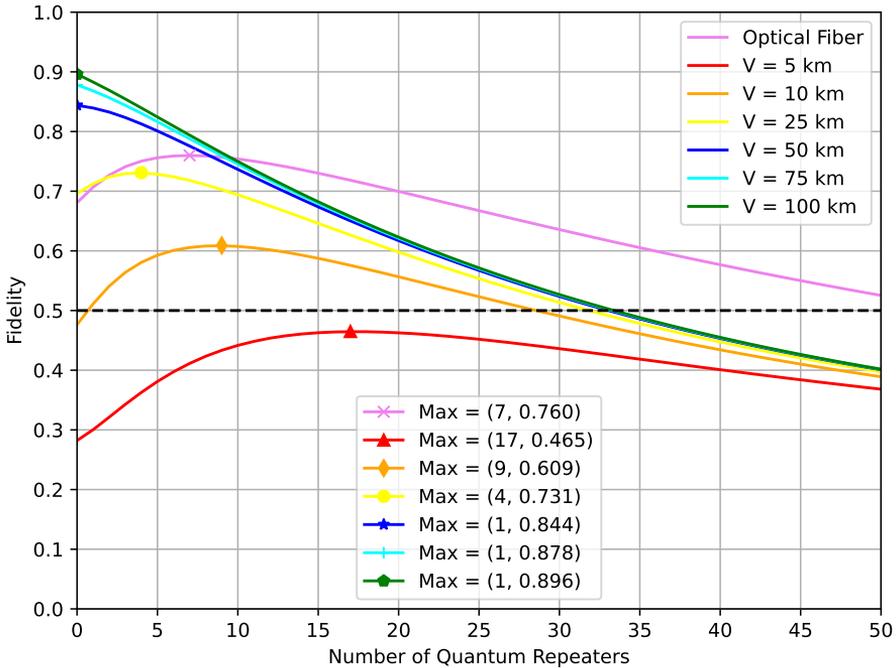


Figure 6.15: Fidelity at varying meteorological conditions at 1550 nm w.r.t. OFs [27] ©2022 IEEE.

results are shown in Fig. 6.16, which points out that increasing the distance between the GSs, makes the fidelity value decreases significantly. Specifically, with a distance between the GSs above 40 km, the maximum fidelity value is

below $F^* = 0.5$ for the considered meteorological conditions. It is clear from Figs 6.14, 6.15 and 6.16 that there is an achievable maximum; this allows obtaining significant information for the organization of the flight mission and the optimization of the E2E path.

Furthermore, we jointly evaluated the entanglement rate and the objective function in (6.11) varying the number of drones on a 10 km path. The results shown in Fig. 6.17, point out that the number of drones employed has a significant impact on the maximum achievable entanglement rate, which rapidly decays as the number of drones increases. Moreover, in Fig. 6.17 the curve in red denotes the values of entanglement rate achievable considering the objective function defined in (6.11), which limits the range of possible drones to a closed interval. As it can be noticed, the optimum value is close to the lower boundary of the eligible range corresponding to the minimum fidelity threshold at 0.5, considering a visibility of 10 km.

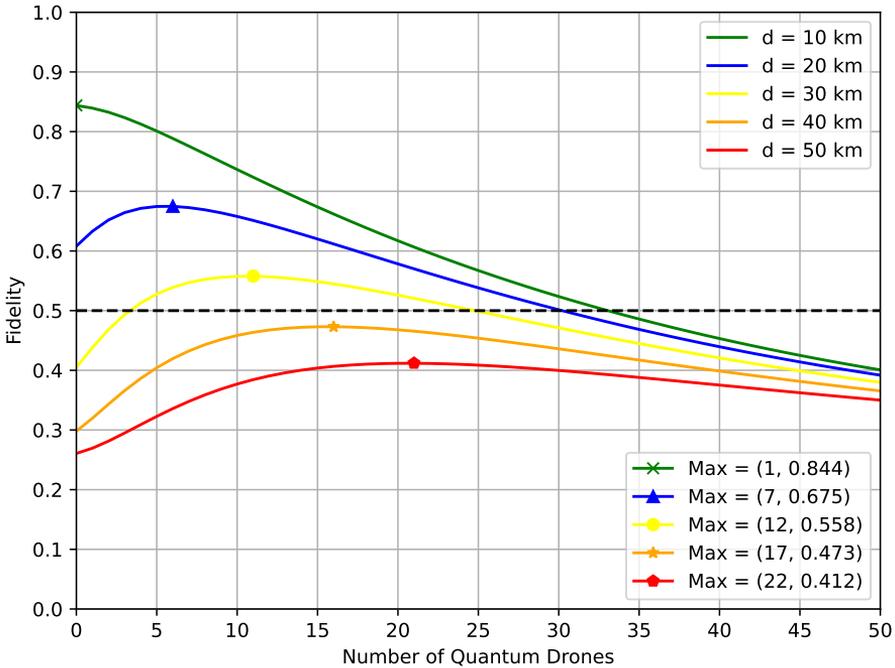


Figure 6.16: Fidelity at varying the distance between the GSs at 1550 nm considering visibility of 50 km [27] ©2022 IEEE.

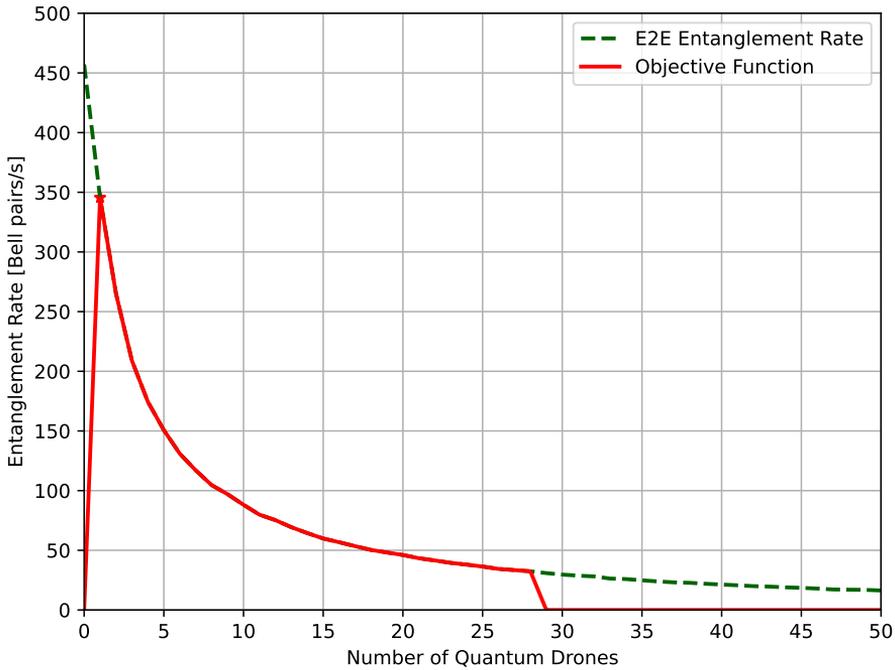


Figure 6.17: Entanglement rate at varying the number of QDs on a 10 km path. The red plot highlights the rate obtainable with fidelity greater than 0.5 with a visibility of 10 km [27] ©2022 IEEE.

Finally, we evaluated the overhead of the proposed control protocol, which performance is depicted in Fig. 6.18. Considering the problems related to the maintenance of drones' positions and that the aerial link can be significantly perturbed, we have introduced a realistic packet loss probability, which is proportional to the number of involved drones. Specifically, as the number of drones increases, the number of packets needed for operations increases, also considering a specific loss factor. The results are reported in Fig. 6.18, in which it can be seen that the loss factor has more influence with a significant number of drones.

The evidence emerging from these simulations show that the number of drones necessary to perform a quantum communication between two GSs depends both on the employed technology and meteorological conditions. Furthermore, we verified that the objective function has a unique maximum. Moreover, these simulations show that the problems of beam wandering due

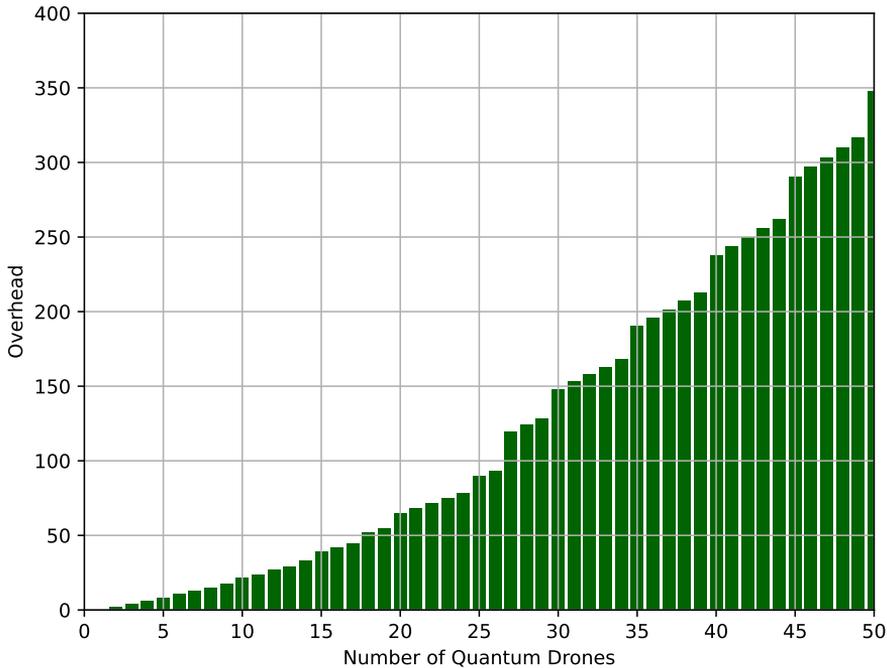


Figure 6.18: Overhead concerning the operations of entanglement generation and entanglement swapping for a single session [27] ©2022 IEEE.

to drones' random fluctuations and atmospheric turbulence [446] significantly degrades performance. As explained in [437], this issue is typical of communications among a large number of drones. In the quantum case, despite the use of multiple drones operating as QRs limits the performance degradation compared to a single link of equal length [429] [430], the effects of beam wandering become increasingly significant as the number of drones increases. Therefore, employing a limited number of drones contributes to maintaining adequate performance for all the evaluated parameters. The aim is achieved considering specific objective functions aimed to balance the evaluated parameters in order to plan the mission properly and limit costs. Furthermore, through the SDN technology, it is possible to coordinate the operations of entanglement generation and swapping between the drones that compose the swarm. Finally, the integration of the CP into the swarm allows performing some of the operations locally, contributing to improving performance and limiting overhead and possible packet losses.

Chapter 7

Conclusions and Future Works

Quantum Mechanics has had a significant development during the early years of the last century, moving from Quantum Theory to Quantum Mechanics with the contributions of many prominent scientists. However, despite the fact that possible applications had already been identified, it took many years before real devices were made. Nevertheless, in the last 40 years, it has exceptionally expanded into the area of information science and technologies, and extremely innovative applications, such as the quantum computing, quantum coding, quantum cryptography, and quantum communications have become a reality. Therefore, considering the progress that has been made recently in making QDs, it is necessary to create specific networks based on quantum physical principles in order to interconnect quantum on Earth servers reaching an unprecedented computational capacity. Several experiments have been conducted in order to create QNs using OFs, however, the performance achieved is not significant and many QRs are required. QSNs can overcome the limitations of terrestrial optical networks and the recent technological developments in terms of quantum satellite communications motivated the investigation conducted in this thesis, with the aim to create an efficient quantum satellite backbone.

First of all, this thesis proposes a near optimum E2E path evaluation procedure allowing an efficient switching in order to maximize the entanglement generation rate. Specifically, in this thesis are compared two distributed approaches MRW and ACO and one centralized using Dijkstra's algorithm in order to achieve a trade-off between performance and cost. We can note that the centralized strategy in addition to solving the problem of the prop-

agation of Bell pairs, it allows reaching higher entanglement rate values by involving an acceptable number of intermediate nodes. Furthermore, the average entanglement rate value of the centralized approach relying on Dijkstra's algorithm is higher than the other ones. This is because Dijkstra's algorithm is able to select E2E links whose maximum inter-satellite distance is less than other algorithms. Furthermore, one of the main objectives of this thesis is to propose several guidelines for the design of a global QI by extending existing systems toward a quantum perspective, considering also the benefits that SDN technology can provide. In fact, the SDN technology is considered significant for the development of QNs and has already been considered in many studies related to new-generation satellite networks.

Moreover, to design the network properly, the type of constellation should also be evaluated, in order to achieve adequate performance and limit costs. Therefore, this thesis evaluates the performance of different constellations based on the GPS, Iridium-NEXT constellations together with a fictitious one made up of Cubesats launched by various agencies. The performance has been compared in terms of the E2E entanglement rate by varying the distance between ground stations on an intercontinental scale. The evaluation conducted pointed out that a dense low-orbit constellation is able to support efficient communications over long distances. The thesis also evaluates the time intervals in which the satellites that constitute the best path are in line of sight with each other in order to support the SDN Controller in the management of setup operations, thus limiting the signalling overhead needed during the communication. This can lead the design, launching and integration of future hybrid quantum satellites to set up a global QI, even though trade-off between complexity, overhead could be investigated in future works by focusing on viable path selection procedures. Another interesting development consists in the use of a dynamic Dijkstra's algorithm based on the Temporal Network theory, which could result to be useful in the search for the best durable path.

However, these early architectures consider the use of a single ground Controller. The use of a greater number of Controllers and the integration of the CP into the constellation itself could provide numerous advantages. Therefore, the use of multiple Controllers integrated into the constellation itself was considered in subsequent simulations. In particular, the thesis proposes a precise architecture consisting of SDN Controllers positioned both on the ground and in the constellation itself with different roles. Specifically,

the main role of the SDN Controllers integrated into the constellation is to control the operations on the entire E2E path. Moreover, we have developed a specific communication protocol through which it is possible to obtain an E2E entanglement. The protocol consists of two main phases, the first of which is the setup of the chosen E2E path. The choice of the path is made through a centralized Dijkstra's algorithm that is executed on the MCS. During the second phase of the protocol, Controllers installed on the satellites of the constellation and which are part of the path chosen for the specific session, manage the entanglement generation and entanglement swapping procedures in order to create multiple E2E entanglements. The satellite repeaters are controlled to operate for a specific period of time corresponding to the period of existence of the E2E path that has been established. Performance has been evaluated considering the time required to establish an E2E entanglement as the conditions of the E2E path change. From the tests conducted, it is possible to deduce that as the number of satellites increases, the performance tends to improve, considering that the shorter distance increases the probability of success in order to obtain an entanglement. In fact, the time needed to obtain the entanglement strongly depends on this probability, and therefore the time needed to obtain it decreases.

Furthermore, given that there are several basic schemes for generating entanglement on a link through the coordinated action of two end nodes, this thesis compares two different procedures for the generation of E2E entanglement on a single Controller scenario located on the ground. Specifically, the considered procedures are the (i) at-midpoint and the (ii) at-source. In the at-midpoint procedure one of the two end nodes sends a flying qubit that is entangled with one of its matter qubits and a transducer at the other end of the link transfers the entanglement from the flying qubit to one of its matter qubits. On the other hand, in the at-source an entangled photon pair positioned between the two nodes with matter qubits sends an entangled photon through a quantum channel to each of the neighboring nodes. In addition, the most effective procedure has been applied to both the scenarios, the former with a single Controller on the ground capable of managing the entire constellation while in the latter we allocated multiple Controllers within the constellation itself. Adopting an architecture comprised of multiple mobile Controllers solves many issues and achieves better performance with respect to the architecture with a single Controller on the ground. In addition to limiting the traffic on the satellite Earth routes, which are the

most critical ones, it can help to reduce the overall delay, which is crucial in distributed quantum computing applications. The performance has been evaluated in terms of the overhead and latency required to establish an E2E entanglement. The proposed SDN backbone based on the use of multiple mobile Controllers deployed in the constellation allows achieving better performance for both the considered parameters with respect to the architecture with a single Controller on the ground.

Future development could consist to integrate within the MCS a specific path selection algorithm designed for QNs, which would take into account the issues of QNs and contribute to further improve performance. Specifically, considering that QRs perform the action of entanglement purification, an algorithm capable of finding the optimal number of satellites so as to guarantee specific fidelity values could partially compensate for losses due to ground-satellite paths. In addition, more accurate analysis in terms of scalability could also provide additional elements in order to allocate Controllers in the constellation even more efficiently.

This thesis also examines scenarios related to areas of more limited dimensions such as those typical of metropolitan networks. Specifically, the aim is to realize efficient QMANs composed of swarms of drones, which are considered crucial for the development of future telecommunications networks. These devices are very versatile, considering that they can be deployed on-demand in any place and time. Moreover, atmospheric links can provide lower attenuation values than OFs, guaranteeing even higher performance.

As a matter of fact, with fair weather conditions, the scattering loss can be mitigated, and the links that can be established have lower attenuation with respect to OFs. However, drones are subject to random fluctuations with respect to their positions. Specifically, these are the pitch, roll, and yaw motions typical of all types of aircraft. Furthermore, weather agents such as wind can cause a change in their position, which must be compensated. Therefore, maintaining pointing on the ground-drone and inter-drone links can result very challenging. These devices have specific systems to correct these pointing errors. As a matter of fact, the Flight Controller mitigates pointing errors compensating the trim changes due to atmospheric agents relying on the position control given by the on-board GPS receiver and IMU. However, these errors cannot be completely neglected. Considering that SDN technology has been recognized as significant for the development of QNs that require intensive control, we propose an architecture that includes

the SDN Controller directly embedded in the swarm of drones with a specific protocol. During the first phase, the mission is properly planned and the drones reach established locations based on specific GPS coordinates. Therefore, the SDN Controller sends entanglement generation messages to the drones that compose the left and right branches of the swarm to interconnect GSs and drones, including itself, on a L2L basis. Once completed this phase, the Controller sends messages to the drones to perform the entanglement swapping in order to create the E2E entanglement.

The results show that despite the atmospheric turbulence and beam wandering issues, planning the mission properly by optimizing specific objective functions, it is possible to reach reasonable fidelity values that also allow distributed quantum processing in a Quantum Cloud context. Employing a limited number of drones, it is possible to achieve significant performance in terms of entanglement rate while maintaining low overhead. Furthermore, the integration of the CP into the swarm allows performing some of the operations directly on board the drone without sending messages, limiting the overhead and packet losses. Future developments should consider the evolution of the proposed protocol in order to consider multi-Controller segments and the interoperability among QMAN also through other kinds of aerial platforms or satellite segments. Furthermore, due to its configuration, the proposed architecture can also be used for applications of QKD and, specifically, to provide entanglement-based protocols such as E91 [447].

The considered scenarios were all analyzed singularly, and an assessment of their interoperability can be indicated among the future developments. The research and definition of new path selection algorithms is fundamental, especially in the satellite field. As a matter of fact, satellites follow predetermined trajectories that can hardly be altered on demand. For this reason, an effective path selection algorithm can guarantee the minimization of the number of satellites employed, ensuring the highest possible fidelity values. In fact, considering that each satellite acts as a QRs, which can have the peculiarity of increasing the fidelity value due to the operation of entanglement purification, the selection of an optimal number of satellites can contribute to finding the right trade-off between entanglement rate and fidelity.

Furthermore, given the time-varying nature of satellite networks, future development could consist on the study of these networks considering the temporal network paradigm [448] [449] [392], where the times when edges are active are an explicit element of the representation [450]. However, con-

sidering the characteristics of QNs, some specific parameters have to be considered. For instance, with regard to the optimization problem, it is also necessary to take into account the occupancy of memories that consist of a limited number of qubits and the timing required to refresh QMs. Moreover, since the characteristics of the ground to satellite link may affect the quality of the connection, the environmental factors such as atmospheric visibility could also be considered in the optimization procedure.

Furthermore, another possible development would consist of the implementation of satellite networks for QKD. As a matter of fact, many of the considered scenarios involved the use of single satellites, and only a few realized real functional applications. Therefore, it is necessary to analyze scenarios involving the distribution of quantum keys to users on the ground by comparing various protocols. As explained in Section 3.1, these protocols consist of a quantum phase and a classical phase and differ between CVQKDs, which exploit classical technologies, and DVQKDs, some of which are purely quantum, considering that they are based on the principle of quantum entanglement.

Moreover, SDN technology can play a key role in the development of such applications. In fact, the SDN Controller could appropriately manage both the initial quantum phase and the classical phase which consists of the reconciliation and privacy amplification phases. Some studies related to this field have already been conducted by developing some of the most important QKD protocols managed through SDN on OFs networks.

In addition, considering that different QKD protocols also require different technologies, it is appropriate to make an energy assessment as well. This evaluation could be significant, especially in scenarios related to drone networks where device consumption is highly dependent on the propulsion equipment of the drones.

Furthermore, in view of the fact that intermediate layers of communications systems between terrestrial and traditional satellite segments have recently emerged, it could be important to evaluate HAPs, which can provide communications services at a regional scale. HAP are typically deployed at an altitude between 18 and 20 *km* and can ensure coverage of a specific area for long periods of time. The communication channel of these architectures requires a more in-depth study, however, they could be an interesting alternative to satellite constellations for which the deployment is very expensive. Therefore, they also need to be considered in order to contain the costs of

both launch and maintenance.

Finally, considering that Machine Learning (ML) is one of the most promising artificial intelligence tools, which was conceived to support smart radio terminals [451], these techniques could be applied to scenarios related to QNs [452]. Quantum Machine Learning (QML) is the intersection of ML and quantum computing [453]. Specifically, QML attempts to use the capacity of QCs to process data at much faster speeds than traditional computers and refers to the use of quantum systems to incarnate algorithms that allow computer programs to improve through experience [454]. As a matter of fact, superpositioned quantum states can lead to important speedups as a result of the ability to evaluate multiple states simultaneously [455]. For instance, the QC-assisted communications has been envisioned as a method to achieve extremely high data rates and link security in future QNs [456]. Furthermore, some approaches such as deep reinforcement learning could be used to address the problem of congestion in satellite or drone networks [457].

Appendix A

List of Parameters

This Appendix is related to the System Model, previously presented in Chapter 5 and Chapter 6. Here I provide a list of the fundamental parameters that have been used to formally present the mathematical model (see Section 5.3.1 and Section 6.3).

p	Entanglement generation probability
p_g	Photons generation probability
η_h	Heralding detector efficiency
η_d	Entangling detector efficiency
$p_{i,j}$	Entanglement generation probability between the i -th and j -th nodes
η_0	Optical BSM efficiency
$d_{i,j}$	Euclidean distance between two nodes
L_α	Electric field attenuation length
α	Attenuation of optical wave amplitude
ε_r	Resistivity
σ	Conductivity
$T_{i,j}$	Average time required to generate a remote entanglement
$T_{i,j}^f$	Average time required for the failed attempt
$T_{i,j}^s$	Average time required for the successful attempt
$T_{i,j}^c$	Time required for ACK transmission over a classical communication link

τ_a	Atomic BSM duration
η_a	Atomic BSM efficiency
T_r	Entanglement rate
\mathcal{G}	Set of satellites that are part of the constellation
\mathcal{V}	Set of visited nodes
L_g	Set of neighboring satellites of a satellite g
$\varphi_{ij}(t)$	Trail intensity
$\Delta\varphi_{ij}^k$	Quantity of trail substance laid on edge (i, j) by the k -th ant between time t and $t + n$
Λ_k	Tour length of the k -th ant
$p_{ij}^k(t)$	Probability of going to the j -th node
β	Weight on pheromone
α	Weight on distance
G	Directed graph
s	Source of a directed graph
$l(v, w)$	Nonnegative length in a directed graph
m	Number of edges
n	Number of vertices
$x \sim \mathcal{N}(\mu_x, \sigma_x^2)$	Misalignment error on the x-axis
$y \sim \mathcal{N}(\mu_y, \sigma_y^2)$	Misalignment error on the y-axis
V	Atmospheric visibility
ξ	Extinction coefficient
A	Specific optical attenuation
η	Drop size distribution coefficient
F^*	Application-specific fidelity threshold

Appendix B

Publications

This research activity has led to several publications in international journals and conferences. These are summarized below.¹

International Journals

1. **R. Picchi**, F. Chiti, R. Fantacci, L. Pierucci. “Towards Quantum Satellite Internetworking: A Software-Defined Networking Perspective”, *IEEE Access*, vol. 8, pp. 210370-210381, 2020. [DOI:10.1109/ACCESS.2020.3038529] 11 citations
2. F. Chiti, R. Fantacci, **R. Picchi**, L. Pierucci. “Towards the Quantum Internet: Satellite Control Plane Architectures and Protocol Design”, *Future Internet*, vol. 13, 2021. [DOI:10.3390/fi13080196] 3 citations
3. F. Chiti, R. Fantacci, **R. Picchi**, L. Pierucci. “Mobile Control Plane Design for Quantum Satellite Backbones”, *IEEE Network*, vol. 36, pp. 91-97, 2022. [DOI:10.1109/MNET.012.2100167] 3 citations
4. F. Chiti, **R. Picchi**, L. Pierucci. “Metropolitan Quantum-Drone Networking and Computing: a Software-Defined Perspective”, *IEEE Access*, vol. 10, pp. 126062-126073, 2022. [DOI:10.1109/ACCESS.2022.3226127]

Submitted

1. F. Chiti, **R. Picchi**, L. Pierucci. “The Role of Satellites for Quantum Networks: an Overview”, *Proceedings of the IEEE*, 2021.

¹The author’s bibliometric indices are the following: *H*-index = 3, total number of citations = 20 (source: Scopus on Month January, 2023).

International Conferences and Workshops

1. F. Chiti, R. Fantacci, **R. Picchi**, L. Pierucci. “Quantum Satellite Backbone Networks Design and Performance Evaluation”, in *ICC 2021 - IEEE International Conference on Communications*, Montreal (Canada), 2021. [DOI: 10.1109/ICC42927.2021.9500327] 3 citations (**Student Travel Grant winner**) .

Book Contributions

1. F. Chiti. “Internet. Prospettive, Architetture, Applicazioni”, *Società Editrice Esculapio*, Third Edition, Chapter 6, 2023.

Bibliography

- [1] D. Burg and J. H. Ausubel, “Moore’s law revisited through intel chip density,” *PLOS ONE*, vol. 16, no. 8, pp. 1–18, 08 2021. [Online]. Available: <https://doi.org/10.1371/journal.pone.0256245>
- [2] National Academies of Sciences, Engineering, and Medicine, *Domestic Manufacturing Capabilities for Critical DoD Applications: Emerging Needs in Quantum-Enabled Systems: Proceedings of a Workshop*, A. F. Johnson, Ed. Washington, DC: The National Academies Press, 2019. [Online]. Available: <https://nap.nationalacademies.org/catalog/25499/domestic-manufacturing-capabilities-for-critical-dod-applications-emerging-needs-in>
- [3] M. Castelluccio, “Holding on in an innovative storm,” *Strategic Finance*, vol. 103, no. 11, pp. 57–58, 2022.
- [4] R. Srivastava, I. Choi, T. Cook, N. Team *et al.*, “The commercial prospects for quantum computing,” *Networked Quantum Information Technologies*, 2016.
- [5] R. P. Rundle, P. W. Mills, T. Tilma, J. H. Samson, and M. J. Everitt, “Simple procedure for phase-space measurement and entanglement validation,” *Phys. Rev. A*, vol. 96, p. 022117, Aug 2017. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.96.022117>
- [6] P. Schwaha, D. Querlioz, P. Dollfus, J. Saint-Martin, M. Nedjalkov, and S. Selberherr, “Decoherence effects in the wigner function formalism,” *Journal of Computational Electronics*, vol. 12, no. 3, pp. 388–396, Sep 2013. [Online]. Available: <https://doi.org/10.1007/s10825-013-0480-9>
- [7] M. A. Schlosshauer, *Decoherence and the Quantum-To-Classical Transition*. Springer Berlin Heidelberg, 2007. [Online]. Available: <https://doi.org/10.1007/978-3-540-35775-9>
- [8] J. M. Gambetta, J. M. Chow, and M. Steffen, “Building logical qubits in a superconducting quantum computing system,” *npj Quantum Information*, vol. 3, no. 1, p. 2, Jan 2017. [Online]. Available: <https://doi.org/10.1038/s41534-016-0004-0>

- [9] J. Russell, "Application of quantum key distribution," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, 2008, pp. 1–6.
- [10] G. Zhao, S. Zhao, Z. Yao, W. Meng, X. Wang, Z. Zhu, and F. Liu, "Forward spectral filtering parallel quantum key distribution system," *Optics Communications*, vol. 298-299, pp. 254–259, 2013. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S003040181300151X>
- [11] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," *IET Quantum Communication*, vol. 1, no. 1, pp. 3–8, 2020. [Online]. Available: <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-qt.2020.0002>
- [12] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, "A quantum network of clocks," *Nature Physics*, vol. 10, no. 8, pp. 582–587, Aug 2014. [Online]. Available: <https://doi.org/10.1038/nphys3000>
- [13] M. Lanzagorta and J. Uhlmann, "Opportunities and challenges of quantum radar," *IEEE Aerospace and Electronic Systems Magazine*, vol. 35, no. 11, pp. 38–56, 2020.
- [14] W. Kozłowski and S. Wehner, "Towards large-scale quantum networks," in *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication*, ser. NANOCOM '19. New York, NY, USA: Association for Computing Machinery, 2019. [Online]. Available: <https://doi.org/10.1145/3345312.3345497>
- [15] C. Liorni, H. Kampermann, and D. Bruß, "Quantum repeaters in space," *New Journal of Physics*, vol. 23, no. 5, p. 053021, may 2021. [Online]. Available: <https://doi.org/10.1088/1367-2630/abfa63>
- [16] M. Gündoğan, J. S. Sidhu, V. Henderson, L. Mazzarella, J. Wolters, D. K. L. Oi, and M. Krutzik, "Proposal for space-borne quantum memories for global quantum networking," *npj Quantum Information*, vol. 7, no. 1, p. 128, Aug 2021. [Online]. Available: <https://doi.org/10.1038/s41534-021-00460-9>
- [17] R. Maaloul, R. Taktak, L. Chaari, and B. Cousin, "Energy-aware routing in carrier-grade ethernet using sdn approach," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 3, pp. 844–858, 2018.
- [18] J. R. Wertz, *Orbit & Constellation Design & Management: Spacecraft Orbit and Attitude Systems*. Microcosm Press, 2001.
- [19] B. Yaglioglu and O. Tekinalp, "Long term and safe relative orbit design for heterogeneous spacecraft clusters," *Advances in Space Research*, vol. 67, no. 11, pp. 3546–3558, 2021, satellite Constellations and Formation Flying. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0273117720304555>

- [20] R. Picchi, F. Chiti, R. Fantacci, and L. Pierucci, "Towards quantum satellite internetworking: A software-defined networking perspective," *IEEE Access*, vol. 8, pp. 210 370–210 381, 2020, ©[2020] IEEE. Reprinted, with permission, from [Chiti Francesco, Romano Fantacci and Laura Pierucci, Towards Quantum Satellite Internetworking: A Software-Defined Networking Perspective, *IEEE Access*, 17 November 2020].
- [21] F. Chiti, R. Fantacci, R. Picchi, and L. Pierucci, "Quantum satellite backbone networks design and performance evaluation," in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6, ©[2021] IEEE. Reprinted, with permission, from [Chiti Francesco, Romano Fantacci and Laura Pierucci, Quantum Satellite Backbone Networks Design and Performance Evaluation, *ICC 2021 - IEEE International Conference on Communications*, 06 August 2021].
- [22] F. Chiti, R. Fantacci, R. Picchi, and L. Pierucci, "Towards the quantum internet: Satellite control plane architectures and protocol design," *Future Internet*, vol. 13, no. 8, 2021. [Online]. Available: <https://www.mdpi.com/1999-5903/13/8/196>
- [23] F. Chiti, R. Fantacci, R. Picchi, and L. Pierucci, "Mobile control plane design for quantum satellite backbones," *IEEE Network*, vol. 36, no. 1, pp. 91–97, 2022, ©[2022] IEEE. Reprinted, with permission, from [Chiti Francesco, Romano Fantacci and Laura Pierucci, Mobile Control Plane Design for Quantum Satellite Backbones, *IEEE Access*, 01 February 2022].
- [24] I. Pogorelov, T. Feldker, C. D. Marciniak, L. Postler, G. Jacob, O. Kriegelsteiner, V. Podlesnic, M. Meth, V. Negnevitsky, M. Stadler, B. Höfer, C. Wächter, K. Lakhmanskiy, R. Blatt, P. Schindler, and T. Monz, "Compact ion-trap quantum computing demonstrator," *PRX Quantum*, vol. 2, p. 020343, Jun 2021. [Online]. Available: <https://link.aps.org/doi/10.1103/PRXQuantum.2.020343>
- [25] J. Zhang, J. F. Campbell, D. C. Sweeney II, and A. C. Hupman, "Energy consumption models for delivery drones: A comparison and assessment," *Transportation Research Part D: Transport and Environment*, vol. 90, p. 102668, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1361920920308531>
- [26] T. Elijah, R. S. Jamisola, Z. Tjiparuro, and M. Namoshe, "A review on control and maneuvering of cooperative fixed-wing drones," *International Journal of Dynamics and Control*, vol. 9, no. 3, pp. 1332–1349, Sep 2021. [Online]. Available: <https://doi.org/10.1007/s40435-020-00710-2>
- [27] F. Chiti, R. Picchi, and L. Pierucci, "Metropolitan quantum-drone networking and computing: A software-defined perspective," *IEEE Access*, vol. 10,

- pp. 126 062–126 073, 2022, ©[2022] IEEE. Reprinted, with permission, from [Chiti Francesco and Laura Pierucci, Metropolitan Quantum-Drone Networking and Computing: A Software-Defined Perspective, IEEE Access, 01 December 2022].
- [28] S.-G. Kim, E. Lee, I.-P. Hong, and J.-G. Yook, “Review of intentional electromagnetic interference on uav sensor modules and experimental study,” *Sensors*, vol. 22, no. 6, 2022. [Online]. Available: <https://www.mdpi.com/1424-8220/22/6/2384>
- [29] “The nobel prize in physics 2022,” 2022, [Online; accessed 27-December-2022]. [Online]. Available: <https://www.nobelprize.org/prizes/physics/2022/summary/>
- [30] A. Peres and D. R. Terno, “Quantum information and relativity theory,” *Rev. Mod. Phys.*, vol. 76, pp. 93–123, Jan 2004. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.76.93>
- [31] C. Bennett and P. Shor, “Quantum information theory,” *IEEE Transactions on Information Theory*, vol. 44, no. 6, pp. 2724–2742, 1998.
- [32] D. Deutsch and R. Penrose, “Quantum theory, the church–turing principle and the universal quantum computer,” *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, no. 1818, pp. 97–117, 1985. [Online]. Available: <https://royalsocietypublishing.org/doi/abs/10.1098/rspa.1985.0070>
- [33] J. Li, N. Li, Y. Zhang, S. Wen, W. Du, W. Chen, and W. Ma, “A survey on quantum cryptography,” *Chinese Journal of Electronics*, vol. 27, no. 2, pp. 223–228, 2018. [Online]. Available: <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cje.2018.01.017>
- [34] A. Kumar and S. Garhwal, “State-of-the-art survey of quantum cryptography,” *Archives of Computational Methods in Engineering*, vol. 28, no. 5, pp. 3831–3868, Aug 2021. [Online]. Available: <https://doi.org/10.1007/s11831-021-09561-2>
- [35] E. Diamanti and A. Leverrier, “Distributing secret keys with quantum continuous variables: Principle, security and implementations,” *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015. [Online]. Available: <https://www.mdpi.com/1099-4300/17/9/6072>
- [36] M. M. Wilde, *Quantum Information Theory*. Cambridge University Press, nov 2016. [Online]. Available: <https://doi.org/10.1017%2F9781316809976>
- [37] C. H. Bennett and S. J. Wiesner, “Communication via one- and two-particle operators on einstein-podolsky-rosen states,” *Phys. Rev. Lett.*, vol. 69, pp. 2881–2884, Nov 1992. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.69.2881>

- [38] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
- [39] M. Keyl, “Fundamentals of quantum information theory,” *Physics Reports*, vol. 369, no. 5, pp. 431–548, 2002. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0370157302002661>
- [40] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, Jan 1992. [Online]. Available: <https://doi.org/10.1007/BF00191318>
- [41] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, “Dense coding in experimental quantum communication,” *Phys. Rev. Lett.*, vol. 76, pp. 4656–4659, Jun 1996.
- [42] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.70.1895>
- [43] P. Shor, “Algorithms for quantum computation: discrete logarithms and factoring,” in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, pp. 124–134.
- [44] P. W. Shor, “Polynomial time algorithms for discrete logarithms and factoring on a quantum computer,” in *Algorithmic Number Theory*, L. M. Adleman and M.-D. Huang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 289–289.
- [45] A. W. Harrow and A. Montanaro, “Quantum computational supremacy,” *Nature*, vol. 549, no. 7671, pp. 203–209, Sep 2017. [Online]. Available: <https://doi.org/10.1038/nature23458>
- [46] A. Papageorgiou and J. F. Traub, “Measures of quantum computing speedup,” *Phys. Rev. A*, vol. 88, p. 022316, Aug 2013. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.88.022316>
- [47] N. Ul Ain and A. ur Rahman, “Quantum cryptography: a comprehensive survey,” *Journal of Information Assurance and Security*, vol. 11, no. 1, pp. 31–38, 2016.
- [48] E. Gibney, “Quantum gold rush: the private funding pouring into quantum start-ups,” *Nature*, vol. 574, no. 7776, pp. 22–24, October 2019. [Online]. Available: <https://doi.org/10.1038/d41586-019-02935-4>
- [49] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, A. Iera, Y. Koucheryavy, and G. Araniti, “Non-terrestrial networks in 5g amp; beyond: A survey,” *IEEE Access*, vol. 8, pp. 165 178–165 200, 2020.

- [50] S. Kota and G. Giambene, “6g integrated non-terrestrial networks: Emerging technologies and challenges,” in *2021 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2021, pp. 1–6.
- [51] M. Giordani and M. Zorzi, “Satellite communication at millimeter waves: a key enabler of the 6g era,” in *2020 International Conference on Computing, Networking and Communications (ICNC)*, 2020, pp. 383–388.
- [52] M. Handley, “Delay is not an option: Low latency routing in space,” in *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*, ser. HotNets ’18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: <https://doi.org/10.1145/3286062.3286075>
- [53] O. Markovitz and M. Segal, “Advanced routing algorithms for low orbit satellite constellations,” in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.
- [54] T. de Cola and I. Bisio, “Qos optimisation of embb services in converged 5g-satellite networks,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 12 098–12 110, 2020.
- [55] S. Watts and O. G. Aliu, “5g resilient backhaul using integrated satellite networks,” in *2014 7th Advanced Satellite Multimedia Systems Conference and the 13th Signal Processing for Space Communications Workshop (ASM-S/SPSC)*, 2014, pp. 114–119.
- [56] H. Kim and N. Feamster, “Improving network management with software defined networking,” *IEEE Communications Magazine*, vol. 51, no. 2, pp. 114–119, 2013.
- [57] I. F. Akyildiz, A. Kak, and S. Nie, “6g and beyond: The future of wireless communications systems,” *IEEE Access*, vol. 8, pp. 133 995–134 030, 2020.
- [58] E. Schrödinger, “Discussion of probability relations between separated systems,” *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 31, no. 4, pp. 555–563, 1935.
- [59] R. Lo Franco and G. Compagno, “Indistinguishability of elementary systems as a resource for quantum information processing,” *Phys. Rev. Lett.*, vol. 120, p. 240403, Jun 2018. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.120.240403>
- [60] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, “Advances in quantum teleportation,” *Nature Photonics*, vol. 9, no. 10, pp. 641–652, Oct 2015. [Online]. Available: <https://doi.org/10.1038/nphoton.2015.154>
- [61] G. Cariolaro, *Quantum Communications*, ser. Signals and Communication Technology. Springer International Publishing, 2015.

- [62] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, Sep 2017. [Online]. Available: <https://doi.org/10.1038/nature23675>
- [63] T. S. Humble and R. J. Sadler, "Software-defined quantum communication systems," *Optical Engineering*, vol. 53, no. 8, 1 2014. [Online]. Available: <https://www.osti.gov/biblio/1150348>
- [64] V. Martin, A. Aguado, J. P. Brito, A. L. Sanz, P. Salas, D. R. López, V. López, A. Pastor-Perales, A. Poppe, and M. Peev, "Quantum aware sdn nodes in the madrid quantum network," in *2019 21st International Conference on Transparent Optical Networks (ICTON)*, 2019, pp. 1–4.
- [65] A. Aguado, V. Martin, D. Lopez, M. Peev, J. Martinez-Mateo, J. Rosales, F. de la Iglesia, M. Gomez, E. Hugues Salas, A. Lord, R. Nejabati, and D. Simeonidou, "Quantum-aware software defined networks," in *6th International Conference on Quantum Cryptography (QCRYPT 2016)*. QCrypt, Sep 2016, 42nd European Conference on Optical Communication, ECOC 2016 : 42nd European Conference and Exhibition on Optical Communication ; Conference date: 18-09-2016 Through 22-09-2016.
- [66] M. Caleffi, "Optimal routing for quantum networks," *IEEE Access*, vol. 5, pp. 22 299–22 312, 2017.
- [67] L. Gyongyosi and S. Imre, "Entanglement access control for the quantum internet," *Quantum Information Processing*, vol. 18, no. 4, p. 107, Feb 2019. [Online]. Available: <https://doi.org/10.1007/s11128-019-2226-5>
- [68] F. Samara, N. Maring, A. Martin, A. S. Raja, T. J. Kippenberg, H. Zbinden, and R. Thew, "Entanglement swapping between independent and asynchronous integrated photon-pair sources," *Quantum Science and Technology*, vol. 6, no. 4, p. 045024, sep 2021. [Online]. Available: <https://doi.org/10.1088/2058-9565/abf599>
- [69] G. Guccione, T. Darras, H. L. Jeannic, V. B. Verma, S. W. Nam, A. Cavallés, and J. Laurat, "Connecting heterogeneous quantum networks by hybrid entanglement swapping," *Science Advances*, vol. 6, no. 22, p. eaba4508, 2020. [Online]. Available: <https://www.science.org/doi/abs/10.1126/sciadv.aba4508>
- [70] Q. Ruihong and M. Ying, "Research progress of quantum repeaters," *Journal of Physics: Conference Series*, vol. 1237, p. 052032, jun 2019. [Online]. Available: <https://doi.org/10.1088/1742-6596/1237/5/052032>

- [71] K. Hammerer, A. S. Sørensen, and E. S. Polzik, “Quantum interface between light and atomic ensembles,” *Rev. Mod. Phys.*, vol. 82, pp. 1041–1093, Apr 2010. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.82.1041>
- [72] A. Kuzmich, K. Mølmer, and E. S. Polzik, “Spin squeezing in an ensemble of atoms illuminated with squeezed light,” *Phys. Rev. Lett.*, vol. 79, pp. 4782–4785, Dec 1997. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.79.4782>
- [73] W. K. Wootters and W. H. Zurek, “The no-cloning theorem,” *Physics Today*, vol. 62, no. 2, pp. 76–77, 2009. [Online]. Available: <https://doi.org/10.1063/1.3086114>
- [74] D. Huang, Y. Zhao, T. Yang, S. Rahman, X. Yu, X. He, and J. Zhang, “Quantum key distribution over double-layer quantum satellite networks,” *IEEE Access*, vol. 8, pp. 16 087–16 098, 2020.
- [75] S. Weigert, *No-Cloning Theorem*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 404–405. [Online]. Available: https://doi.org/10.1007/978-3-540-70626-7_124
- [76] M. G. Kuzyk, “Quantum no-cloning theorem and entanglement,” *American Journal of Physics*, vol. 87, no. 5, pp. 325–327, 2019. [Online]. Available: <https://doi.org/10.1119/1.5093815>
- [77] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, “Inside quantum repeaters,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 78–90, 2015.
- [78] C. Agnesi, F. Vedovato, M. Schiavon, D. Dequal, L. Calderaro, M. Tomasin, D. G. Marangon, A. Stanco, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, “Exploring the boundaries of quantum mechanics: advances in satellite quantum communications,” *Philosophical Transactions of the Royal Society of London Series A*, vol. 376, no. 2123, p. 20170461, Jul. 2018.
- [79] W. Kozłowski, S. Wehner, R. V. Meter, B. Rijsman, A. S. Cacciapuoti, M. Caleffi, and S. Nagayama, “Architectural Principles for a Quantum Internet,” Internet Engineering Task Force, Internet-Draft draft-irtf-qirg-principles-10, Feb. 2022, work in Progress. [Online]. Available: <https://datatracker.ietf.org/doc/html/draft-irtf-qirg-principles-10>
- [80] W. H. Zurek, “Decoherence, einselection, and the quantum origins of the classical,” *Rev. Mod. Phys.*, vol. 75, pp. 715–775, May 2003. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.75.715>
- [81] L. Lerner, “A demonstration of decoherence for beginners,” *American Journal of Physics*, vol. 85, no. 11, pp. 870–872, 2017. [Online]. Available: <https://doi.org/10.1119/1.5005526>

- [82] S. Pirandola, "Satellite quantum communications: Fundamental bounds and practical security," *Phys. Rev. Research*, vol. 3, p. 023130, May 2021. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevResearch.3.023130>
- [83] 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. 82–82, Oct 2002. [Online]. Available: <https://doi.org/10.1088/1367-2630/4/1/382>
- [84] J. H. Reina, L. Quiroga, and N. F. Johnson, "Decoherence of quantum registers," *Phys. Rev. A*, vol. 65, p. 032326, Mar 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.65.032326>
- [85] L. Bacsardi, "On the way to quantum-based satellite communication," *IEEE Communications Magazine*, vol. 51, no. 8, pp. 50–55, 2013.
- [86] Laszlo Bacsardi, "Satellite communication over quantum channel," *Acta Astronautica*, vol. 61, no. 1, pp. 151–159, 2007, bringing Space Closer to People, Selected Proceedings of the 57th IAF Congress, Valencia, Spain, 2-6 October, 2006. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S009457650700032X>
- [87] J. M. Perdignes Armengol, B. Furch, C. J. de Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Quantum communications at esa: Towards a space experiment on the iss," *Acta Astronautica*, vol. 63, no. 1, pp. 165–178, 2008, touching Humanity - Space for Improving Quality of Life. Selected Proceedings of the 58th International Astronautical Federation Congress, Hyderabad, India, 24-28 September 2007. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0094576507003359>
- [88] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdignes, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, no. 7, pp. 481–486, Jul 2007. [Online]. Available: <https://doi.org/10.1038/nphys629>
- [89] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, "High-fidelity transmission of entanglement over a high-loss free-space channel," *Nature Physics*, vol. 5, no. 6, pp. 389–392, Jun 2009. [Online]. Available: <https://doi.org/10.1038/nphys1255>
- [90] M. Grabner and V. Kvicera, "The wavelength dependent model of extinction in fog and haze for free space optical communication," *Opt.*

- Express*, vol. 19, no. 4, pp. 3379–3386, Feb 2011. [Online]. Available: <http://opg.optica.org/oe/abstract.cfm?URI=oe-19-4-3379>
- [91] I. I. Kim, B. McArthur, and E. J. Korevaar, “Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications,” in *Optical Wireless Communications III*, E. J. Korevaar, Ed., vol. 4214, International Society for Optics and Photonics. SPIE, 2001, pp. 26 – 37. [Online]. Available: <https://doi.org/10.1117/12.417512>
- [92] N. Alshaer, A. Moawad, and T. Ismail, “Reliability and security analysis of an entanglement-based qkd protocol in a dynamic ground-to-uav fso communications system,” *IEEE Access*, vol. 9, pp. 168 052–168 067, 2021.
- [93] D. K. Oi, A. Ling, G. Vallone, P. Villoresi, S. Greenland, E. Kerr, M. Macdonald, H. Weinfurter, H. Kuiper, E. Charbon, and R. Ursin, “Cubesat quantum communications mission,” *EPJ Quantum Technology*, vol. 4, no. 1, p. 6, Apr 2017. [Online]. Available: <https://doi.org/10.1140/epjqt/s40507-017-0060-1>
- [94] M. Sasaki, “Quantum networks: where should we be heading?” vol. 2, no. 2, p. 020501, apr 2017. [Online]. Available: <https://doi.org/10.1088/2058-9565/aa6994>
- [95] Y. Su, Y. Liu, Y. Zhou, J. Yuan, H. Cao, and J. Shi, “Broadband leo satellite communications: Architectures and key technologies,” *IEEE Wireless Communications*, vol. 26, no. 2, pp. 55–61, 2019.
- [96] A. Guidotti, A. Vanelli-Coralli, T. Foggi, G. Colavolpe, M. Caus, J. Bas, S. Cioni, and A. Modenini, “Lte-based satellite communications in leo mega-constellations,” *International Journal of Satellite Communications and Networking*, vol. 37, no. 4, pp. 316–330, 2019. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.1258>
- [97] R. Bedington, J. M. Arrazola, and A. Ling, “Progress in satellite quantum key distribution,” *npj Quantum Information*, vol. 3, no. 1, p. 30, Aug 2017. [Online]. Available: <https://doi.org/10.1038/s41534-017-0031-5>
- [98] A. Papa, T. De Cola, P. Vizarreta, M. He, C. Mas Machuca, and W. Kellerer, “Dynamic sdn controller placement in a leo constellation satellite network,” in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 206–212.
- [99] S. Hassas Yeganeh and Y. Ganjali, “Kandoo: A framework for efficient and scalable offloading of control applications,” in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, ser. HotSDN ’12. New York, NY, USA: Association for Computing Machinery, 2012, pp. 19–24. [Online]. Available: <https://doi.org/10.1145/2342441.2342446>

- [100] R. Ahmed and R. Boutaba, "Design considerations for managing wide area software defined networks," *IEEE Communications Magazine*, vol. 52, no. 7, pp. 116–123, 2014.
- [101] D. Tuncer, M. Charalambides, S. Clayman, and G. Pavlou, "Adaptive resource management and control in software defined networks," *IEEE Transactions on Network and Service Management*, vol. 12, no. 1, pp. 18–33, 2015.
- [102] M. Najafi, H. Ajam, V. Jamali, P. D. Diamantoulakis, G. K. Karagiannidis, and R. Schober, "Statistical modeling of fso fronthaul channel for drone-based networks," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.
- [103] H.-Y. Liu *et al.*, "Optical-relayed entanglement distribution using drones as mobile nodes," *Phys. Rev. Lett.*, vol. 126, p. 020503, Jan 2021. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.126.020503>
- [104] M. Petkovic and M. Narandzic, "Overview of uav based free-space optical communication systems," in *Interactive Collaborative Robotics*, A. Ronzhin, G. Rigoll, and R. Meshcheryakov, Eds. Cham: Springer International Publishing, 2019, pp. 270–277.
- [105] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *J. Lightwave Technol.*, vol. 25, no. 7, pp. 1702–1710, Jul 2007. [Online]. Available: <http://opg.optica.org/jlt/abstract.cfm?URI=jlt-25-7-1702>
- [106] H. AlQuwaiee, H.-C. Yang, and M.-S. Alouini, "On the asymptotic capacity of dual-aperture fso systems with generalized pointing error model," *IEEE Transactions on Wireless Communications*, vol. 15, no. 9, pp. 6502–6512, 2016.
- [107] A. D. Hill, J. Chapman, K. Herndon, C. Chopp, D. J. Gauthier, and P. Kwiat, "Drone-based quantum key distribution," *Urbana*, vol. 51, pp. 61 801–63 003, 2017.
- [108] Z. Wang, Z. Guo, G. Mogos, and Z. Gao, "Quantum key distribution by drone," *Journal of Physics: Conference Series*, vol. 2095, no. 1, p. 012080, nov 2021. [Online]. Available: <https://doi.org/10.1088/1742-6596/2095/1/012080>
- [109] H.-Y. Liu, X.-H. Tian, C. Gu, P. Fan, X. Ni, R. Yang, J.-N. Zhang, M. Hu, J. Guo, X. Cao, X. Hu, G. Zhao, Y.-Q. Lu, Y.-X. Gong, Z. Xie, and S.-N. Zhu, "Drone-based entanglement distribution towards mobile quantum networks," *National Science Review*, vol. 7, no. 5, pp. 921–928, 01 2020. [Online]. Available: <https://doi.org/10.1093/nsr/nwz227>

- [110] L. Gupta, R. Jain, and G. Vaszkun, "Survey of important issues in uav communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123–1152, 2016.
- [111] M. Caleffi, A. S. Cacciapuoti, and G. Bianchi, "Quantum internet: From communication to distributed computing!" in *Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication*, ser. NANOCOM '18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: <https://doi.org/10.1145/3233188.3233224>
- [112] K. S. Chou, J. Z. Blumoff, C. S. Wang, P. C. Reinhold, C. J. Axline, Y. Y. Gao, L. Frunzio, M. H. Devoret, L. Jiang, and R. J. Schoelkopf, "Deterministic teleportation of a quantum gate between two logical qubits," *Nature*, vol. 561, no. 7723, pp. 368–373, Sep 2018. [Online]. Available: <https://doi.org/10.1038/s41586-018-0470-y>
- [113] C. Wang, A. Rahman, R. Li, M. Aelmans, and K. Chakraborty, "Application Scenarios for the Quantum Internet," Internet Engineering Task Force, Internet-Draft draft-irtf-qirg-quantum-internet-use-cases-13, Jun. 2022, work in Progress. [Online]. Available: <https://datatracker.ietf.org/doc/html/draft-irtf-qirg-quantum-internet-use-cases-13>
- [114] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, p. 040502, Jul 2015. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.115.040502>
- [115] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*. Springer International Publishing, 2019. [Online]. Available: <https://doi.org/10.1007%2F978-3-030-27565-5>
- [116] M. Schlosshauer, "Quantum decoherence," *Physics Reports*, vol. 831, pp. 1–57, 2019, quantum decoherence. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0370157319303084>
- [117] M. Matriani and S. S. Iyengar, "Satellite quantum repeaters for a quantum internet," *Quantum Engineering*, vol. 2, no. 4, p. e55, 2020. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/que2.55>
- [118] M. Caleffi, D. Chandra, D. Cuomo, S. Hassanpour, and A. S. Cacciapuoti, "The rise of the quantum internet," *Computer*, vol. 53, no. 6, pp. 67–72, 2020.
- [119] M. R. Abd Rahim, R. A. Rashid, A. M. Rateb, M. A. Sarijari, A. S. Abdullah, A. H. F. A. Hamid, H. Sayuti, and N. Fisal, *Service-Oriented Architecture for IoT Home Area Networking in 5G*. John Wiley & Sons, Ltd, 2018, ch. 16, pp. 577–602. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119333142.ch16>

- [120] M. P. Papazoglou and W.-J. Van Den Heuvel, "Service oriented architectures: approaches, technologies and research issues," *The VLDB Journal*, vol. 16, no. 3, pp. 389–415, Jul 2007. [Online]. Available: <https://doi.org/10.1007/s00778-007-0044-3>
- [121] R. Segura, "Service-oriented architecture for coalition satellite communications," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, 2008, pp. 1–8.
- [122] G. Amponis, T. Lagkas, M. Zevgara, G. Katsikas, T. Xirofotou, I. Moscholios, and P. Sarigiannidis, "Drones in b5g/6g networks as flying base stations," *Drones*, vol. 6, no. 2, 2022. [Online]. Available: <https://www.mdpi.com/2504-446X/6/2/39>
- [123] D. Mishra *et al.*, "Drone networking in the 6g era: A technology overview," *IEEE Communications Standards Magazine*, vol. 5, no. 4, pp. 88–95, 2021.
- [124] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced positioning and clock synchronization," *Nature*, vol. 412, no. 6845, pp. 417–419, Jul 2001. [Online]. Available: <https://doi.org/10.1038/35086525>
- [125] R. Ross and R. Hoque, "Augmenting gps with geolocated fiducials to improve accuracy for mobile robot applications," *Applied Sciences*, vol. 10, no. 1, 2020. [Online]. Available: <https://www.mdpi.com/2076-3417/10/1/146>
- [126] T. D. Nguyen, "Evaluation of the accuracy of the ship location determined by GPS global positioning system on a given sea area," vol. 1515, p. 042010, apr 2020. [Online]. Available: <https://doi.org/10.1088/1742-6596/1515/4/042010>
- [127] A. Kumar, S. Kumar, P. Lal, P. Saikia, P. K. Srivastava, and G. P. Petropoulos, "Chapter 1 - introduction to gps/gnss technology," in *GPS and GNSS Technology in Geosciences*, G. p. Petropoulos and P. K. Srivastava, Eds. Elsevier, 2021, pp. 3–20. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780128186176000019>
- [128] R. Kaltenbaek, A. Acin, L. Bacsardi, P. Bianco, P. Bouyer, E. Diamanti, C. Marquardt, Y. Omar, V. Pruneri, E. Rasel, B. Sang, S. Seidel, H. Ulbricht, R. Ursin, P. Villorosi, M. van den Bossche, W. von Klitzing, H. Zbinden, M. Paternostro, and A. Bassi, "Quantum technologies in space," *Experimental Astronomy*, vol. 51, no. 3, pp. 1677–1694, Jun 2021. [Online]. Available: <https://doi.org/10.1007/s10686-021-09731-x>
- [129] W. F. McGrew, X. Zhang, R. J. Fasano, S. A. Schäffer, K. Beloy, D. Nicolodi, R. C. Brown, N. Hinkley, G. Milani, M. Schioppo, T. H. Yoon, and A. D. Ludlow, "Atomic clock performance enabling geodesy below the centimetre level," *Nature*, vol. 564, no. 7734, pp. 87–90, Dec 2018. [Online]. Available: <https://doi.org/10.1038/s41586-018-0738-2>

- [130] W. Dür, R. Lamprecht, and S. Heusler, “Towards a quantum internet,” *European Journal of Physics*, vol. 38, no. 4, p. 043001, may 2017. [Online]. Available: <https://doi.org/10.1088/1361-6404/aa6df7>
- [131] J. D. Monnier, “Optical interferometry in astronomy,” *Reports on Progress in Physics*, vol. 66, no. 5, pp. 789–857, apr 2003. [Online]. Available: <https://doi.org/10.1088/0034-4885/66/5/203>
- [132] D. Gottesman, T. Jennewein, and S. Croke, “Longer-baseline telescopes using quantum repeaters,” *Phys. Rev. Lett.*, vol. 109, p. 070503, Aug 2012. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.109.070503>
- [133] J. J. C. Teixeira-Dias, “How to teach the postulates of quantum mechanics without enigma,” *Journal of Chemical Education*, vol. 60, no. 11, p. 963, Nov 1983. [Online]. Available: <https://doi.org/10.1021/ed060p963>
- [134] S. Imre, “Quantum communications: explained for communication engineers,” *IEEE Communications Magazine*, vol. 51, no. 8, pp. 28–35, 2013.
- [135] R. Friedberg and T. Lee, “New ways to solve the schroedinger equation,” *Annals of Physics*, vol. 316, no. 1, pp. 44–106, 2005. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0003491604001460>
- [136] L. Nottale and M.-N. Célérier, “Derivation of the postulates of quantum mechanics from the first principles of scale relativity,” *Journal of Physics A: Mathematical and Theoretical*, vol. 40, no. 48, pp. 14 471–14 498, nov 2007. [Online]. Available: <https://doi.org/10.1088/1751-8113/40/48/012>
- [137] N. Wiener and A. Siegel, “A new form for the statistical postulate of quantum mechanics,” *Phys. Rev.*, vol. 91, pp. 1551–1560, Sep 1953. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRev.91.1551>
- [138] S. Imre and F. Balázs, *Quantum Computing Basics*. John Wiley & Sons, Ltd, 2004, ch. 2, pp. 7–42. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470869048.ch2>
- [139] M. Y. Siraichi, V. F. d. Santos, C. Collange, and F. M. Q. Pereira, “Qubit allocation,” in *Proceedings of the 2018 International Symposium on Code Generation and Optimization*, ser. CGO 2018. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: <https://doi.org/10.1145/3168822>
- [140] M. Schlosshauer, “Decoherence, the measurement problem, and interpretations of quantum mechanics,” *Rev. Mod. Phys.*, vol. 76, pp. 1267–1305, Feb 2005. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.76.1267>
- [141] K. E. Cahill and R. J. Glauber, “Density operators and quasiprobability distributions,” *Phys. Rev.*, vol. 177, pp. 1882–1902, Jan 1969. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRev.177.1882>

- [142] L. Jaeger, *The Second Quantum Revolution: From Entanglement to Quantum Computing and Other Super-Technologies*. Springer, 2018.
- [143] *Quantum Teleportation and Entanglement*. John Wiley & Sons, Ltd, ch. 3, pp. 125–178. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/9783527635283.ch3>
- [144] R. D. Taylor, “Quantum artificial intelligence: A "precautionary" u.s. approach?” *Telecommunications Policy*, vol. 44, no. 6, p. 101909, 2020, artificial intelligence, economy and society. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S030859612030001X>
- [145] D. Sych and G. Leuchs, “A complete basis of generalized bell states,” *New Journal of Physics*, vol. 11, no. 1, p. 013006, jan 2009. [Online]. Available: <https://doi.org/10.1088/1367-2630/11/1/013006>
- [146] L. Gyongyosi, S. Imre, and H. V. Nguyen, “A survey on quantum channel capacities,” *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1149–1205, 2018.
- [147] R. V. Meter, *Quantum Networking*. John Wiley & Sons, Ltd, apr 2014. [Online]. Available: <https://doi.org/10.1002%2F9781118648919>
- [148] L. Gyongyosi and S. Imre, “Multilayer optimization for the quantum internet,” *Scientific Reports*, vol. 8, no. 1, p. 12690, Aug 2018. [Online]. Available: <https://doi.org/10.1038/s41598-018-30957-x>
- [149] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, “Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres,” *Nature*, vol. 526, no. 7575, pp. 682–686, Oct 2015. [Online]. Available: <https://doi.org/10.1038/nature15759>
- [150] A. Tchebotareva, S. L. N. Hermans, P. C. Humphreys, D. Voigt, P. J. Harmsma, L. K. Cheng, A. L. Verlaan, N. Dijkhuizen, W. de Jong, A. Dréau, and R. Hanson, “Entanglement between a diamond spin qubit and a photonic time-bin qubit at telecom wavelength,” *Phys. Rev. Lett.*, vol. 123, p. 063601, Aug 2019. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.123.063601>
- [151] D. D. Awschalom, R. Hanson, J. Wrachtrup, and B. B. Zhou, “Quantum technologies with optically interfaced solid-state spins,” *Nature Photonics*, vol. 12, no. 9, pp. 516–527, Sep 2018. [Online]. Available: <https://doi.org/10.1038/s41566-018-0232-2>

- [152] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct 1982. [Online]. Available: <https://doi.org/10.1038/299802a0>
- [153] J. Ortigoso, "Twelve years before the quantum no-cloning theorem," *American Journal of Physics*, vol. 86, no. 3, pp. 201–205, 2018. [Online]. Available: <https://doi.org/10.1119/1.5021356>
- [154] N. D. Mermin, *Quantum Computer Science: An Introduction*. USA: Cambridge University Press, 2007.
- [155] M. Soeken, D. M. Miller, and R. Drechsler, "Quantum circuits employing roots of the pauli matrices," *Phys. Rev. A*, vol. 88, p. 042322, Oct 2013. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.88.042322>
- [156] G. L. Light, "Pauli matrices immersion," *Materials Science and Engineering: B*, vol. 264, p. 114910, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0921510720304177>
- [157] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Phys. Rev. A*, vol. 52, pp. 3457–3467, Nov 1995. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.52.3457>
- [158] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," *Phys. Rev. Lett.*, vol. 75, pp. 4714–4717, Dec 1995. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.75.4714>
- [159] G. Nannicini, "An introduction to quantum computing, without the physics," *SIAM Review*, vol. 62, no. 4, pp. 936–981, 2020. [Online]. Available: <https://doi.org/10.1137/18M1170650>
- [160] S. MohammadNejad and A. KhodadadKashi, "Cnot-based quantum swapping of polarization and modal encoded qubits in photonic ti:linbo3 channel waveguides," *Optical and Quantum Electronics*, vol. 51, no. 9, p. 301, Aug 2019. [Online]. Available: <https://doi.org/10.1007/s11082-019-2011-9>
- [161] J. Joo, Y.-J. Park, S. Oh, and J. Kim, "Quantum teleportation via a w state," *New Journal of Physics*, vol. 5, pp. 136–136, oct 2003. [Online]. Available: <https://doi.org/10.1088/1367-2630/5/1/136>
- [162] K. Yang, L. Huang, W. Yang, and F. Song, "Quantum teleportation via ghz-like state," *International Journal of Theoretical Physics*, vol. 48, no. 2, pp. 516–521, Feb 2009. [Online]. Available: <https://doi.org/10.1007/s10773-008-9827-6>
- [163] B. Coecke and A. Kissinger, "The compositional structure of multipartite quantum entanglement," in *Automata, Languages and Programming*,

- S. Abramsky, C. Gavoiile, C. Kirchner, F. Meyer auf der Heide, and P. G. Spirakis, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 297–308.
- [164] D. Cruz, R. Fournier, F. Gremion, A. Jeannerot, K. Komagata, T. Tomic, J. Thiesbrummel, C. L. Chan, N. Macris, M.-A. Dupertuis, and C. Javerzac-Galy, “Efficient quantum algorithms for ghz and w states, and implementation on the ibm quantum computer,” *Advanced Quantum Technologies*, vol. 2, no. 5-6, p. 1900015, 2019. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.201900015>
- [165] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Going Beyond Bell’s Theorem*. Dordrecht: Springer Netherlands, 1989, pp. 69–72. [Online]. Available: https://doi.org/10.1007/978-94-017-0849-4_10
- [166] W. Dür, G. Vidal, and J. I. Cirac, “Three qubits can be entangled in two inequivalent ways,” *Phys. Rev. A*, vol. 62, p. 062314, Nov 2000. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.62.062314>
- [167] A. Cabello, “Bell’s theorem with and without inequalities for the three-qubit greenberger-horne-zeilinger and w states,” *Phys. Rev. A*, vol. 65, p. 032108, Feb 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.65.032108>
- [168] M. Bourennane, M. Eibl, S. Gaertner, N. Kiesel, C. Kurtsiefer, and H. Weinfurter, “Entanglement persistency of multiphoton entangled states,” *Phys. Rev. Lett.*, vol. 96, p. 100502, Mar 2006. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.96.100502>
- [169] N. Brunner and T. Vértesi, “Persistency of entanglement and nonlocality in multipartite quantum systems,” *Phys. Rev. A*, vol. 86, p. 042113, Oct 2012. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.86.042113>
- [170] F. Fröwis and W. Dür, “Stable macroscopic quantum superpositions,” *Phys. Rev. Lett.*, vol. 106, p. 110402, Mar 2011. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.106.110402>
- [171] S. Lloyd, J. H. Shapiro, F. N. C. Wong, P. Kumar, S. M. Shahriar, and H. P. Yuen, “Infrastructure for the quantum internet,” *SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 5, pp. 9–20, oct 2004. [Online]. Available: <https://doi.org/10.1145/1039111.1039118>
- [172] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, “Experimental quantum teleportation,” *Nature*, vol. 390, no. 6660, pp. 575–579, Dec 1997. [Online]. Available: <https://doi.org/10.1038/37539>
- [173] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, “Experimental realization of teleporting an unknown pure quantum

- state via dual classical and einstein-podolsky-rosen channels,” *Phys. Rev. Lett.*, vol. 80, pp. 1121–1125, Feb 1998. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.80.1121>
- [174] F. Vatan and C. Williams, “Optimal quantum circuits for general two-qubit gates,” *Phys. Rev. A*, vol. 69, p. 032315, Mar 2004. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.69.032315>
- [175] K. M. Svore and M. Troyer, “The quantum future of computation,” *Computer*, vol. 49, no. 9, pp. 21–30, 2016.
- [176] 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.
- [177] A. Gilchrist, N. K. Langford, and M. A. Nielsen, “Distance measures to compare real and ideal quantum processes,” *Phys. Rev. A*, vol. 71, p. 062310, Jun 2005. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.71.062310>
- [178] S. Barnett, *Quantum Information*, ser. Oxford Master Series in Physics. Oxford: Oxford University Press, 2009. [Online]. Available: <https://oxford.universitypressscholarship.com/10.1093/oso/9780198527626.001.0001/isbn-9780198527626>
- [179] R. Van Meter, T. Satoh, T. D. Ladd, W. J. Munro, and K. Nemoto, “Path selection for quantum repeater networks,” *Networking Science*, vol. 3, no. 1, pp. 82–95, Dec 2013. [Online]. Available: <https://doi.org/10.1007/s13119-013-0026-2>
- [180] R. Valivarthi, S. I. Davis, C. Peña, S. Xie, N. Lauk, L. Narváez, J. P. Allmaras, A. D. Beyer, Y. Gim, M. Hussein, G. Iskander, H. L. Kim, B. Korzh, A. Mueller, M. Rominsky, M. Shaw, D. Tang, E. E. Wollman, C. Simon, P. Spentzouris, D. Oblak, N. Sinclair, and M. Spiropulu, “Teleportation systems toward a quantum internet,” *PRX Quantum*, vol. 1, p. 020317, Dec 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PRXQuantum.1.020317>
- [181] H.-Q. Zhou and J. P. Barjaktarevič, “Fidelity and quantum phase transitions,” *Journal of Physics A: Mathematical and Theoretical*, vol. 41, no. 41, p. 412001, sep 2008. [Online]. Available: <https://doi.org/10.1088/1751-8113/41/41/412001>
- [182] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems*. Oxford University Press, 2002.
- [183] M. Schlosshauer, *Decoherence: and the Quantum-To-Classical Transition*, ser. The Frontiers Collection. Springer Berlin Heidelberg, 2007.

- [184] J. Fischer and D. Loss, “Dealing with decoherence,” *Science*, vol. 324, no. 5932, pp. 1277–1278, 2009. [Online]. Available: <https://www.science.org/doi/abs/10.1126/science.1169554>
- [185] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, “Experimental comparison of two quantum computing architectures,” *Proceedings of the National Academy of Sciences*, vol. 114, no. 13, pp. 3305–3310, 2017. [Online]. Available: <https://www.pnas.org/doi/abs/10.1073/pnas.1618020114>
- [186] W. Yang, W.-L. Ma, and R.-B. Liu, “Quantum many-body theory for electron spin decoherence in nanoscale nuclear spin baths,” *Reports on Progress in Physics*, vol. 80, no. 1, p. 016001, nov 2016. [Online]. Available: <https://doi.org/10.1088/0034-4885/80/1/016001>
- [187] J. A. Schreier, A. A. Houck, J. Koch, D. I. Schuster, B. R. Johnson, J. M. Chow, J. M. Gambetta, J. Majer, L. Frunzio, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, “Suppressing charge noise decoherence in superconducting charge qubits,” *Phys. Rev. B*, vol. 77, p. 180502, May 2008. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevB.77.180502>
- [188] V. V. Dobrovitski, A. E. Feiguin, D. D. Awschalom, and R. Hanson, “Decoherence dynamics of a single spin versus spin ensemble,” *Phys. Rev. B*, vol. 77, p. 245212, Jun 2008. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevB.77.245212>
- [189] J. Neuwirth, F. B. Basset, M. B. Rota, E. Rocca, C. Schimpf, K. D. Jöns, A. Rastelli, and R. Trotta, “Quantum dot technology for quantum repeaters: from entangled photon generation toward the integration with quantum memories,” *Materials for Quantum Technology*, vol. 1, no. 4, p. 043001, dec 2021. [Online]. Available: <https://doi.org/10.1088/2633-4356/ac3d14>
- [190] L. Gyongyosi and S. Imre, “A survey on quantum computing technology,” *Computer Science Review*, vol. 31, pp. 51–71, 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1574013718301709>
- [191] H. Häffner, C. Roos, and R. Blatt, “Quantum computing with trapped ions,” *Physics Reports*, vol. 469, no. 4, pp. 155–203, 2008. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0370157308003463>
- [192] R. Blatt and D. Wineland, “Entangled states of trapped atomic ions,” *Nature*, vol. 453, no. 7198, pp. 1008–1015, Jun 2008. [Online]. Available: <https://doi.org/10.1038/nature07125>
- [193] L. S. Brown and G. Gabrielse, “Geonium theory: Physics of a single electron or ion in a penning trap,” *Rev. Mod. Phys.*, vol. 58, pp. 233–311, Jan 1986. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.58.233>

- [194] T. Eronen *et al.*, *JYFLTRAP: a Penning trap for precision mass spectroscopy and isobaric purification*. Dordrecht: Springer Netherlands, 2014, pp. 61–81. [Online]. Available: https://doi.org/10.1007/978-94-007-5555-0_3
- [195] M. H. Devoret and R. J. Schoelkopf, “Superconducting circuits for quantum information: An outlook,” *Science*, vol. 339, no. 6124, pp. 1169–1174, 2013. [Online]. Available: <https://www.science.org/doi/abs/10.1126/science.1231930>
- [196] U. Banin, Y. Cao, D. Katz, and O. Millo, “Identification of atomic-like electronic states in indium arsenide nanocrystal quantum dots,” *Nature*, vol. 400, no. 6744, pp. 542–544, Aug 1999. [Online]. Available: <https://doi.org/10.1038/22979>
- [197] N. P. de Leon, K. M. Itoh, D. Kim, K. K. Mehta, T. E. Northup, H. Paik, B. S. Palmer, N. Samarth, S. Sangtawesin, and D. W. Steuerman, “Materials challenges and opportunities for quantum computing hardware,” *Science*, vol. 372, no. 6539, p. eabb2823, 2021. [Online]. Available: <https://www.science.org/doi/abs/10.1126/science.abb2823>
- [198] K. Heshami, D. G. England, P. C. Humphreys, P. J. Bustard, V. M. Acosta, J. Nunn, and B. J. Sussman, “Quantum memories: emerging applications and recent advances,” *Journal of Modern Optics*, vol. 63, no. 20, pp. 2005–2028, 2016, pMID: 27695198. [Online]. Available: <https://doi.org/10.1080/09500340.2016.1148212>
- [199] R. Bose, D. Sridharan, H. Kim, G. S. Solomon, and E. Waks, “Low-photon-number optical switching with a single quantum dot coupled to a photonic crystal cavity,” *Phys. Rev. Lett.*, vol. 108, p. 227402, May 2012. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.108.227402>
- [200] M. V. G. Dutt, L. Childress, L. Jiang, E. Togan, J. Maze, F. Jelezko, A. S. Zibrov, P. R. Hemmer, and M. D. Lukin, “Quantum register based on individual electronic and nuclear spin qubits in diamond,” *Science*, vol. 316, no. 5829, pp. 1312–1316, 2007. [Online]. Available: <https://www.science.org/doi/abs/10.1126/science.1139831>
- [201] A. J. Sigillito, A. M. Tyryshkin, T. Schenkel, A. A. Houck, and S. A. Lyon, “All-electric control of donor nuclear spin qubits in silicon,” *Nature Nanotechnology*, vol. 12, no. 10, pp. 958–962, Oct 2017. [Online]. Available: <https://doi.org/10.1038/nnano.2017.154>
- [202] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, “Topological quantum memory,” *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4452–4505, 2002. [Online]. Available: <https://doi.org/10.1063/1.1499754>
- [203] P. Bonderson, M. Freedman, and C. Nayak, “Measurement-only topological quantum computation,” *Phys. Rev. Lett.*, vol. 101, p. 010501, Jun 2008.

- [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.101.010501>
- [204] C. Nayak, S. H. Simon, A. Stern, M. Freedman, and S. Das Sarma, “Non-abelian anyons and topological quantum computation,” *Rev. Mod. Phys.*, vol. 80, pp. 1083–1159, Sep 2008. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.80.1083>
- [205] F. Bova, A. Goldfarb, and R. G. Melko, “Commercial applications of quantum computing,” *EPJ Quantum Technology*, vol. 8, no. 1, p. 2, Jan 2021. [Online]. Available: <https://doi.org/10.1140/epjqt/s40507-021-00091-1>
- [206] M. D. Lukin, “Colloquium: Trapping and manipulating photon states in atomic ensembles,” *Rev. Mod. Phys.*, vol. 75, pp. 457–472, Apr 2003. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.75.457>
- [207] W. Tittel, M. Afzelius, T. Chanelière, R. Cone, S. Kröll, S. Moiseev, and M. Sellars, “Photon-echo quantum memory in solid state systems,” *Laser & Photonics Reviews*, vol. 4, no. 2, pp. 244–267, 2010. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/lpor.200810056>
- [208] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, “Quantum repeaters based on atomic ensembles and linear optics,” *Rev. Mod. Phys.*, vol. 83, pp. 33–80, Mar 2011. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.83.33>
- [209] E. Saglamyurek, N. Sinclair, J. Jin, J. Slater, D. Oblak, F. Bussi eres, M. George, R. Ricken, W. Sohler, and W. Tittel, “Quantum memory for quantum repeaters,” in *Proceedings of the International Quantum Electronics Conference and Conference on Lasers and Electro-Optics Pacific Rim 2011*. Optica Publishing Group, 2011, p. I93. [Online]. Available: <https://opg.optica.org/abstract.cfm?URI=IQEC-2011-I93>
- [210] F. R. Lebrun-Gallagher, N. I. Johnson, M. Akhtar, S. Weidt, D. Breaud, S. J. Hile, A. Owens, F. Bonus, and W. K. Hensinger, “A scalable helium gas cooling system for trapped-ion applications,” *Quantum Science and Technology*, vol. 7, no. 2, p. 024002, mar 2022. [Online]. Available: <https://doi.org/10.1088/2058-9565/ac5d7d>
- [211] N. Elsayed, A. S. Maida, and M. Bayoumi, “A review of quantum computer energy efficiency,” in *2019 IEEE Green Technologies Conference (GreenTech)*, 2019, pp. 1–3.
- [212] M. J. Martin, C. Hughes, G. Moreno, E. B. Jones, D. Sickinger, S. Narumanchi, and R. Grout, “Energy use in quantum data centers: Scaling the impact of computer architecture, qubit performance, size, and thermal parameters,” *IEEE Transactions on Sustainable Computing*, pp. 1–12, 2022.

- [213] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, “Linear optical quantum computing with photonic qubits,” *Rev. Mod. Phys.*, vol. 79, pp. 135–174, Jan 2007. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.79.135>
- [214] B. A. Forouzan, *Introduction to Cryptography and Network Security*, 2008.
- [215] W. Stallings, *Cryptography and Network Security*, 09 2016.
- [216] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” *Commun. ACM*, vol. 21, no. 2, pp. 120–126, feb 1978. [Online]. Available: <https://doi.org/10.1145/359340.359342>
- [217] K. A. Balygin, V. I. Zaitsev, A. N. Klimov, A. I. Klimov, S. P. Kulik, and S. N. Molotkov, “Practical quantum cryptography,” *JETP Letters*, vol. 105, no. 9, pp. 606–612, May 2017. [Online]. Available: <https://doi.org/10.1134/S0021364017090077>
- [218] F. Cavaliere, E. Prati, L. Poti, I. Muhammad, and T. Catuogno, “Secure quantum communication technologies and systems: From labs to markets,” *Quantum Reports*, vol. 2, no. 1, pp. 80–106, 2020. [Online]. Available: <https://www.mdpi.com/2624-960X/2/1/7>
- [219] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.81.1301>
- [220] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, “Secure quantum key distribution with realistic devices,” *Rev. Mod. Phys.*, vol. 92, p. 025002, May 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.92.025002>
- [221] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” *npj Quantum Information*, vol. 2, no. 1, p. 16025, Nov 2016. [Online]. Available: <https://doi.org/10.1038/npjqi.2016.25>
- [222] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, “Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook,” *IEEE Communications Surveys Tutorials*, vol. 21, no. 1, pp. 881–919, 2019.
- [223] L. Gyongyosi and S. Imre, “Secret key rate adaption for multicarrier continuous-variable quantum key distribution,” *SN Computer Science*, vol. 1, no. 1, p. 33, Oct 2019. [Online]. Available: <https://doi.org/10.1007/s42979-019-0027-7>

- [224] L. Gyongyosi and S. Imre, “Adaptive multicarrier quadrature division modulation for long-distance continuous-variable quantum key distribution,” in *Quantum Information and Computation XII*, E. Donkor, A. R. Pirich, H. E. Brandt, M. R. Frey, S. J. L. Jr., and J. M. Myers, Eds., vol. 9123, International Society for Optics and Photonics. SPIE, May 2014, pp. 52 – 66.
- [225] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, “Advances in quantum cryptography,” *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, Dec 2020. [Online]. Available: <http://aop.osa.org/abstract.cfm?URI=aop-12-4-1012>
- [226] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, “Continuous variable quantum cryptography: Beating the 3 db loss limit,” *Phys. Rev. Lett.*, vol. 89, p. 167901, Sep 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.89.167901>
- [227] F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.*, vol. 88, p. 057902, Jan 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.88.057902>
- [228] L. Gyöngyösi, L. Bacsardi, and S. Imre, “A survey on quantum key distribution,” *Infocommunications Journal*, vol. 11, no. 2, pp. 14–21, 2019.
- [229] K. Inoue, E. Waks, and Y. Yamamoto, “Differential phase shift quantum key distribution,” *Phys. Rev. Lett.*, vol. 89, p. 037902, Jun 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.89.037902>
- [230] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, “Fast and simple one-way quantum key distribution,” *Applied Physics Letters*, vol. 87, no. 19, p. 194108, 2005. [Online]. Available: <https://doi.org/10.1063/1.2126792>
- [231] T. Sasaki, Y. Yamamoto, and M. Koashi, “Practical quantum key distribution protocol without monitoring signal disturbance,” *Nature*, vol. 509, no. 7501, pp. 475–478, May 2014. [Online]. Available: <https://doi.org/10.1038/nature13303>
- [232] K. Boström and T. Felbinger, “Deterministic secure direct communication using entanglement,” *Phys. Rev. Lett.*, vol. 89, p. 187902, Oct 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.89.187902>
- [233] M. Lucamarini and S. Mancini, “Secure deterministic communication without entanglement,” *Phys. Rev. Lett.*, vol. 94, p. 140501, Apr 2005. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.94.140501>
- [234] B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, Eds., *Handbook of Computer Networks and Cyber Security*. Springer International Publishing, 2020. [Online]. Available: <https://doi.org/10.1007%2F978-3-030-22277-2>

- [235] J. Javanainen, “Quantum optics: An introduction, mark fox , oxford u. press, new york, 2006. \$44.50 paper (400 pp.). isbn 978-0-19-856673-1,” *Physics Today*, vol. 60, no. 9, pp. 74–75, Sep 2007. [Online]. Available: <https://doi.org/10.1063/1.2784691>
- [236] M. H. Adnan, Z. Ahmad Zukarnain, and N. Z. Harun, “Quantum key distribution for 5g networks: A review, state of art and future directions,” *Future Internet*, vol. 14, no. 3, 2022. [Online]. Available: <https://www.mdpi.com/1999-5903/14/3/73>
- [237] A. V. Ryzhkov and D. S. Zrnic, *Polarization, Scattering, and Propagation of Electromagnetic Waves*. Cham: Springer International Publishing, 2019, pp. 1–18. [Online]. Available: https://doi.org/10.1007/978-3-030-05093-1_1
- [238] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar 2002. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.74.145>
- [239] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O’Brien, and M. G. Thompson, “Chip-based quantum key distribution,” *Nature Communications*, vol. 8, no. 1, p. 13984, Feb 2017. [Online]. Available: <https://doi.org/10.1038/ncomms13984>
- [240] A. Madaan and G. Raj, “Analysis of quantum cryptosystems using key distribution and attacking strategies over security protocols,” in *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2018, pp. 710–715.
- [241] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, theoretical Aspects of Quantum Cryptography celebrating 30 years of BB84. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0304397514004241>
- [242] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” *Nature Photonics*, vol. 8, no. 8, pp. 595–604, Aug 2014. [Online]. Available: <https://doi.org/10.1038/nphoton.2014.149>
- [243] A. K. Ekert, “Quantum cryptography based on bell’s theorem,” *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.67.661>
- [244] P. Vlamos, Ed., *GeNeDis 2016*. Springer International Publishing, 2017. [Online]. Available: <https://doi.org/10.1007%2F978-3-319-56246-9>
- [245] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” *Phys. Rev. Lett.*, vol. 23,

- pp. 880–884, Oct 1969. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.23.880>
- [246] D. E. Bruschi, T. C. Ralph, I. Fuentes, T. Jennewein, and M. Razavi, “Spacetime effects on satellite-based quantum communications,” *Phys. Rev. D*, vol. 90, p. 045041, Aug 2014. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevD.90.045041>
- [247] C. Gobby, Z. L. Yuan, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” *Applied Physics Letters*, vol. 84, no. 19, pp. 3762–3764, 2004. [Online]. Available: <https://doi.org/10.1063/1.1738173>
- [248] E. Y.-Z. Tan, C. C.-W. Lim, and R. Renner, “Advantage distillation for device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 124, p. 020502, Jan 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.124.020502>
- [249] G. Murta, F. Rozpędek, J. Ribeiro, D. Elkouss, and S. Wehner, “Key rates for quantum key distribution protocols with asymmetric noise,” *Phys. Rev. A*, vol. 101, p. 062321, Jun 2020. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.101.062321>
- [250] M. Niemiec, “Error correction in quantum cryptography based on artificial neural networks,” *Quantum Information Processing*, vol. 18, no. 6, p. 174, Apr 2019. [Online]. Available: <https://doi.org/10.1007/s11128-019-2296-4>
- [251] 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,” *Phys. Rev. A*, vol. 91, p. 052325, May 2015. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.91.052325>
- [252] C. Simon, “Towards a global quantum network,” *Nature Photonics*, vol. 11, no. 11, pp. 678–680, Nov 2017. [Online]. Available: <https://doi.org/10.1038/s41566-017-0032-0>
- [253] P. Grangier, J. A. Levenson, and J.-P. Poizat, “Quantum non-demolition measurements in optics,” *Nature*, vol. 396, no. 6711, pp. 537–542, Dec 1998. [Online]. Available: <https://doi.org/10.1038/25059>
- [254] I. B. Djordjevic, “On global quantum communication networking,” *Entropy*, vol. 22, no. 8, 2020. [Online]. Available: <https://www.mdpi.com/1099-4300/22/8/831>
- [255] Y. Wang *et al.*, “Routing and key resource allocation in sdn-based quantum satellite networks,” in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 2016–2021.
- [256] C. Wang, A. Rahman, R. Li, M. Aelmans, and K. Chakraborty, “Application Scenarios for the Quantum Internet,” *Internet Engineering*

- Task Force, Internet-Draft draft-irtf-qirg-quantum-internet-use-cases-12, May 2022, work in Progress. [Online]. Available: <https://datatracker.ietf.org/doc/html/draft-irtf-qirg-quantum-internet-use-cases-12>
- [257] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, and R. V. Meter, “Attacking the quantum internet,” *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1–17, 2021.
- [258] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2027–2051, 2016.
- [259] L. Mucchi, F. Nizzi, T. Pecorella, R. Fantacci, and F. Esposito, “Benefits of physical layer security to cryptography: Tradeoff and applications,” in *2019 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2019, pp. 1–3.
- [260] I. Khan, B. Heim, A. Neuzner, and C. Marquardt, “Satellite-based qkd,” *Opt. Photon. News*, vol. 29, no. 2, pp. 26–33, Feb 2018. [Online]. Available: <http://www.optica-opn.org/abstract.cfm?URI=opn-29-2-26>
- [261] X. Sun and I. B. Djordjevic, “Physical-layer security in orbital angular momentum multiplexing free-space optical communications,” *IEEE Photonics Journal*, vol. 8, no. 1, pp. 1–10, 2016.
- [262] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, “Experimental verification of the feasibility of a quantum channel between space and earth,” *New Journal of Physics*, vol. 10, no. 3, p. 033038, mar 2008. [Online]. Available: <https://doi.org/10.1088/1367-2630/10/3/033038>
- [263] P. Jianwei, “Progress of the quantum experiment science satellite (guess) micus project,” *Chinese Journal of Space Science*, vol. 38, no. 5, p. 604, 2018. [Online]. Available: http://www.cjss.ac.cn/CN/abstract/article_2596.shtml
- [264] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, “Satellite-relayed intercontinental quantum network,” *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan 2018. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.120.030501>
- [265] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, F.-Z. Li, X.-W. Chen, L.-H. Sun, J.-J. Jia, J.-C. Wu, X.-J. Jiang, J.-F. Wang, Y.-M. Huang, Q. Wang, Y.-L. Zhou, L. Deng, T. Xi, L. Ma, T. Hu, Q. Zhang, Y.-A. Chen, N.-L.

- Liu, X.-B. Wang, Z.-C. Zhu, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sep 2017. [Online]. Available: <https://doi.org/10.1038/nature23655>
- [266] J. Yin *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017. [Online]. Available: <https://science.sciencemag.org/content/356/6343/1140>
- [267] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Information*, vol. 7, no. 1, p. 3, Jan 2021. [Online]. Available: <https://doi.org/10.1038/s41534-020-00336-4>
- [268] H. Singh and A. Sachdev, "The quantum way of cloud computing," in *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)*, 2014, pp. 397–400.
- [269] P. J. Karalekas, N. A. Tezak, E. C. Peterson, C. A. Ryan, M. P. da Silva, and R. S. Smith, "A quantum-classical cloud platform optimized for variational hybrid algorithms," *Quantum Science and Technology*, vol. 5, no. 2, p. 024003, apr 2020. [Online]. Available: <https://doi.org/10.1088/2058-9565/ab7559>
- [270] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, Jun 2008. [Online]. Available: <https://doi.org/10.1038/nature07127>
- [271] F. Grodzinsky, M. J. Wolf, and K. Miller, "Quantum computing and cloud computing: humans trusting humans via machines," in *2011 IEEE International Symposium on Technology and Society (ISTAS)*, 2011, pp. 1–5.
- [272] G. Murali and R. S. Prasad, "Secured cloud authentication using quantum cryptography," in *2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS)*, 2017, pp. 3753–3756.
- [273] B. Kelley, J. J. Prevost, P. Rad, and A. Fatima, "Securing cloud containers using quantum networking channels," in *2016 IEEE International Conference on Smart Cloud (SmartCloud)*, 2016, pp. 103–111.
- [274] A. S. Cacciapuoti and M. Caleffi, "Toward the quantum internet: A directional-dependent noise model for quantum signal processing," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, pp. 7978–7982.
- [275] J. Lopez-Jimenez, J. L. Gutierrez-Rivas, E. Marin-Lopez, M. Rodriguez-Alvarez, and J. Diaz, "Time as a service based on white rabbit for finance applications," *IEEE Communications Magazine*, vol. 58, no. 4, pp. 60–66, 2020.

- [276] E. Pedrozo-Peñafiel, S. Colombo, C. Shu, A. F. Adiyatullin, Z. Li, E. Mendez, B. Braverman, A. Kawasaki, D. Akamatsu, Y. Xiao, and V. Vuletić, “Entanglement on an optical atomic-clock transition,” *Nature*, vol. 588, no. 7838, pp. 414–418, Dec 2020. [Online]. Available: <https://doi.org/10.1038/s41586-020-3006-1>
- [277] M. Kitagawa and M. Ueda, “Squeezed spin states,” *Phys. Rev. A*, vol. 47, pp. 5138–5143, Jun 1993. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.47.5138>
- [278] J. Jacobson, G. Björk, I. Chuang, and Y. Yamamoto, “Photonic de broglie waves,” *Phys. Rev. Lett.*, vol. 74, pp. 4835–4838, Jun 1995. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.74.4835>
- [279] D. Feng, “Review of quantum navigation,” *IOP Conference Series: Earth and Environmental Science*, vol. 237, p. 032027, mar 2019. [Online]. Available: <https://doi.org/10.1088/1755-1315/237/3/032027>
- [280] G. Armendáriz, J. Cravioto-Lagos, V. Velázquez, M. Grether, E. López-Moreno, and E. J. Galvez, “Teaching quantum mechanics with the hong-ou-mandel interferometer,” in *ETOP 2013 Proceedings*. Optical Society of America, 2013, p. EWB4. [Online]. Available: <http://www.osapublishing.org/abstract.cfm?URI=ETOP-2013-EWB4>
- [281] D. N. Makarov, “Fluctuations in the detection of the hom effect,” *Scientific Reports*, vol. 10, no. 1, p. 20124, Nov 2020. [Online]. Available: <https://doi.org/10.1038/s41598-020-77189-6>
- [282] H. Hong-Mei and X. Lu-Ping, “Design and analysis of the secure scheme for quantum positioning based on entangled photon pair,” in *2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 2015, pp. 849–852.
- [283] X. Guo, C. R. Breum, J. Borregaard, S. Izumi, M. V. Larsen, T. Gehring, M. Christandl, J. S. Neergaard-Nielsen, and U. L. Andersen, “Distributed quantum sensing in a continuous-variable entangled network,” *Nature Physics*, vol. 16, no. 3, pp. 281–284, Mar 2020. [Online]. Available: <https://doi.org/10.1038/s41567-019-0743-x>
- [284] S. Isaac, A. Conrad, T. Rezaei, D. Sanchez-Rosales, R. Cochran, A. Gutha, D. Gauthier, and P. Kwiat, “Drone-based quantum key distribution,” in *2021 Conference on Lasers and Electro-Optics (CLEO)*, 2021, pp. 1–2.
- [285] S. Barzanjeh, S. Pirandola, D. Vitali, and J. M. Fink, “Microwave quantum illumination using a digital receiver,” *Science Advances*, vol. 6, no. 19, p. eabb0451, 2020. [Online]. Available: <https://www.science.org/doi/abs/10.1126/sciadv.abb0451>

- [286] R. Jonsson and M. Ankel, "Quantum radar - what is it good for?" in *2021 IEEE Radar Conference (RadarConf21)*, 2021, pp. 1–6.
- [287] R. V. METER, J. TOUCH, and C. HORSMAN, "Recursive quantum repeater networks," *Progress in Informatics*, no. 8, p. 65, mar 2011. [Online]. Available: <https://doi.org/10.2201%2Fniipi.2011.8.8>
- [288] D. Castelvecchi, "The quantum internet has arrived (and it hasn't)," *Nature*, vol. 554, no. 7692, pp. 289–292, feb 2018. [Online]. Available: <https://doi.org/10.1038%2Fd41586-018-01835-3>
- [289] W. Kozłowski, A. Dahlberg, and S. Wehner, *Designing a Quantum Network Protocol*. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–16. [Online]. Available: <https://doi.org/10.1145/3386367.3431293>
- [290] Z.-S. Yuan, X.-H. Bao, C.-Y. Lu, J. Zhang, C.-Z. Peng, and J.-W. Pan, "Entangled photons and quantum communication," *Physics Reports*, vol. 497, no. 1, pp. 1–40, 2010. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0370157310001833>
- [291] R. Van Meter, T. D. Ladd, W. J. Munro, and K. Nemoto, "System design for a long-line quantum repeater," *IEEE/ACM Transactions on Networking*, vol. 17, no. 3, pp. 1002–1013, 2009.
- [292] R. V. Meter and J. Touch, "Designing quantum repeater networks," *IEEE Communications Magazine*, vol. 51, no. 8, pp. 64–71, 2013.
- [293] M. Uphoff, M. Brekenfeld, G. Rempe, and S. Ritter, "An integrated quantum repeater at telecom wavelength with single atoms in optical fiber cavities," *Applied Physics B*, vol. 122, no. 3, p. 46, Mar 2016. [Online]. Available: <https://doi.org/10.1007/s00340-015-6299-2>
- [294] G.-L. L. Husain Athar and K.-W. Ng, *Astroparticle Physics*. World Scientific Publishing Co. Pte. Ltd., 2002.
- [295] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Communications*, vol. 6, no. 1, p. 6787, Apr 2015. [Online]. Available: <https://doi.org/10.1038/ncomms7787>
- [296] J.-L. L. Gouët and S. Moiseev, "Quantum memory," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 45, no. 12, p. 120201, jun 2012. [Online]. Available: <https://doi.org/10.1088/0953-4075/45/12/120201>
- [297] M. Centenaro, C. E. Costa, F. Granelli, C. Sacchi, and L. Vangelista, "A survey on technologies, standards and open challenges in satellite iot," *IEEE Communications Surveys Tutorials*, vol. 23, no. 3, pp. 1693–1720, 2021.
- [298] E. M. Alessi, F. Deleflie, A. J. Rosengren, A. Rossi, G. B. Valsecchi, J. Daquin, and K. Merz, "A numerical investigation on the eccentricity

- growth of gnss disposal orbits,” *Celestial Mechanics and Dynamical Astronomy*, vol. 125, no. 1, pp. 71–90, May 2016. [Online]. Available: <https://doi.org/10.1007/s10569-016-9673-4>
- [299] S. H. Blumenthal, “Medium earth orbit ka band satellite communications system,” in *MILCOM 2013 - 2013 IEEE Military Communications Conference*, 2013, pp. 273–277.
- [300] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, “Satellite communications in the new space era: A survey and future challenges,” *IEEE Communications Surveys Tutorials*, vol. 23, no. 1, pp. 70–109, 2021.
- [301] D. K. Skoulidou, A. J. Rosengren, K. Tsiganis, and G. Voyatzis, “Medium earth orbit dynamical survey and its use in passive debris removal,” *Advances in Space Research*, vol. 63, no. 11, pp. 3646–3674, 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S027311771930119X>
- [302] J. C. McDowell, “The low earth orbit satellite population and impacts of the SpaceX starlink constellation,” vol. 892, no. 2, p. L36, apr 2020. [Online]. Available: <https://doi.org/10.3847/2041-8213/ab8016>
- [303] S. Cakaj, B. Kamo, A. Lala, and A. Rakipi, “The coverage analysis for low earth orbiting satellites at low elevation,” *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 6, 2014. [Online]. Available: <http://dx.doi.org/10.14569/IJACSA.2014.050602>
- [304] A. P. Trishchenko, L. Garand, and L. D. Trichtchenko, “Observing polar regions from space: Comparison between highly elliptical orbit and medium earth orbit constellations,” *Journal of Atmospheric and Oceanic Technology*, vol. 36, no. 8, pp. 1605–1621, 2019. [Online]. Available: <https://journals.ametsoc.org/view/journals/atot/36/8/jtech-d-19-0030.1.xml>
- [305] N. Crisp *et al.*, “The benefits of very low earth orbit for earth observation missions,” *Progress in Aerospace Sciences*, vol. 117, p. 100619, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0376042120300312>
- [306] J. Llop, P. Roberts, Z. Hao, L. Tomas, and V. Beauplet, “Very low earth orbit mission concepts for earth observation: Benefits and challenges.” in *Reinventing Space Conference*, Nov 2014, reinventing Space Conference ; Conference date: 18-11-2014 Through 20-11-2014.
- [307] V. R. Baraniello, G. Persechino, C. V. Angelino, and F. Tufano, “The application of high altitude pseudo-satellites for a rapid disaster response,” in *2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS*, 2021, pp. 8400–8403.

- [308] T. Tozer and D. Grace, "High-altitude platforms for wireless communications," *Electronics & communication engineering journal*, vol. 13, no. 3, pp. 127–137, 2001.
- [309] X. Cao, P. Yang, M. Alzenad, X. Xi, D. Wu, and H. Yanikomeroglu, "Airborne communication networks: A survey," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 9, pp. 1907–1926, 2018.
- [310] L. Reynaud and T. Rasheed, "Deployable aerial communication networks: Challenges for futuristic applications," in *Proceedings of the 9th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*, ser. PE-WASUN '12. New York, NY, USA: Association for Computing Machinery, 2012. [Online]. Available: <https://doi.org/10.1145/2387027.2387030>
- [311] J. Qiu, D. Grace, G. Ding, M. D. Zakaria, and Q. Wu, "Air-ground heterogeneous networks for 5g and beyond via integrating high and low altitude platforms," *IEEE Wireless Communications*, vol. 26, no. 6, pp. 140–148, 2019.
- [312] Z. Wang, R. Malaney, and J. Green, "Inter-satellite quantum key distribution at terahertz frequencies," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 2019, pp. 1–7.
- [313] Y. Chu, R. Donaldson, R. Kumar, and D. Grace, "Feasibility of quantum key distribution from high altitude platforms," vol. 6, no. 3, p. 035009, jun 2021. [Online]. Available: <https://doi.org/10.1088/2058-9565/abf9ae>
- [314] T. S. Humble, R. J. Sadlier, B. P. Williams, and R. C. Prout, "Software-defined quantum network switching," in *Disruptive Technologies in Information Sciences*, M. Blowers, R. D. Hall, and V. R. Dasari, Eds., vol. 10652, International Society for Optics and Photonics. SPIE, 2018, pp. 72 – 79. [Online]. Available: <https://doi.org/10.1117/12.2303800>
- [315] A. Orioux, M. A. M. Versteegh, K. D. Jöns, and S. Ducci, "Semiconductor devices for entangled photon pair generation: a review," *Reports on Progress in Physics*, vol. 80, no. 7, p. 076001, may 2017. [Online]. Available: <https://doi.org/10.1088/1361-6633/aa6955>
- [316] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3808–3833, 2020.
- [317] O. Amer, W. O. Krawec, and B. Wang, "Efficient routing for quantum key distribution networks," in *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2020, pp. 137–147.

- [318] M. Cozzini, R. Ionicioiu, and P. Zanardi, “Quantum fidelity and quantum phase transitions in matrix product states,” *Phys. Rev. B*, vol. 76, p. 104420, Sep 2007. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevB.76.104420>
- [319] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, “Purification of noisy entanglement and faithful teleportation via noisy channels,” *Phys. Rev. Lett.*, vol. 76, pp. 722–725, Jan 1996. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.76.722>
- [320] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, “Quantum repeaters based on entanglement purification,” *Phys. Rev. A*, vol. 59, pp. 169–181, Jan 1999. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.59.169>
- [321] J.-W. Pan, C. Simon, Č. Brukner, and A. Zeilinger, “Entanglement purification for quantum communication,” *Nature*, vol. 410, no. 6832, pp. 1067–1070, Apr 2001. [Online]. Available: <https://doi.org/10.1038/35074041>
- [322] M. Caleffi and A. S. Cacciapuoti, “Quantum switch for the quantum internet: Noiseless communications through noisy channels,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 3, pp. 575–588, 2020.
- [323] C. Mukhopadhyay and A. K. Pati, “Superposition of causal order enables quantum advantage in teleportation under very noisy channels,” *Journal of Physics Communications*, vol. 4, no. 10, p. 105003, oct 2020. [Online]. Available: <https://doi.org/10.1088/2399-6528/abb477>
- [324] H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin, “Long-distance entanglement swapping with photons from separated sources,” *Phys. Rev. A*, vol. 71, p. 050302, May 2005. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.71.050302>
- [325] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ““event-ready-detectors” bell experiment via entanglement swapping,” *Phys. Rev. Lett.*, vol. 71, pp. 4287–4290, Dec 1993. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.71.4287>
- [326] A. M. Goebel, C. Wagenknecht, Q. Zhang, Y.-A. Chen, K. Chen, J. Schmiedmayer, and J.-W. Pan, “Multistage entanglement swapping,” *Phys. Rev. Lett.*, vol. 101, p. 080403, Aug 2008. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.101.080403>
- [327] D. E. Bruschi, T. M. Barlow, M. Razavi, and A. Beige, “Repeat-until-success quantum repeaters,” *Phys. Rev. A*, vol. 90, p. 032306, Sep 2014. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.90.032306>
- [328] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, “Routing entanglement in the quantum internet,” *npj*

- Quantum Information*, vol. 5, no. 1, p. 25, Mar 2019. [Online]. Available: <https://doi.org/10.1038/s41534-019-0139-x>
- [329] A. Manzalini, “Quantum communications in future networks and services,” *Quantum Reports*, vol. 2, no. 1, pp. 221–232, 2020. [Online]. Available: <https://www.mdpi.com/2624-960X/2/1/14>
- [330] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, and T. Länger, “Security of trusted repeater quantum key distribution networks,” *Journal of Computer Security*, vol. 18, no. 1, January 2010.
- [331] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger, “Long-distance quantum communication with entangled photons using satellites,” *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 9, no. 6, pp. 1541–1551, 2003.
- [332] H. Kaushal, V. K. Jain, and S. Kar, *Overview of Wireless Optical Communication Systems*. New Delhi: Springer India, 2017, pp. 1–39. [Online]. Available: https://doi.org/10.1007/978-81-322-3691-7_1
- [333] S. Bloom, E. Korevaar, J. Schuster, and H. Willebrand, “Understanding the performance of free-space optics,” *J. Opt. Netw.*, vol. 2, no. 6, pp. 178–200, Jun 2003. [Online]. Available: <http://www.osapublishing.org/jon/abstract.cfm?URI=jon-2-6-178>
- [334] P. M. Goorjian, “Free-space optical communication for spacecraft and satellites, including cubesats in low earth orbit (leo),” in *OSA Advanced Photonics Congress (AP) 2019 (IPR, Networks, NOMA, SPPCom, PVLED)*. Optical Society of America, 2019, p. NeM2D.4. [Online]. Available: <http://www.osapublishing.org/abstract.cfm?URI=Networks-2019-NeM2D.4>
- [335] B. S. Robinson, D. M. Boroson, D. A. Burianek, and D. V. Murphy, “The lunar laser communications demonstration,” in *2011 International Conference on Space Optical Systems and Applications (ICSOS)*, 2011, pp. 54–57.
- [336] B. L. Edwards, “NASA’s current activities in free space optical communications,” in *International Conference on Space Optics*, vol. 10563, International Society for Optics and Photonics. SPIE, 2017, pp. 255 – 263. [Online]. Available: <https://doi.org/10.1117/12.2304175>
- [337] Peter M. Goorjian, “Free-space optical communication for CubeSats in low lunar orbit: LLO,” in *Free-Space Laser Communications XXXII*, H. Hemmati and D. M. Boroson, Eds., vol. 11272, International Society for Optics and Photonics. SPIE, 2020, pp. 254 – 262. [Online]. Available: <https://doi.org/10.1117/12.2542134>
- [338] R. W. Kingsbury, D. O. Caplan, and K. L. Cahoy, “Compact optical transmitters for CubeSat free-space optical communications,” in

- Free-Space Laser Communication and Atmospheric Propagation XXVII*, H. Hemmati and D. M. Boroson, Eds., vol. 9354, International Society for Optics and Photonics. SPIE, 2015, pp. 231 – 237. [Online]. Available: <https://doi.org/10.1117/12.2080122>
- [339] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, “Quantum key distribution over fso: Current development and future perspectives,” in *2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama)*, 2018, pp. 1672–1679.
- [340] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Soriano, F. Vedovato, G. Vallone, and P. Villaresi, “Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics,” *npj Quantum Information*, vol. 7, no. 1, p. 93, Jun 2021. [Online]. Available: <https://doi.org/10.1038/s41534-021-00421-2>
- [341] S. P. Neumann, S. K. Joshi, M. Fink, T. Scheidl, R. Blach, C. Scharlemann, S. Abouagaga, D. Bamberg, E. Kerstel, M. Barthelemy, and R. Ursin, “Q3sat: quantum communications uplink to a 3u cubesat—feasibility & design,” *EPJ Quantum Technology*, vol. 5, no. 1, p. 4, Apr 2018. [Online]. Available: <https://doi.org/10.1140/epjqt/s40507-018-0068-1>
- [342] A. Kak, E. Guven, U. E. Ergin, and I. F. Akyildiz, “Performance evaluation of sdn-based internet of space things,” in *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–6.
- [343] W. Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Pearson Education, 2015.
- [344] J. C. Correa Chica, J. C. Imbachi, and J. F. Botero Vega, “Security in sdn: A comprehensive survey,” *Journal of Network and Computer Applications*, vol. 159, p. 102595, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1084804520300692>
- [345] R. Silva, D. Santos, F. Meneses, D. Corujo, and R. L. Aguiar, “A hybrid sdn solution for mobile networks,” *Computer Networks*, vol. 190, p. 107958, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1389128621000931>
- [346] D. Kreutz, F. M. V. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmoly, and S. Uhlig, “Software-defined networking: A comprehensive survey,” *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015.
- [347] K. Benzekki, A. El Fergougui, and A. Elbelrhiti Elalaoui, “Software-defined networking (sdn): a survey,” *Security and Communication*

- Networks*, vol. 9, no. 18, pp. 5803–5833, 2016. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1737>
- [348] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, “Openflow: Enabling innovation in campus networks,” *SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, mar 2008. [Online]. Available: <https://doi.org/10.1145/1355734.1355746>
- [349] T. Koponen, M. Casado, N. Gude, J. Stribling, L. Poutievski, M. Zhu, R. Ramanathan, Y. Iwata, H. Inoue, T. Hama, and S. Shenker, “Onix: A distributed control platform for large-scale production networks,” in *9th USENIX Symposium on Operating Systems Design and Implementation (OSDI 10)*. Vancouver, BC: USENIX Association, oct 2010. [Online]. Available: <https://www.usenix.org/conference/osdi10/onix-distributed-control-platform-large-scale-production-networks>
- [350] B. Heller, R. Sherwood, and N. McKeown, “The controller placement problem,” in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, ser. HotSDN '12. New York, NY, USA: Association for Computing Machinery, 2012, pp. 7–12. [Online]. Available: <https://doi.org/10.1145/2342441.2342444>
- [351] D. Tuncer, M. Charalambides, S. Clayman, and G. Pavlou, “On the placement of management and control functionality in software defined networks,” in *2015 11th International Conference on Network and Service Management (CNSM)*, 2015, pp. 360–365.
- [352] S. Nazari, P. Du, M. Gerla, C. Hoffmann, J. H. Kim, and A. Capone, “Software defined naval network for satellite communications (sdn-sat),” in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, 2016, pp. 360–366.
- [353] A. Lara, A. Kolasani, and B. Ramamurthy, “Network innovation using openflow: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 493–512, 2014.
- [354] S. Jamali, A. Badirzadeh, and M. S. Siapoush, “On the use of the genetic programming for balanced load distribution in software-defined networks,” *Digital Communications and Networks*, vol. 5, no. 4, pp. 288–296, 2019. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S235286481830261X>
- [355] R. Ferrus, O. Sallent, T. Ahmed, and R. Fedrizzi, “Towards sdn/nfv-enabled satellite ground segment systems: End-to-end traffic engineering use case,” in *2017 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2017, pp. 888–893.

- [356] R. Ferrús, H. Koumaras, O. Sallent, G. Agapiou, T. Rasheed, M.-A. Kourtis, C. Boustie, P. Gélard, and T. Ahmed, “Sdn/nfv-enabled satellite communications networks: Opportunities, scenarios and challenges,” *Physical Communication*, vol. 18, pp. 95–112, 2016, special Issue on Radio Access Network Architectures and Resource Management for 5G. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1874490715000543>
- [357] D. Vallado and P. Cefola, “Two-line element sets - practice and use,” *Proceedings of the International Astronautical Congress, IAC*, vol. 7, pp. 5812–5825, 01 2012.
- [358] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpundek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner, “A link layer protocol for quantum networks,” in *Proceedings of the ACM Special Interest Group on Data Communication*, ser. SIGCOMM '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 159–173. [Online]. Available: <https://doi.org/10.1145/3341302.3342070>
- [359] B. Rhodes, “Skyfield: High precision research-grade positions for planets and earth satellites generator,” Astrophysics Source Code Library, record ascl:1907.024, p. ascl:1907.024, jul 2019.
- [360] F. R. Hoots and R. L. Roehrich, “Models for propagation of NORAD element sets,” Tech. Rep., dec 1980. [Online]. Available: <https://doi.org/10.21236%2Fada093554>
- [361] D. Vallado, P. Crawford, R. Hujsak, and T. Kelso, “Revisiting spacetrack report #3,” in *AIAA/AAS Astrodynamics Specialist Conference and Exhibit*. American Institute of Aeronautics and Astronautics, jun 2006. [Online]. Available: <https://doi.org/10.2514%2F6.2006-6753>
- [362] C. Hilton and J. Kuhlman, “Mathematical models for the space defense center,” *Philco-Ford Publication No. U-3871*, vol. 17, p. 28, 1966.
- [363] M. H. Lane and F. R. Hoots, “General perturbations theories derived from the 1965 lane drag theory,” Tech. Rep., dec 1979. [Online]. Available: <https://doi.org/10.21236%2Fada081264>
- [364] K. CRANFORD, *An improved analytical drag theory for the artificial satellite problem*. [Online]. Available: <https://arc.aiaa.org/doi/abs/10.2514/6.1969-925>
- [365] D. Brouwer, “Solution of the problem of artificial satellite theory without drag,” *The Astronomical Journal*, vol. 64, p. 378, nov 1959. [Online]. Available: <https://doi.org/10.1086%2F107958>

- [366] R. S. Hujsak, "A restricted four body solution for resonating satellites without drag," Tech. Rep., nov 1979. [Online]. Available: <https://doi.org/10.21236%2Fada081263>
- [367] F. Hoots, "A short efficient analytical satellite theory," *Journal of Guidance, Control, and Dynamics*, vol. 5, no. 2, pp. 194–199, 1982. [Online]. Available: <https://doi.org/10.2514/3.56157>
- [368] M. Soffel, S. A. Klioner, G. Petit, P. Wolf, S. M. Kopeikin, P. Bretagnon, V. A. Brumberg, N. Capitaine, T. Damour, T. Fukushima, B. Guinot, T.-Y. Huang, L. Lindgren, C. Ma, K. Nordtvedt, J. C. Ries, P. K. Seidelmann, D. Vokrouhlick, C. M. Will, and C. Xu, "The IAU 2000 resolutions for astrometry, celestial mechanics, and metrology in the relativistic framework: Explanatory supplement," *The Astronomical Journal*, vol. 126, no. 6, pp. 2687–2706, dec 2003. [Online]. Available: <https://doi.org/10.1086/378162>
- [369] G. J. Dittberner *et al.*, "Medium earth orbit (meo) as a venue for future noaa satellite systems."
- [370] P. Bolli, A. Orlati, L. Stringhetti, A. Orfei, S. Righini, R. Ambrosini, M. Bartolini, C. Bortolotti, F. Buffa, M. Buttu, A. Cattani, N. D'Amico, G. Deiana, A. Fara, F. Fiocchi, F. Gaudiomonte, A. Maccaferri, S. Mariotti, P. Marongiu, A. Melis, C. Migoni, M. Morsiani, M. Nanni, F. Nasyr, A. Pellizzoni, T. Pisanu, M. Poloni, S. Poppi, I. Porceddu, I. Prandoni, J. Roda, M. Roma, A. Scalambra, G. Serra, A. Trois, G. Valente, G. P. Vargiu, and G. Zacchiroli, "Sardinia radio telescope: General description, technical commissioning and first light," *Journal of Astronomical Instrumentation*, vol. 04, no. 03n04, p. 1550008, 2015. [Online]. Available: <https://doi.org/10.1142/S2251171715500087>
- [371] I.-A. S. D. C. Committee *et al.*, "Iadc space debris mitigation guidelines," URL: http://www.iadc-online.org/Documents/Docu/I-ADC_Mitigation_Guidelines_Rev1_Sep07.pdf [cited: 20 July 2011], 2007.
- [372] S. J. Campanella and T. J. Kirkwood, "Faster than fiber: advantages and challenges of leo communications satellite systems," in *AIP conference proceedings*, vol. 325, no. 1. American Institute of Physics, 1995, pp. 39–43.
- [373] G. K. Nigel May, "Design approach and challenges for the iridium next constellation command and control system," in *SpaceOps Conference, Marseille, France*, vol. 28, 2018.
- [374] U. C. Guard, "Navstar gps user equipment introduction (public release version)," *Papers Published in Journal of Navigation*, vol. 1, 1996.
- [375] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking,"

- Nature Photonics*, vol. 4, no. 11, pp. 792–796, Nov 2010. [Online]. Available: <https://doi.org/10.1038/nphoton.2010.213>
- [376] A. Bassi, M. Paternostro *et al.*, “Quantum technologies in space,” The Quantum Spaceship, Tech. Rep., 5 August 2019. [Online]. Available: https://www.cosmos.esa.int/documents/1866264/3219248/BassiA_QT_In_Space_-_White_Paper.pdf/6f50e4bc-9fac-8f72-0ec0-f8e030adc499?t=1565184619333
- [377] M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden, “Entangling independent photons by time measurement,” *Nature Physics*, vol. 3, no. 10, pp. 692–695, Oct 2007. [Online]. Available: <https://doi.org/10.1038/nphys700>
- [378] S. Bose, V. Vedral, and P. L. Knight, “Multiparticle generalization of entanglement swapping,” *Phys. Rev. A*, vol. 57, pp. 822–829, Feb 1998. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.57.822>
- [379] S. E. Nathan Blaunstein, E. Krouk, and M. Sergeev, *Fiber optic and atmospheric optical communication*. John Wiley and Sons, Inc., 2020.
- [380] “Relative permittivity,” https://www.engineeringtoolbox.com/relative-permittivity-d_1660.html, online; accessed 19 Feb 2020.
- [381] “Table of electrical resistivity and conductivity,” [thoughtco.com/table-of-electrical-resistivity-conductivity-608499](https://www.thoughtco.com/table-of-electrical-resistivity-conductivity-608499), online; accessed 1 Feb 2020.
- [382] K. C. Tan and H. Jeong, “Entanglement as the symmetric portion of correlated coherence,” *Phys. Rev. Lett.*, vol. 121, p. 220401, Nov 2018. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.121.220401>
- [383] M. Steger, K. Saeedi, M. L. W. Thewalt, J. J. L. Morton, H. Riemann, N. V. Abrosimov, P. Becker, and H.-J. Pohl, “Quantum information storage for over 180 s using donor spins in a ²⁸Si “semiconductor vacuum,”” *Science*, vol. 336, no. 6086, pp. 1280–1283, 2012. [Online]. Available: <https://science.sciencemag.org/content/336/6086/1280>
- [384] K. Saeedi, S. Simmons, J. Z. Salvail, P. Dluhy, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, J. J. L. Morton, and M. L. W. Thewalt, “Room-temperature quantum bit storage exceeding 39 minutes using ionized donors in silicon-28,” *Science*, vol. 342, no. 6160, pp. 830–833, 2013. [Online]. Available: <https://www.science.org/doi/abs/10.1126/science.1239584>
- [385] W. P. Grice, “Arbitrarily complete bell-state measurement using only linear optical elements,” *Phys. Rev. A*, vol. 84, p. 042331, Oct 2011. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.84.042331>

- [386] F. Benatti, A. M. Liguori, and G. Paluzzano, “Entanglement and entropy rates in open quantum systems,” *Journal of Physics A: Mathematical and Theoretical*, vol. 43, no. 4, p. 045304, jan 2010. [Online]. Available: <https://doi.org/10.1088/1751-8113/43/4/045304>
- [387] “Introduction to controller-based networking,” <https://www.ciscopress.com/articles/article.asp?p=2995354&seqNum=2>, online; accessed 4 May 2020.
- [388] C. V., B. S., H. A., T. L. ad Durst R., S. K., F. K., and H. Weiss, “Delay-tolerant networking architecture,” Internet Requests for Comments, RFC Editor, RFC 4838, April 2007. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc4838.txt>
- [389] L. A., D. A., D. E., and S. Grasic, “Probabilistic routing protocol for intermittently connected networks,” Internet Requests for Comments, RFC Editor, RFC 6693, August 2012. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc6693.txt>
- [390] E. Sigel, B. Denby, and S. Le Hégarat-Masclé, “Application of ant colony optimization to adaptive routing in aleo telecommunications satellite network,” *Annales Des Télécommunications*, vol. 57, no. 5, pp. 520–539, May 2002. [Online]. Available: <https://doi.org/10.1007/BF02995174>
- [391] P. Cong-Vinh, *Nature-Inspired Networking: Theory and Applications*. CRC Press, 2018, pp. 31–48.
- [392] H. Petter and J. Saramäki, *Temporal Networks*. Springer, Berlin, Heidelberg, 2013. [Online]. Available: <https://doi.org/10.1007/978-3-642-36461-7>
- [393] M. Dorigo, V. Maniezzo, and A. Colorni, “Ant system: optimization by a colony of cooperating agents,” *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 26, no. 1, pp. 29–41, 1996.
- [394] S. Kilic and O. Ozkan, “Ant colony optimization approach for satellite broadcast scheduling problem,” in *2017 8th International Conference on Recent Advances in Space Technologies (RAST)*, 2017, pp. 273–277.
- [395] C. Iacopino, P. Palmer, N. Policella, A. Donati, and A. Brewer, “How ants can manage your satellites,” *Acta Futura*, vol. 9, pp. 57–70, 2014.
- [396] J. Cao and M. Stefanovic, “Cross entropy accelerated ant routing in satellite networks,” in *Proceedings of the 2010 American Control Conference*, 2010, pp. 5080–5087.
- [397] M. L. Fredman and R. E. Tarjan, “Fibonacci heaps and their uses in improved network optimization algorithms,” *J. ACM*, vol. 34, no. 3, pp. 596–615, jul 1987. [Online]. Available: <https://doi.org/10.1145/28869.28874>
- [398] J. Sneyers, T. Schrijvers, and B. Demoen, “Dijkstra’s algorithm with fibonacci heaps: An executable description in chr,” *CW Reports*, pp. 13–13, 2005.

- [399] V. Kotronis, X. Dimitropoulos, and B. Ager, "Outsourcing the routing control logic: Better internet routing based on sdn principles," in *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*, ser. HotNets-XI. New York, NY, USA: Association for Computing Machinery, 2012, pp. 55–60. [Online]. Available: <https://doi.org/10.1145/2390231.2390241>
- [400] "Norad two-line element sets current data," <https://celestrak.com/NORAD/elements/>, online; accessed 03 July 2021.
- [401] H. Ollivier, I. Maillette de Buy Wenniger, S. Thomas, S. C. Wein, A. Harouri, G. Coppola, P. Hilaire, C. Millet, A. Lemaître, I. Sagnes *et al.*, "Reproducibility of high-performance quantum dot single-photon sources," *ACS Photonics*, vol. 7, no. 4, pp. 1050–1059, 2020.
- [402] S. Ramelow, A. Mech, M. Giustina, S. Gröblacher, W. Wieczorek, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam *et al.*, "Highly efficient heralding of entangled single photons," *Optics express*, vol. 21, no. 6, pp. 6707–6717, 2013.
- [403] Z.-Q. Zhou, W.-B. Lin, M. Yang, C.-F. Li, and G.-C. Guo, "Realization of reliable solid-state quantum memory for photonic polarization qubit," *Physical review letters*, vol. 108, no. 19, p. 190505, 2012.
- [404] Z. Gao, Q. Guo, and Z. Na, "Novel optimized routing algorithm for leo satellite ip networks," *Journal of Systems Engineering and Electronics*, vol. 22, no. 6, pp. 917–925, 2011.
- [405] L. Liu, X. Chen, Y. Wang, Z. Liu, and X. Qi, "Research on multi-layer satellite network qos routing strategy based on logical clustering," in *Space Information Networks*, Q. Yu, Ed. Singapore: Springer Singapore, 2019, pp. 71–76.
- [406] F. Long, *Satellite network robust QoS-aware routing*. Springer, 2014, pp. 1–131.
- [407] C. Chen, E. Ekici, and I. F. Akyildiz, "Satellite grouping and routing protocol for leo/meo satellite ip networks," in *Proceedings of the 5th ACM International Workshop on Wireless Mobile Multimedia*, ser. WOWMOM '02. New York, NY, USA: Association for Computing Machinery, 2002, pp. 109–116. [Online]. Available: <https://doi.org/10.1145/570790.570809>
- [408] F. Davoli, C. Kourogorgas, M. Marchese, A. Panagopoulos, and F. Patrone, "Small satellites and cubesats: Survey of structures, architectures, and protocols," *International Journal of Satellite Communications and Networking*, vol. 37, no. 4, pp. 343–359, 2019. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/sat.1277>
- [409] S. P. Neumann, S. K. Joshi, T. Scheidl, R. Blach, C. Scharlemann, S. Abouagaga, D. Bambery, E. Kerstel, M. Barthelemy, R. Ursin, and

- M. Fink, "Feasibility of a 3U CubeSat for uplink quantum communications," in *International Conference on Space Optics - ICSSO 2018*, Z. Sodnik, N. Karafolas, and B. Cugny, Eds., vol. 11180, International Society for Optics and Photonics. SPIE, 2019, p. 111801V. [Online]. Available: <https://doi.org/10.1117/12.2535986>
- [410] A. Mehrparvar, D. Pignatelli, J. Carnahan, R. Munakat, W. Lan, A. Toorian, A. Hutputanasin, and S. Lee, "Cubesat design specification rev. 13," *The CubeSat Program, Cal Poly San Luis Obispo, US*, vol. 1, no. 2, 2014.
- [411] National Academies of Sciences, Engineering, and Medicine, *Achieving Science with CubeSats: Thinking Inside the Box*. Washington, DC: The National Academies Press, 2016. [Online]. Available: <https://nap.nationalacademies.org/catalog/23503/achieving-science-with-cubesat-s-thinking-inside-the-box>
- [412] "Celestrak," <https://celestrak.org/>, online; accessed 25 October 2022.
- [413] Y. Li, "Methods of generating entangled photon pairs," *Journal of Physics: Conference Series*, vol. 1634, p. 012172, Sep 2020. [Online]. Available: <https://doi.org/10.1088/1742-6596/1634/1/012172>
- [414] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Phys. Rev. A*, vol. 52, pp. R2493–R2496, Oct 1995. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.52.R2493>
- [415] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, no. 7415, pp. 269–273, Sep 2012. [Online]. Available: <https://doi.org/10.1038/nature11472>
- [416] W. Paul, "Electromagnetic traps for charged and neutral particles," *Rev. Mod. Phys.*, vol. 62, pp. 531–540, Jul 1990. [Online]. Available: <https://link.aps.org/doi/10.1103/RevModPhys.62.531>
- [417] M. H. Kadhim, J. A. K. Hasan, and R. S. Alhumaima, "Performance analysis of quantum repeaters based hybrid communications networks," *IOP Conference Series: Materials Science and Engineering*, vol. 1076, no. 1, p. 012054, feb 2021. [Online]. Available: <https://dx.doi.org/10.1088/1757-899X/1076/1/012054>
- [418] L. Gyongyosi and S. Imre, "Resource optimization for the quantum Internet," in *Quantum Computing, Communication, and Simulation II*, P. R. Hemmer and A. L. Migdall, Eds., vol. 12015, International Society for Optics and Photonics. SPIE, 2022, p. 120150F. [Online]. Available: <https://doi.org/10.1117/12.2607957>

- [419] Q. Gong, W. Kang, N. S. Bedrossian, F. Fahroo, P. Sekhavat, and K. Bollino, “Pseudospectral optimal control for military and industrial applications,” in *2007 46th IEEE Conference on Decision and Control*, 2007, pp. 4128–4142.
- [420] L. A. Zhukas, P. Svihra, A. Nomerotski, and B. B. Blinov, “High-fidelity simultaneous detection of a trapped-ion qubit register,” *Phys. Rev. A*, vol. 103, p. 062614, Jun 2021. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.103.062614>
- [421] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. Torres-Knoop, D. Elkouss, and S. Wehner, “Netsquid, a network simulator for quantum information using discrete events,” *Communications Physics*, vol. 4, no. 1, p. 164, Jul 2021. [Online]. Available: <https://doi.org/10.1038/s42005-021-00647-8>
- [422] A. Dahlberg and S. Wehner, “SimulaQron—a simulator for developing quantum internet software,” *Quantum Science and Technology*, vol. 4, no. 1, p. 015001, sep 2018. [Online]. Available: <https://doi.org/10.1088/2058-9565/aad56e>
- [423] S. Diadamo, J. Nötzel, B. Zanger, and M. M. Beşe, “Qunetsim: A software framework for quantum networks,” *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1–12, 2021.
- [424] B. Bartlett, “A distributed simulation framework for quantum networks and channels,” 2018. [Online]. Available: <https://arxiv.org/abs/1808.07047>
- [425] T. Matsuo, “Simulation of a dynamic, ruleset-based quantum network,” 2019. [Online]. Available: <https://arxiv.org/abs/1908.10758>
- [426] R. Satoh, M. Hajdušek, N. Benchasattabuse, S. Nagayama, K. Teramoto, T. Matsuo, S. A. Metwalli, T. Satoh, S. Suzuki, and R. Van Meter, “Quisp: a quantum internet simulation package,” 2021. [Online]. Available: <https://arxiv.org/abs/2112.07093>
- [427] L. O. Mailloux, J. D. Morris, M. R. Grimaila, D. D. Hodson, D. R. Jacques, J. M. Colombi, C. V. Mclaughlin, and J. A. Holes, “A modeling framework for studying quantum key distribution system implementation nonidealities,” *IEEE Access*, vol. 3, pp. 110–130, 2015.
- [428] X. Wu, A. Kolar, J. Chung, D. Jin, T. Zhong, R. Kettimuthu, and M. Suchara, “SeQUeNCe: a customizable discrete-event simulator of quantum networks,” *Quantum Science and Technology*, vol. 6, no. 4, p. 045027, sep 2021. [Online]. Available: <https://doi.org/10.1088/2058-9565/ac22f6>

- [429] S. Langenfeld, P. Thomas, O. Morin, and G. Rempe, “Quantum repeater node demonstrating unconditionally secure key distribution,” *Phys. Rev. Lett.*, vol. 126, p. 230506, Jun 2021. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevLett.126.230506>
- [430] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science*, vol. 362, no. 6412, p. eaam9288, 2018. [Online]. Available: <https://www.science.org/doi/abs/10.1126/science.aam9288>
- [431] E. Torenbeek and H. Wittenberg, *Flight Physics*. Springer Netherlands, 2009. [Online]. Available: <https://doi.org/10.1007%2F978-1-4020-8664-9>
- [432] A. Garcia, E. Mattison, and K. Ghose, “High-speed vision-based autonomous indoor navigation of a quadcopter,” in *2015 International Conference on Unmanned Aircraft Systems (ICUAS)*, 2015, pp. 338–347.
- [433] P. Foehn, D. Brescianini, E. Kaufmann, T. Cieslewski, M. Gehrig, M. Muglikar, and D. Scaramuzza, “Alphapilot: autonomous drone racing,” *Autonomous Robots*, vol. 46, no. 1, pp. 307–320, Jan 2022. [Online]. Available: <https://doi.org/10.1007/s10514-021-10011-y>
- [434] M. Gowda, J. Manweiler, A. Dhekne, R. R. Choudhury, and J. D. Weisz, “Tracking drone orientation with multiple gps receivers,” in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom ’16. New York, NY, USA: Association for Computing Machinery, 2016, pp. 280–293. [Online]. Available: <https://doi.org/10.1145/2973750.2973768>
- [435] K. Fukuda, S. Kawai, and H. Nobuhara, “Attitude estimation by kalman filter based on the integration of imu and multiple gpss and its application to connected drones,” in *2020 59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 2020, pp. 1286–1292.
- [436] A. Trichili, M. A. Cox, B. S. Ooi, and M.-S. Alouini, “Roadmap to free space optics,” *J. Opt. Soc. Am. B*, vol. 37, no. 11, pp. A184–A201, Nov 2020. [Online]. Available: <http://opg.optica.org/josab/abstract.cfm?URI=josab-37-11-A184>
- [437] S. S. Muhammad, T. Plank, E. Leitgeb, A. Friedl, K. Zettl, T. Javornik, and N. Schmitt, “Challenges in establishing free space optical communications between flying vehicles,” in *2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing*, 2008, pp. 82–86.
- [438] A. K. Majumdar, *Free-space Optical (FSO) Platforms: Unmanned Aerial Vehicle (UAV) and Mobile*. New York, NY: Springer New York, 2015, pp. 203–225. [Online]. Available: https://doi.org/10.1007/978-1-4939-0918-6_6
- [439] B. Ndagano, B. Perez-Garcia, F. S. Roux, M. McLaren, C. Rosales-Guzman, Y. Zhang, O. Mouane, R. I. Hernandez-Aranda, T. Konrad, and A. Forbes,

- “Characterizing quantum channels with non-separable states of classical light,” *Nature Physics*, vol. 13, no. 4, pp. 397–402, Apr 2017. [Online]. Available: <https://doi.org/10.1038/nphys4003>
- [440] P. Kruse, P. Kruse, L. Glauchlin, M. Mellon, L. McGlauchlin, R. McQuistan, and J. W. . Sons, *Elements of Infrared Technology: Generation, Transmission, and Detection*, ser. Elements of Infrared Technology. Wiley, 1962.
- [441] S. Shah, S. Mughal, and S. Memon, “Theoretical and empirical based extinction coefficients for fog attenuation in terms of visibility at 850 nm,” in *2015 International Conference on Emerging Technologies (ICET)*, 2015, pp. 1–4.
- [442] R. Jozsa, “Fidelity for mixed quantum states,” *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994. [Online]. Available: <https://doi.org/10.1080/09500349414552171>
- [443] B. Li, T. Coopmans, and D. Elkouss, “Efficient optimization of cut-offs in quantum repeater chains,” in *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2020, pp. 158–168.
- [444] G. Soni, “A performance analysis of free-space optical link at 1,550 nm, 850 nm, 650 nm and 532 nm optical wavelengths,” *Journal of Optical Communications*, vol. 39, no. 3, pp. 335–341, 2018. [Online]. Available: <https://doi.org/10.1515/joc-2016-0118>
- [445] J.-F. Libert and G. Waterworth, “13 - cable technology,” in *Undersea Fiber Communication Systems (Second Edition)*, second edition ed., J. Chesnoy, Ed. Academic Press, 2016, pp. 465–508. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/B9780128042694000131>
- [446] V. Sharma and S. Banerjee, “Analysis of atmospheric effects on satellite-based quantum communication: a comparative study,” *Quantum Information Processing*, vol. 18, no. 3, p. 67, Jan 2019. [Online]. Available: <https://doi.org/10.1007/s11128-019-2182-0>
- [447] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, “Long-distance entanglement-based quantum key distribution,” *Phys. Rev. A*, vol. 63, p. 012309, Dec 2000. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.63.012309>
- [448] P. Holme and J. Saramäki, “Temporal networks,” *Physics Reports*, vol. 519, no. 3, pp. 97–125, 2012, temporal Networks. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0370157312000841>
- [449] H. Wu, J. Cheng, S. Huang, Y. Ke, Y. Lu, and Y. Xu, “Path problems in temporal graphs,” *Proc. VLDB Endow.*, vol. 7, no. 9, pp. 721–732, may 2014. [Online]. Available: <https://doi.org/10.14778/2732939.2732945>

- [450] N. Masuda and R. Lambiotte, *A Guide to Temporal Networks*, 2nd ed. WORLD SCIENTIFIC (EUROPE), 2020. [Online]. Available: <https://www.worldscientific.com/doi/abs/10.1142/q0268>
- [451] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98–105, 2017.
- [452] 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. 46 317–46 350, 2019.
- [453] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," *Nature*, vol. 549, no. 7671, pp. 195–202, Sep 2017. [Online]. Available: <https://doi.org/10.1038/nature23474>
- [454] D. Sierra-Sosa, M. Telahun, and A. Elmaghraby, "Tensorflow quantum: Impacts of quantum state preparation on quantum machine learning performance," *IEEE Access*, vol. 8, pp. 215 246–215 255, 2020.
- [455] T. M. Khan and A. Robles-Kelly, "Machine learning: Quantum vs classical," *IEEE Access*, vol. 8, pp. 219 275–219 294, 2020.
- [456] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1209–1242, 2019.
- [457] L. Le, T. N. Nguyen, A. Lee, and B. Dumba, "Entanglement routing for quantum networks: A deep reinforcement learning approach," in *ICC 2022 - IEEE International Conference on Communications*, 2022, pp. 395–400.

Index

- A
- Acquisition, Tracking, and Aiming, 78
 - Ant Colony Optimization, 132, 134, 135, 138, 140–144, 199
 - Application Programming Interface, 107, 124, 127, 128, 154, 155, 165
 - Atmospheric visibility, 181, 187, 190, 193
- B
- Bell State Measurement, 37, 92, 100, 128–131, 137, 138
 - Bloch’s Sphere, 24, 25, 30
 - Bring Your Own Device, 106
- C
- Coherent One-Way, 59
 - Commercial Off-The-Shelf, 145
 - Computational Basis, 23
 - Computational Basis State, 23, 24, 26
 - Continuous-Variable QKD, 5, 57, 58, 72, 204
 - Control Plane, viii, 11, 15, 16, 106, 107, 109, 110, 123, 132, 136, 153–155, 162, 168, 175, 180, 190, 197, 200, 203
 - Controlled NOT, 33, 38, 40
- D
- Cooling System, 50, 52
 - Data Plane, 11, 106, 107, 109, 111, 113, 123, 127, 136, 153, 154, 163, 165, 168
 - Delay-Tolerant Networking Architecture, 132
 - Density Matrix, 26, 43–46, 175
 - Detector Count Rate, 71
 - Differential Phase Shift, 59
 - Discrete-Variable QKD, 5, 57, 59, 64, 204
 - Distributed Quantum Compiler, 73
 - Drop size distribution, 181, 187
- E
- Entangled Photon Source, 80
 - Equatorial-Polar, 124
- F
- Far-Infrared, 102
 - First Postulate, 21
 - Fourth Postulate, 23
 - Free Space Optics, ix, 14, 16, 102, 103, 123, 126, 154, 163, 172, 181, 182, 191
- G

- Gaussian Modulated Coherent-State, 58
- Geostationary Earth Orbit, 69, 94, 124, 127, 144
- Geosynchronous Orbit, 94
- Global Navigation Satellites Systems, 18, 78, 94
- Global Positioning System, 76, 78, 125, 127, 145, 150, 185, 200, 202, 203
- Greenberger-Horne-Zeilinger, 35–37, 81
- Ground Station, viii, ix, 13, 14, 16, 18, 68, 69, 71, 72, 81, 104, 123–125, 127, 128, 142, 144, 149, 150, 153–157, 160, 163–169, 173, 180, 185–187, 189, 190, 192–196, 203
- H**
- High Altitude Platforms, 94–96, 204
- Highly Elliptical Orbit, 94
- Hong-on-Mandel, 79, 80
- I**
- Inertial Measurement Unit, 183, 185, 202
- Inter-Satellite Links, 138, 144
- International Space Station, 118
- Internet of Things, 104
- Intrusion Detection System/Intrusion Prevention Systems, 105
- Ion traps, 46, 47
- L**
- Local Oscillator, 76–78
- Long-Infrared, 102
- Low Altitude Platforms, 95, 96
- Low Earth Orbit, vii, viii, 10, 14, 15, 20, 69, 70, 72, 96, 103, 114, 117, 124, 125, 127, 139, 143, 144, 146, 147, 153, 154, 163, 164
- Low Lunar Orbit, 103
- M**
- MA measurement-device independent QKD, 68
- Machine Learning, 205
- Master Control Station, 123, 127, 153–158, 160, 161, 201, 202
- Medium Earth Orbit, 15, 69, 94, 96, 124, 125, 144, 145, 149
- Metropolitan Quantum Drone Networks, ix, 16, 172, 173
- Mid-Infrared, 102
- Modified Random Walk, 132, 138, 140–144, 199
- Moore’s Law, 4
- N**
- Near-Infrared, 102, 103
- NetSquid, 175–180
- Network Operating Systems, 106, 136
- Nitrogen Vacancy, 27, 28, 49
- Non-Terrestrial Networks, 10
- NORAD, 118
- O**
- Open Shortest Path First, 132
- P**
- Pitch axis, 182
- Probability Density Functions, 140

- Q
- QBER, 71, 81
 - Quality of Service, 10, 82
 - Quantum SDN, 11
 - Quantum Bit Error Rate, 63, 67, 68
 - Quantum Computer, vii, 5, 6, 8, 17, 50, 52, 70, 72–75, 96, 100, 113, 205
 - Quantum Computers, 162, 187, 190
 - Quantum Computing System, 49, 175
 - Quantum Data Center, 52
 - Quantum Data Centers, 17, 73, 74
 - Quantum Device, 3, 17, 29, 51, 53, 171, 199
 - Quantum dots, 46, 48
 - Quantum Drone Networks, ix, 173
 - Quantum Error Correction processor, 49, 51
 - Quantum Internet, vii, 17, 70, 90, 175, 200
 - Quantum Key Distribution, ix, 5, 11, 16, 20, 55, 57, 59, 64, 69, 70, 72, 81, 98, 115, 173, 180, 186, 187, 203, 204
 - Quantum Machine Learning, 205
 - Quantum Mechanics, 3–5
 - Quantum Memory, 12, 20, 21, 29, 50, 68, 69, 113, 128, 178, 204
 - Quantum Metropolitan Area Network, ix, 202, 203
 - Quantum Network, viii, 3, 11, 16, 18–21, 27, 28, 69, 75, 77, 78, 80, 87, 89, 92, 101, 102, 113–115, 128, 132, 147, 154, 162, 163, 171–173, 175, 177–179, 185, 189, 190, 199, 200, 202, 204, 205
 - Quantum Nondemolition Detectors, 68
 - Quantum Phase Transitions, 42, 98, 189
 - Quantum Positioning System, 19, 55, 78–80
 - Quantum Radar, 82, 83
 - Quantum Repeater, 12, 14, 16–18, 50, 68, 72, 81, 82, 87, 88, 92, 100, 101, 113, 151, 155, 162, 163, 166, 173, 178, 180–182, 187, 189, 190, 193, 197, 199, 202, 203
 - Quantum Satellite Control Stations, 163–165
 - Quantum Satellite Networks, vii, 14, 15, 17, 18, 20, 87, 91, 102, 104, 114, 117, 199
 - Quantum Satellite Repeaters, 123, 124, 127, 129, 147, 154–157, 160, 163, 165
 - Quantum SDN, 153, 164
 - Quantum Supremacy, 6
 - QuISP, 179, 180
 - QuNetSim, 179
- R
- Roll axis, 182
 - Round-Robin Differential Phase Shift, 59
 - Routing and Key Allocation, 125
 - Routing and Resource Allocation in Free Space QKD, 69

- RSA, 56, 57
- S
- Satellite Laser Ranging, 71
- Second Postulate, 22
- SeQUeNCe, 179, 180
- Service-Oriented Architecture, 17, 171
- Short-Infrared, 102, 103
- Simplified Deep Space Perturbations, 118, 120
- Simplified General Perturbations, 118, 120
- Skyfield, 117, 137, 148, 160
- Software-Defined Networking, vii–ix, 10–12, 15–20, 55, 69, 73, 74, 87, 91, 104, 106–115, 117, 122, 124, 127, 132, 136, 143, 151, 153–155, 162, 165, 171, 173, 185, 186, 188, 189, 197, 200–204
- Solid-State Spin, 46, 49
- SQUANCH, 179
- Superconducting qubits, 46, 48
- T
- Third Postulate, 22
- Time Of Arrival, 78
- Topological, 46, 49
- Two-Line Element set, 113, 117, 118, 120, 137, 148
- U
- Unified Communications, 106
- V
- Very Low Earth Orbit, 94, 96
- Virtual Quantum Processor, 73
- W
- W, 36
- Y
- Yaw axis, 182