UAB
Universitat Autònoma
de Barcelona

Treball Fi de Grau

Grau d'Enginyeria Electrònica de Telecomunicació

Quantum Internet

Kevin Saltos Galvez

Director: Angeles Vázquez Castro

Departament de Telecomunicació i Eng. de Sistemes

Escola d'Enginyeria
Universitat Autònoma de Barcelona (UAB)

Juliol 2023

Index

1 Introduction 1

1.1 Definition 1

1.1.1 Qubit 2

1.1.2 Properties of Qubit 2

1.2 Quantum communication 3

1.2.1 QKD 3

1.2.2 QKD Architectures for quantum networks 4

1.2.3 Deployment of QKD 4

2 Literature Review of QKD Networks 5

2.1 QKD experiments 5

2.1.1Advances in short-distance links (metropolitan links) 5

2.1.2 Advances in medium-distance links (intercity links) 6

2.1.3 Advances in intercontinental links 7

3 Entanglement functionalities on a network 8

3.1 Gral concept 8

3.2 Principles 8

3.3 Key components 9

3.4 Challenges 10

3.5 Error control 11

3.6 Architecture model of quantum internet 11

3.7 Entanglement experiments 12

3.7.1 Labs experiments 12

3.7.2 Metropolitan / intercity entanglement experiments 13

3.7.3 Initiatives 14

3.8 Conclusions 15

4 Study Case (Entanglement Assisted Classical Capacity) 16

4.1 Shannon theory 16

4.2 Scenario 16

4.3 Background 17

4.4 Performance 18

4.5 Classical capacity 18

4.6 Simulation on Matlab 19

4.7 Conclusion 21

5. Conclusion 22

Acknowledgment 22

References 22

Quantum Internet

Kevin Saltos Galvez, *UAB*

Abstract—During the development of my TFG, I did an investigation into the current state of quantum technologies, with a special focus on quantum communications and the deployment of the Quantum Internet.

The initial phase of my research includes analyzing the fundamental characteristics of quantum communications, which involves the use of qubits. Qubits have unique properties, such as entanglement and superposition. I mentioned the most advanced deployments of quantum networks to date, specifically Quantum Key Distribution (QKD) networks, as well as the potential of entanglement networks, which are considered to be the main objective of the Quantum Internet.

In my study, I analyzed the principles of entanglement networks, which utilize techniques such as teleportation and entanglement swapping, and I analyzed their deployment experiments. Nevertheless, entanglement provides significant advantages for several applications, including distributed entangled computing, quantum sensing, and QKD as well.

My final study case was based on exploring the potential of entanglement to improve classical communication capacity. It is possible with entanglement, particularly in the presence of noise and losses in the bosonic channel. The advantages of Entanglement-Assisted (EA) capacity become evident in such scenarios. Unfortunately, these advantages are significantly reduced when considering an imperfect entanglement distribution.

The goal of my case study was to determine the specific ranges and conditions under which EA continues providing beneficial classical capacity.

Index Terms—Keywords: Quantum Internet, Quantum network, QKD, Qubit, Superposition, Entanglement, Entanglement-Assisted Classical Capacity, Quantum computer, Trusted node, Satellite, Quantum repeater, Quantum memory, Architecture model, QKD experiments, Entanglement experiments, Holevo capacity, Shannon theory, Quantum Shannon theory

1 INTRODUCTION

In recent years, new and innovative quantum technology has arisen that has the potential to change the nature of computing and communications as we know it. Giant tech companies are already aware of this and are eager to enter the quantum race for quantum supremacy. For instance, IBM intends to achieve a quantum computer with over 1000 qubits by this year 2023, and more than 4000 qubits by 2025 [1]. Despite this great milestone that awaits us this year, it is still a small number of qubits and thus it gets short to fulfill the entire potential that quantum computing can achieve [2]. However, once we reach the whole potential, it would undoubtedly change markets and industries.

This shows that we are in such an ongoing development and research in quantum technology (within the so-called “2nd quantum revolution"), which could have a certain analogy to the classical computer's impact in its first steps.

At first, no one expected how the internet would change our lifestyle and communication methods. Today's internet connects computers and devices from all over the world. It is hard to visualize a future without the Internet since we utilize it for practically everything: inline shopping, communicating, even managing our finances through an online bank, etc.

Nevertheless, due to its wide usage, the Internet has a certain fragility when it comes to protecting our confidential information. Many so-called classical cryptographic systems confront hacking attempts when trying to steal information. But, even so, there is always the possibility (even if minimal) that this hacker circumvents the cryptography system, and gains access to our confidential information. In fact, super-powerful computers are increasingly being introduced into the market, and that poses encryption methods at even more risk.

One of the problems that the Quantum Internet spans is the improvement of the security in the communications of our global network, enabling the detection of eavesdroppers and ensuring secure transmission.

In addition, with the boost of quantum computing in giant tech firms, it is necessary to design a network that connects each quantum machine and establishes reliable communication between them. Hence, the presence of the Quantum Internet will be necessary.

1.1 Definition

The Quantum Internet (**QI**) is the final stage of the current quantum revolution [3]. Physics, scientists, and engineers who are working on quantum technology came up with a new form of the Internet.

Generally, QI is a network that allows every quantum device to exchange quantum data inside the environment that takes advantage of quantum physics laws. This advantage opens doors to new communications and computing capabilities. Despite this, the goal of a quantum internet is not to replace today's internet, instead, to create a co-existent network that can be used just for specific types of problems.

But first, what kind of data does QI manage? The current classical communication utilizes bits, the well-known minimum unit of information. But in quantum computing, the minimum unit of information is the quantum data, also known as a qubit.

1.1.1 Qubit

As Moore's law tells us, the number of transistors in a microprocessor increases over time, enabling the development of smaller computers with smaller circuits. However, there will come a point where the circuit signals reach the scale of an atom. At this scale, classical physics begins to behave differently, and quantum mechanics begins to emerge. Thus, a **qubit** is a basic unit of quantum information that use these quantum mechanics and can have different subatomic forms such as atoms, electrons, photons, and ions as information bits [4].

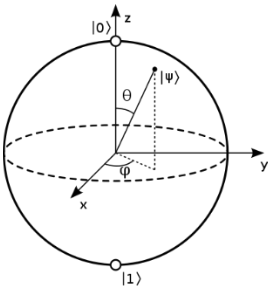


Fig. 1. A qubit depicted in a Bloch sphere with 3 axes. Source: [5].

The qubit can be represented in the **Bloch sphere**, as we can see in Figure 1, so it helps to visualize its quantum state better. In the Bloch sphere, the qubit's state is represented as a vector extending from the center of the sphere to any point on its surface. The position of this point on the sphere's surface determines the probabilities of measuring states 0 or 1, and the direction of the vector determines the qubit's phase [5].

On the Bloch sphere, the "0" state of the qubit is at the north pole of the sphere, and the "1" state is at the south pole. But, since this vector can be in any direction of the sphere, the qubit can have linear combinations of these 0 and 1 states, even being complex. The point is defined by **Dirac notation** [5] as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are the coefficients of both states that determine their probabilities making its square, so that $|\alpha|^2+|\beta|^2 =1$ must be 1, that is, 100%.

1.1.2 Properties of Qubit

That is the way the qubit is represented, as a sum of multiple states, where its coefficients could be complex depending on the position of the vector and determines the probability of being state |0> or being |1>. And even exits the case where both probabilities could be 50%, then the qubit state would be completely random by nature. So, the qubit cannot be defined as only one state, unlike a classic bit that always has the probability of 100% of being the state 1 o the state 0 separately. This feature is called **superposition** [6].

The superposition allows the qubit to have greater capacities than the bit because with the qubit it is possible to operate at the same time and make the operations faster. As [3] says, while classical 'n' bits can encode only one of 2^n possible states, 'n' qubits allow encoding all 2^n possible states at once. This, along with techniques such as Grover's algorithm or Shor's algorithm [4], allows quantum machines to perform operations in relatively short times compared to current classical computers which could take years.

Another characteristic of the qubit that is rather important, is **quantum measurement**. We must consider when it is the right moment to measure a qubit because when we make it, the measurement will irreversibly alter the original state of the qubit and make it collapse in a value, which depends on the probabilities of the states, and it won't be possible to change it anymore, keeping it at that value. That makes the qubit become a classical bit as long as it is measured in the same axes.

For example, if we measure a superposed qubit and the outcome is state 1, the superposition is lost and whenever we measure, the outcome will be state 1 regardless of the amount of probability that state 0 has. Thus, measurement can also result in the loss of information by disrupting the quantum state.

This property also affects the next quantum theorem, the **No Cloning Theorem** [7]. Basically, a qubit cannot be cloned because of quantum measurement since it is not possible to clone a qubit without measuring it beforehand. And if you do so, you will make the qubit collapse to a final state killing the qubit superposition. So, we cannot use the information stored in qubit as many times as we want to.

Classical communication and computing are based on the ability to copy data, even the simplest classical operation relies on copying bits. But in quantum communication is not possible. This mainly affects the quantum network design. So, we cannot use the same methods of classical communication to build a quantum network, and a new system and protocol will be implemented.

However, the biggest and most important difference between the qubit and the bit is the **entanglement** [8]. Two qubits are entangled when they share properties that depend on each other and they have an incredibly strong connection, that is, any change in one particle will turn into changes in the other no matter how far away they are. Two qubits entangled cannot be characterized independently and are defined as one only state. Thus, by measuring the state of a qubit, you will instantly determine the state of the other. This allows the teleportation of data without the need for a physical channel that connects them during transmission.

In fact, three physicists recently won the Nobel Prize in Physics (in 2022) on quantum physics [8], proving that entanglement exists since it violated Bell's inequalities. Even so, it is not possible to use entanglement by itself in order to create communication, but it is necessary for a classical channel as we will show below.

As we have seen, the qubit has special properties with no counterpart in the classical bit. All these features are consequences of the quantum mechanic's laws that make qubit a peculiar and very interesting element to use in computing and communication. But at the same time, these properties complicate the engineering behind the design of quantum devices.

Although the power of quantum devices exponentially increases as the number of qubits increases, the higher you increase, the harder the control, the interconnection, and the preservation of qubits will be. One of the reasons why the QI could be useful is because it can unlock the quantum computing potential so that connecting several quantum computers through the QI creates a far more capable system and increases the total computing power [9]. Even so, the main application of quantum communication es security.

The issue is that the implementation of a quantum network also has its difficulties, as we will see later.

1.2 Quantum communication

One of the main differences between QI and today's internet is that current network functionalities assume that data can be safely read and copied, as I mentioned before. But in QI, it is not possible due to the No-Cloning theorem, so another system and protocols will be necessary to run a quantum network.

While today's internet relies on the distribution of bits, the future QI aims to distribute qubits in a more secure way. Nowadays, qubits are not optimized to convey large amounts of data compared to classical bits. That's why the qubits are used just as a valuable resource within a quantum system. Quantum communication relay on conveying qubits through quantum channels, exploiting their properties such as measurement, superposition, and entanglement, for a specific application.

Overall, the most advanced application of quantum communication is security. To send a classical message, there is one specific application to encrypt the classical message with a quantum key.

1.2.1 QKD

The first quantum encryption comes from **BB84** [11], which is based on the transmission of superposed states. Thanks to the quantum measurement property, if any eavesdropping would like to read the message, he will require to measure the qubits, which can be easily detected since it alters the qubit state and, therefore, we abort the transmission of the qubits. In this way, BB84 is a protocol to produce a secret key to share between two users, guaranteeing the secrecy of posterior communication. The process of transmitting the secret key between two end users is called **Quantum Key Distribution** (QKD).

The goal of **QKD** is to share a quantum key to, then, encrypt the classical message you want to send. It is important to mention that QKD is just responsible for the creation of the quantum key.

The qubits for the quantum key are distributed through a quantum channel using random values. However, the transmitter, Alice, randomly chooses the basis in which she will encode the qubits obtaining a qubit sequence for transmission. This qubit sequence is then sent to the receiver, Bob, who also randomly chooses a basis to measure each qubit. The measured basis of each qubit is discussed by a public classical channel following a specific protocol such as the BB84.

Following BB84, if both Alice and Bob measure the qubit on the same basis, they always obtain the same measurement result (measurement property) for both parts providing classic bits for the encryption key. In return, if both Alice and Bob choose different basis, the result will be completely random and nothing useful, so these qubits will be discarded.

In this way, QKD offers a secure quantum key exchanged between Alice and Bob, since any attempt at eavesdropping qubits on the quantum channel modifies the qubit state, which will be detected by users with a probability of $P_{detection} = 1 - (3/4)^n$ [11], being "n" the numbers of eavesdropped qubits. The more eavesdropped qubits, the more detection probability.

Once the quantum key is established, the most famous technic for encrypting the message with the quantum key is the One Time Pad [12] which produces a cryptogram, or ciphertext, (bit-by-bit XOR operation between the message to send and the quantum key) that will be public and will be transmitted through a classic channel.

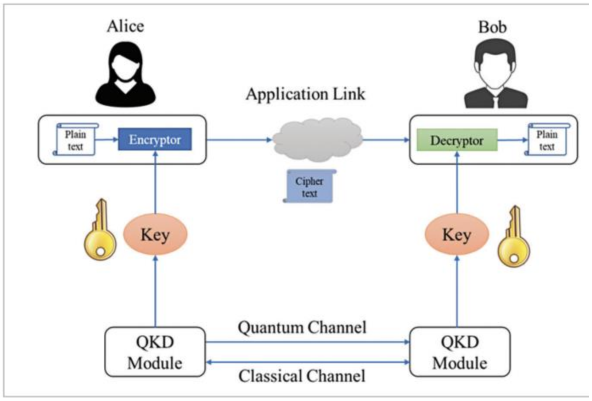


Fig. 2. *Typically, QKD link architecture between Alice and Bob. Source:* [10]

Figure 2 gives us a more understandable vision. It can be observed the separation between the QKD protocol in charge of distributing the key (the bottom of figure2), and the later use of the key by classical encryption at the application layer by Alice and Bob (the top of figure2).

Once the quantum key is obtained and is used for the cryptogram, shifting to the second part not related to QKD, Alice sends the ciphertext to Bob, who applies the same (XOR) operation with the shared quantum key in order to obtain the classical message from Alice.

The common way to apply QKD applications is by conveying qubits through **optic fiber** links via photons, but this limits the protocol's effectiveness. Because qubits can easily be lost in optic fiber links due to the attenuation, noise, and dispersión effects. If that finally happens, the qubit will be destroyed forever. Since quantum signals are very error-prone and normally don't reach more than 100 km according to [13]. However, as time goes and quantum technologies get better with new methods, this distance increases. However, there is a **physical distance**

limit that fiber optics have.

Note that due to the no-cloning theorem, qubits cannot be copied and retransmitted. That's why it is super important to keep the qubits in the perfect condition and environment in order not to lose any qubits, but after all, it is unavoidable.

1.2.2 QKD Architectures for quantum networks

The first implementations of QKD were point-to-point links between only 2 regional users (see Chapter 2). This limited the QKD's application and was not feasible at all. Hence, experts have been developing methods to extend the distance of QKD links, since quantum networks own multiple QKD links.

Several companies mainly implement the **Trusted Nodes** architecture to extend QKD links [13]. In this case, users ask the quantum network for creating secure keys. These trusted nodes of the quantum network act as intermediaries for the exchange of quantum keys between end users, which cannot be directly connected via a quantum channel. We can follow the process seeing Figure 3:

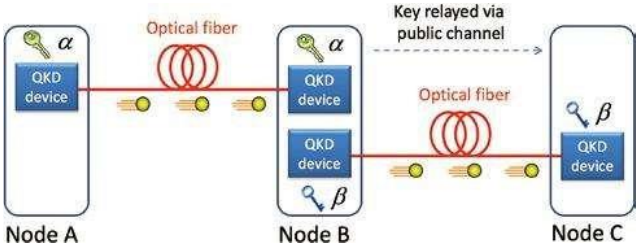


Fig. 3. *A QKD network where keys are relayed via trusted nodes. Source:* [15]

The sender (node A) creates qubits, typically single photons, and sends them through a quantum channel, which can be an optical fiber or free space, to the trusted node (node B). To extend the distance as much as possible, the satellite is normally used as a trusted node because it has fewer losses by free space [16].

Thus, a shared quantum key 'α' is generated between nodes A and B. This trusted node does the same process with the receiver (Node C) to obtain the quantum key 'β'. Thus, node B gets two different keys, but by processing these both keys (usually with bit-by-bit XOR operation), it generates a combined secret key, known by the sender (A) and the receiver (C).

Then this key is relayed via a public channel to the receiver (C), thereby, node C knows about its own key and the combined key. Therefore, the receiver made the same XOR operation to obtain the key from A, and it is used to encrypt their classical data providing quantum security.

If we need more trusted nodes for further distance, the same process is performed but classic information (quantum key) is transmitted between each intermediate node until it reaches the receiver [17, pp. 8-10].

In this scenario, we do not only need the trusted node, but we need to rely on the entire path achieved by an unconditionally secure transport. However, it is important to note that the theoretical security mainly relies on the end nodes, since here is where quantum procedures are performed.

The thing to consider is that a trusted node knows the intermediate and end keys, so it needs to be trusted by users. But this is a disadvantage at the same because we must assume that the trusted nodes are not malicious and that they will not try to compromise the security of the channel, but even so, there is the possibility of a failure that could compromise the security.

That is why other types of implementations have been investigated using untrusted nodes. For example, the approach of Arqit Ltd [16, pp. 3-5] can provide long-range quantum security through an untrusted satellite node. In this case, a new classical secure communication channel that operates directly between Sender and receiver must be trusted instead of the intermediate node. But this protocol has not been proven as true further than theoretical.

In summary, the use of trusted nodes in QKD allows longer and more efficient communications to be established through quantum networks, but it is necessary to completely rely on the node, which might not guarantee 100% security of communication. For this, it is necessary to use untrusted satellites node, which do not depend on other nodes. With the current technology, those would be some of the options for full security by quantum key exchange and maximum distance.

1.2.3 Deployment of QKD

Currently, there are already QKD networks that are being deployed in field trials around the world, establishing a quantum network.

We must remember that QKD works with point-to-point connections and if we want to make a global distribution to build a quantum network, we will have an architecture like Figure 4.

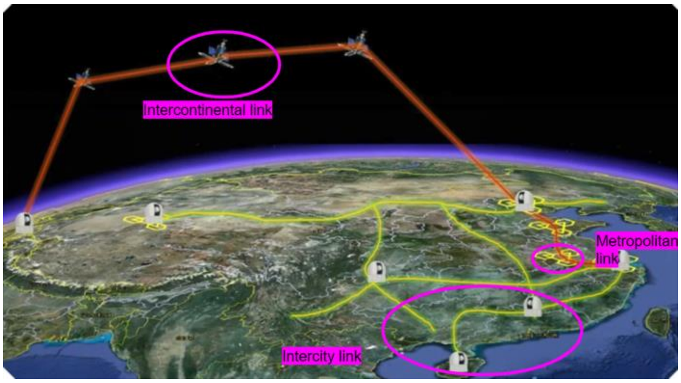


Fig. 4. *Global QKD network, where we identify the metropolitan links, intercity links, and intercontinental links. Source:* [14]

Seeing the figure, we can identify 3 types of connection. It will have urban nuclei with a great number of nodes to establish secure links. These urban nuclei are connected to each other by optical fiber links. And in order to achieve the ultimate goal of global QKD, it will be necessary to use satellites to reach greater distances.

The distance between two communication nodes cannot be very large because QKD works with individual photons that are very attenuated and, therefore, in SNR unfavorable conditions.

QKD infrastructure is organized into 3 segments [14]:

- "**Metropolitan links**" (<100 km): these links require very low-cost systems since it does not reach long distances. These try to use the existing fiber optic links to manage the quantum signals as well, with some specific characteristics. The idea is to use the same fibers to put very weak quantic signals, in order to coexist with the classic telecommunications traffic signals.

- "Intercity links" (<200 km): for this range, it is not necessary the coexistence, but it does need more dedicated links since there are more distant links with medium losses. These links connect metropolitan links thanks to the use of trusted nodes.

- "Intercontinental links": in this case, we will have higher losses, which with fiber optics could not be fixed. Hence, it is used satellite-based links as trusted nodes for long distances. Thus, the satellite is a mobile node that, at some point, may connect with a terrestrial station and generate a key.

If we aim to further project our vision towards the quantum internet, we must increase these link distances to connect large quantum networks with each other. For this, it is necessary to use other technologies and quantum properties that we will discuss below.

2 LITERATURE REVIEW OF QKD NETWORKS

Lately, other options for QKD networks are being considered, especially with the use of **entanglement**. All the quantum networks mentioned so far have provided quantum keys for their encryption. But experts are looking for the next step, that is, making full quantum communication, where all the exchanges are at the same quantum level. The way to make this possible is by sharing quantum states between remote nodes, that is, entanglement. That is the idea of the QI.

In this way, the quantum network will not only exchange keys but will offer a completely new service based on entangled states. Thus, the quantum information would be invisible to third parties, impossible to intercept, and reliably transported between sender and receiver [19].

So, we can tell that quantum networks are divided into two categories: unentangled and entangled, depending on the connections of nodes. The primary goal of unentangled networks basically is to employ QKD. In contrast, the main task of entangled networks is to distribute entanglement over long distances. Even so, the entangled network can be also used for QKD applications.

2.1 QKD experiments

From now on, we will see some examples of experiments of quantum communication networks, whether unentangled (QKD) or entangled networks. We will begin by looking at QKD networks and some experiments made recently, separating them according to the "QKD's deployment" paragraph.

2.1.1 Advances in short-distance links (metropolitan links)

In [18], they present a practical QKD system that can reach a 5GHz symbol repetition rate based on polarization. They use a method of pre-compensation of errors to be able to separate the symbols in time. They use a quantum channel of 151.5 km of fiber, with an efficient BB84 protocol that ignores one state using only 3 out of 4 states. Researchers were interested if there was crosstalk due to limitations of the bandwidth. However, there was not a lot of dispersion, there were no significant negative effects of demanding high repetition systems. So, they basically showed that it is viable to work at 5GHz. The downside is that the secure key generation rate (named SKR) is 392.7 kbps at 100km, but at the max distance it is 54.5 kbps. Throughout this project, we will realize the secure key rate and the maximum distance reached are inversely proportional, due to the longer the channel, the more losses there will be.

In [19], they worked mainly on the post-processing of the key, encoding in Time-Bin and not in polarization. Instead of having a high repetition system like the previous one, this works with only a 1GHz system. However, the main effort was applied to the classical layer of key post-processing thanks to the programmed FPGA, which allowed them to create a real-time secure key rate (SKR) of 10Mbps. They, in return, used a short communication channel of 10km (2dB loss only) to generate these many bits per second. Besides, this value is not high enough for continuous encrypted communications with extreme security, but it is useful if we accumulated a key to be used at a specific time. The system was running for 1 month without any intervention.

In [20], in order to coexist with classical communications, we need point-to-point connections that don't have an amplifier, or if it is possible to make a "bypass" (alternative path) from those amplifiers, since quantum channels cannot be amplified. They use a classic 100Gbps channel with -2.6dBm, coexisting with a polarization-encoding quantum channel and power of -70dBm (much lower power). As there is a great power difference, it means that the quantum channel will not affect the classical channel almost at all. But, in return, due to scattering in the fiber, photons in the classical channel band jump to the quantum channel band and generate noise. For short distances, this noise has a greater effect than long distance, and make detection hard. They showed that with normal single-mode fiber, they could reach 86 km of optical fiber, with a 625MHz repetition rate system. But with new fibers called Few-mode-fiber (with larger cores than single-mode fibers, which causes less presence of scattering) they can extend it up to 120km.

In [21], this is a case of final use, which had a functional network for 31 months in the city of Hefei (China). This example is a polarization-encoding, 46-node quantum metropolitan-area network implementation (Figure 5).

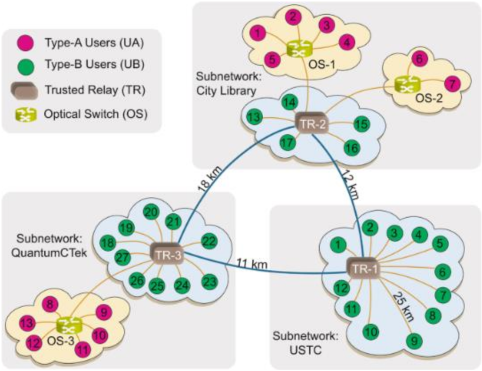


Fig. 5. *46 nodes-network schemes*, *Source:* [21]

They used this network to make real-time phone communications, text messages, and file transmission.

The network connects 40 user nodes, three trusted relays (TR), and three optical switches (OS). The network is divided into three subnetworks that are connected to each other, as we see. In each subnetwork, multiple users are connected to intermediate nodes using different methods, such as "fully connected" and "star" topology, reaching 49.5 kbps of key rate (SKR) at 18 km as maximum.

The users in the yellow cloud have a quantum transmitter and a receiver due to an optical switch. The users in the blue cloud only have a quantum transmitter.

Here each user is directly linked to all other users in the network. Consequently, it is robust against a single point of failure, and users need not rely on each other. This means that even if there is a system malfunction or a deceitful user, it would not affect communication between other users. However, the downside of this network is that the number of connections and costs increase with the number of users. Therefore, it is primarily employed for interconnecting a small number of nodes.

2.1.2 Advances in medium-distance links (intercity links)

The most chosen practical approach normally is having optical fiber's backbones that connect different metropolitan points due to propagating keys through trusted intermediate nodes. But there is also research in long-range systems.

In [22], it is implemented a practical system with the longest range nowadays: 421 km. At least the longest practical one since there are systems with greater distances but the complexity scales enormously. So, all the components they use are commercial, there is nothing of specific development, and any dedicated firm could reproduce this system. It has a 2.5 GHz repetition rate using time-bin, with Ultra Lost Loss (ULL) fiber, which has losses just below the telecom standard. The downside is that the key generation rate (SKR) is 0.25bps, very low, however, we can only increase this rate if we decrease the distance.

In [23], they use "twin-field QKD" (TF-QKD). Increasing the bit rate and range of QKD simultaneously is a challenge, and overcoming the fundamental rate-distance limit of QKD is considered unfeasible without quantum repeaters. Hence, with this different protocol, we have two emitters. Both Alice and Bob transmit light pulses with 2 lasers that are at random phases, and the two signals interfere through a quantum channel. The measurements are made in a central measuring station named Charlie, which only counts when the pulses arrive without getting the key, so we do not need to trust Charlie. This protocol reaches channels above 500km to generate a key but with roughly a 1bps Key rate. The downside is that is not a practical system like the previous one, and very good stability is needed, the lasers should act as if both were the same source at 100 km away. Hence, a lot of hardware is needed for a good synch.

In [24], the fiber QKD records were set up by this TF-QKD system. They achieved 658 km optical fibers with Ultra-Low Loss, and a Secure Key Rate (SKR) of $9.22 \cdot 10^{-10}$ per pulses. They require many devices and conditions that are far from practical implementations. However, this especially aims at ultra-long-distance vibration sensings, such as in earthquake detection and landslide monitoring, while distributing secure keys. They achieved vibration sensing by monitoring the phase of the radio frequency signal, one may identify frequency/phase disturbances of the transmitted light caused by vibration in optical fiber.

In [25], they utilized the One-Time Pad encryption for creating the Quantum Network, which consists of 10 nodes linked through an optical fiber network of active switches. The mesh-type network has six separate QKD systems built into it. They exhibit secure TV conferencing across a 45km distance for the first time using QKD connections at GHz.

The distance and the SKR are limited by the optical loss and therefore the network scheme depends mainly on the purpose and the infrastructure to be installed. Here it is used trusted nodes for increasing distance, on transparent links via optical switching, but expand QKD distance

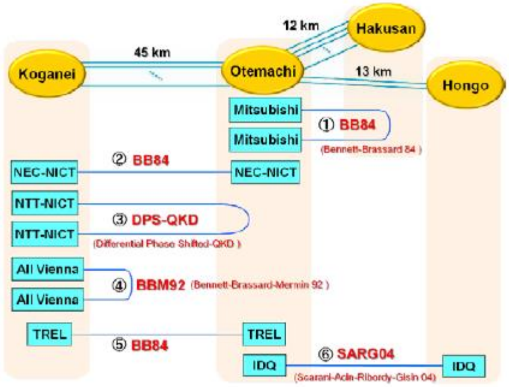


Fig. 6. a) *Tokyo QKD Network with 4 access points and six types of QKD system*

arbitrarily.

In Figure 6 a), we identify it has 4 access points connected by fibers (Koganei, Otemachi, Hakusan, and Hongo). 50% of the fibers were aerial, causing quite a few lossy links and susceptible to fluctuations. The losses are 0.3 – 0.5 dB/km. The other remaining 50% used noisy optical fibers, with photons that leak through neighboring fibers causing crosstalk.

The participating companies are from Japan and the US, with 6 QKD links (using protocols arbitrarily like BB84, BBM92,…), and some of them with reverse loops. QKD applications include smartphone QKD and secure TV conferencing. This is done with 2 relay QKD paths, each including a trusted relay node, and a redirection function to switch from when a spy is detected.

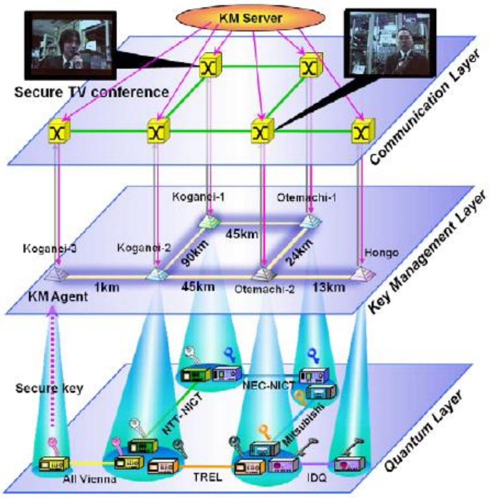


Fig. 6. b) *Three-layer architecture of Tokyo QKD Network. Source:* [25]

In Figure 6 b), we observe that Tokyo's quantum layer consists of point-to-point quantum links as all QKD is required. Each link generates the secure key in its way. QKD devices push the secure keys to the intermediate layer called the key management layer. In this layer, a Key Management Agent (KMA) located at each site receives the key through the application interface. Each KMA is actually a PC, physically protected since is a trusted node. The network functions are entirely performed in this "Key Management" layer by software. A KMA can transmit a shared secure key from one node to a second node. Therefore, a secure key can be shared between nodes that are not directly connected.

In the communication layer, secure classical communication is ensured by using distributed quantum keys for encryption and decryption of text, audio, or video data.

So basically, for reaching medium distance, we need optical fiber with intermediate trusted nodes, even though there are other alternatives that achieve the most distance (by optical fiber), but they are impractical.

2.1.3 Advances in intercontinental links

As we see, practical QKD on the ground with reasonable key generation rates (SKR) reaches around 200km. But in order to further increase the distance, satellites need to be used as trusted nodes for long-distance QKD. [16]. So, in this way, a satellite connects two ground stations. In addition, an advantage of satellites for long distances is the losses, because links in the air have a better dependence and efficiency than optical fiber links. This we can see in Figure 7.

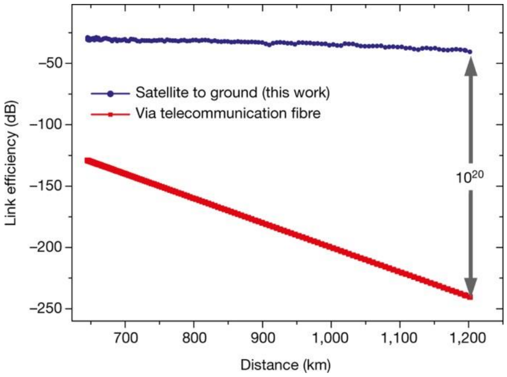


Fig. 7. *QKD link efficiencies. Source:* [26]

We observe that at 1200 km (a distance that keys can be created with satellites) there are 20 orders of magnitude of difference. Satellites are the only way to reach great distances without the need for trusted intermediate nodes.

In [26], they utilized Sat-to-ground QKD with polarization encoding. A medium-sized satellite (600 kg) called Micius has different payloads to carry out different quantum communications experiments besides QKD, such as teleportation and entanglement distribution. In order to establish this optical link between the satellite (transmitter) and the ground station (receiver), it is necessary to have a fine "pointing and tracking" system that allows establishing a stable link at least for the data-transmission time with very low losses (1-3% QBER). This system generated pulses at a rate of 100MHz (much lower than what is obtained on land) and has a secure key rate (SKR) of 0.1bps at a maximum distance (1.1 kbits/s is the minimum at a short distance). The quantum channel reached between 500km and 1200km with positive SKR. The shortcomings of this low-Earth-orbit satellite are limited coverage area and the amount of time spent within the range of each ground station. Every time the satellite contacts the ground station, it lasts a few minutes.

In [27], they related the most final example of the QKD network with all the necessary segments in China (Figure 8).

This system integrates a large-scale fiber network with over 700 fiber QKD links and 2 high-speed satellite-to-ground free-space QKD links. Along the 2000km backbone network, there were 4 metropolitan networks (in Hefei, Shanghai, Jinan, and Beijing) with different topologies, which are connected by trusted nodes. Regarding the satellite-to-ground QKD link, it achieves an impressive average SKR of 47.8 kbps during a typical satellite pass. By combining the fiber and free space, the QKD

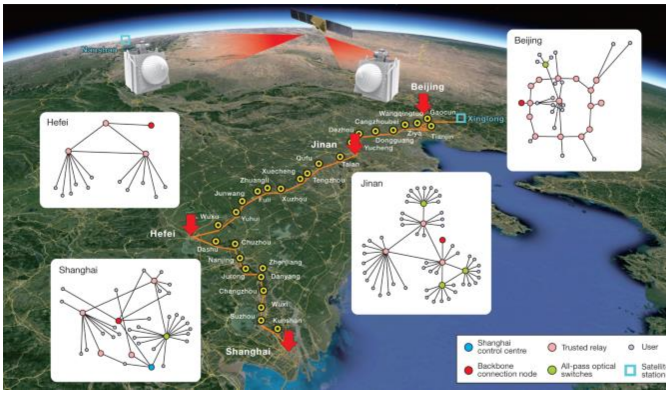


Fig. 8. *Advanced quantum communication network that operates between space and ground in China. Source:* [27]

network extends to a remote node that is over 2,600 kilometers away, allowing any user in the network to communicate with any other user, up to a maximum distance of 4,600 kilometers.

Thus, they could share keys that allowed video calls, audio calls, fax, and file transmission. This technology will exceptionally dominate in China and demonstrate that quantum technology has matured enough for practical applications. And if we want to extend it more, a global quantum network could be achieved by connecting national quantum networks from different countries via ground or ground-satellite links.

One downside is that satellite does not work the whole day, it only does when it flies over the ground station, and, with the current technology, works only when it is sunny (not rainy, foggy, or hazy conditions).

3 Entanglement functionalities on a network

3.1 Gral concept

Even with the use of satellites, while unentangled networks are still limited due to point-by-point communication, the entangled networks can be used to build a more complex network structure, which is the core network of the quantum internet.

We use entanglement because entangled qubits have unique non-local characteristics. For example, think about transferring one qubit to a different device. In theory, this device might be located anywhere (across the room, in different nations, or even on another planet). So, the two qubits will always keep the entanglement until a measurement is made (all this obviously not considering the noise). Another useful property of entanglement is that it is impossible to share entanglement with a third party if two qubits are already maximally entangled, that is when two-qubit states are called “Bell pair” [28]. So, once entanglement is created, it provides a kind of personal and unbreakable connection between the two nodes.

However, there are still important open issues for entangled networks’ implementation, research, and standardization to fully unleash the vision of Quantum Internet towards an entanglement network. Since no one has been able to successfully build an entanglement-based quantum network on a large scale. But even so, researchers are still perfecting its essential hardware, for generating, transmitting, and synchronizing qubits.

For example, as we saw, QKD networks use the trusted node architecture to lengthen the distance, but these same nodes delay the global deployment of QKD, and all the security depends on relying on the nodes. That is why the implementation of entanglement is needed.

An example of an entanglement application for QKD is having a satellite node that distributes entanglement simultaneously between the users [16]. In this way, the entanglement prevents the satellite from knowing the state of each particle, and the users can obtain the secret keys.

The disadvantage of doing it simultaneously is the fact that it requires that the users are both in the line-of-sight of the satellite, which limits the range to 1000km. But this could change in the future with the presence of quantum memory, which would store the information until it was close to the other user. This quantum memory technic along with the quantum repeater could eliminate the need for relying on keys at any intermediate node. Instead, new nodes will only act as relays and transfer qubits without measurement, providing a high level of security.

With the development of quantum memory, it might be possible to realize quantum repeaters over large areas in the near future, since nowadays they do not exist with enough maturity and are still in a state of development.

3.2 Principles

Since we want to communicate by entanglement, we must find some way to distribute entangled qubits. So, in [3], they present us with an approach that can solve this issue by **quantum teleportation**.

Quantum teleportation is just a consequence of entanglement. When two qubits are entangled, it means that one’s state cannot be defined without the other, no matter how far away they are. Thus, the information of a quantum state can be transmitted between two remote quantum devices without a physical transfer.
We could say that information is instantly teleported from one qubit to another. But that is not completely true, because the receiver must know what the sender measured, and in order to do so, a classical channel must be necessarily employed. In Figure 9, we can figure it out clearly.

So, pretend Alice wants to send Bob a message, but it is personal. The first step would be the generation and distribution of an entangled qubit pair, which comes from the Entanglement Generator and is usually a **Bell Pair** or EPR (Einstein-Podolski-Rosen) pair. Bell pair are a two-qubits state that is maximally entangled and has a great correlation. They are used as a general building block for distributed quantum applications as computing in this case since they are more convenient to distribute than an arbitrary quantum state which may have less entanglement and would place certain restrictions on distributed quantum algorithms.

Then, one of the entangled Bell Pair is sent to a receiver

Bob, while the other is to the sender Alice; all this through quantum communication. This process is, so far, the only quantum channel employed for communication.

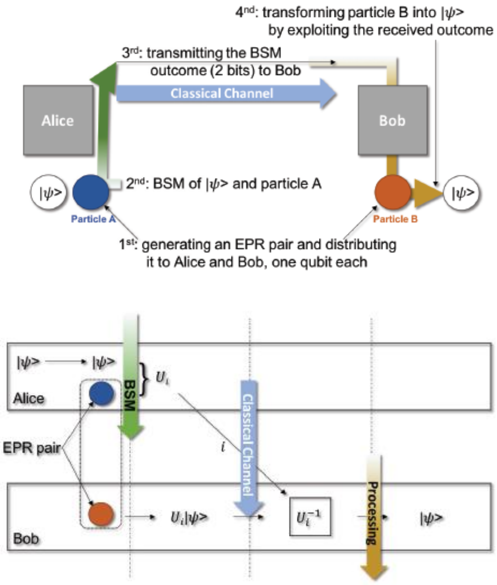

4nd: transforming particle B into |ψ>
by exploiting the received outcome
3rd: transmitting the BSM
outcome (2 bits) to Bob
Classical Channel
Alice
Bob
|ψ>
2nd: BSM of |ψ> and particle A
|ψ>
Particle A
Particle B
1st: generating an EPR pair and distributing
it to Alice and Bob, one qubit each
|ψ>
|ψ>
Alice
BSM
U_i
Classical Channel
EPR pair
i
Processing
Bob
$U_i|\psi>$
U_i^{-1}
|ψ>

Fig. 9. *Teleportation process based on Distributed Quantum Computing, Source:* [3]

The quantum state to be transmitted is applied to a third qubit called $|\psi>$. Then Alice performs a Bell-State-Measurement (BSM), a local operation to measure the qubit to be teleported $|\psi>$ and on the entangled qubit (called particle A) which both are entangled somehow. But since particle A is entangled with B, the measurement operation is like it were a combined state measurement operation of the three qubits, which causes a quantum correlation among the qubits at the two locations.

Then, Alice sends the measurement of the BSM outcome through a classical channel with 2 bits to Bob. He processes his entangled particle B according to the measurement outcome come from Alice, reconstructing the original quantum state $|\psi>$. Thus, quantum state teleportation consumes an unknown qubit state that we wish to transfer and recreate it at the destination.

As we can see, the fact of exchanging information in a classical channel means that the transmission is not instantaneous and, therefore, it does not go faster than light's speed (it satisfies the physical laws as well).

Here we can realize how crucial is the integration of classical and quantum resources for quantum networks. We cannot do without either of them in a quantum internet.

Regarding the entangled pair, the measurement BSM at the source destroys the entanglement. Hence, if another qubit needs to be teleported, a new Bell pair must be created and distributed between the source and the destination. In this way, the network needs to consistently create Bell pairs between two nodes, and thus, the entangled network just will be based on offering the resources necessary to communicate.

Another important feature for achieving an entangled network is **entanglement swapping**. We are limited to not being able to amplify any quantum signal (no-cloning theorem) and whether optical fiber or free space channels are lossy, we need a quantum repeater using this property, which an entangled pair could be created between any 2 nodes passing through an individual connection on the path. Let's see an example in Figure 10

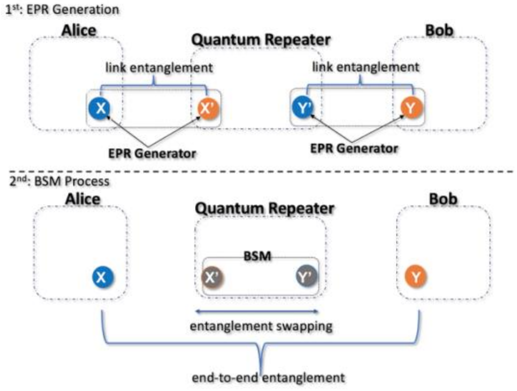


Fig. 10. *Entanglement swapping procedure in a quantum repeater. Source: [3]*

We want to connect qubit X to qubit Y through entanglement swapping, bearing in mind that we use a quantum repeater that shares an entangled state with Alice (X and X') and at the same time share another entangled state with Bob (Y and Y'). To achieve entanglement swapping the repeater carries out a Bell State Measurement (BSM) on X' and Y', which causes the end-to-end entanglement between X and Y. Hence, as the outcome of this operation is likewise a Bell Pair, it is still necessary to convey the two classical bits from the measurement since repeater contains data about which Bell pair was really generated and the received need to be informed.

3.3 Key components

We need certain hardware components to be established for the development of the quantum internet, such as quantum information sources, entanglement generator devices, detectors for quantum information, etc [28]. Nevertheless, the two main components to build the expected entanglement network are the quantum repeater and the quantum memory. Next, we will see some of its features, although they are currently under development and cannot be practically implemented.

- Quantum repeater

Quantum repeaters [29] are necessary if we wish to achieve a greater distance distribution. Quantum communication can be divided into several segments by the quantum repeater, which can establish the long-distance entanglement between sender and receiver.

A quantum repeater is one of the key **components** that constitute an entangled quantum network and acts as the core block for long-distance communication. Hence, the quantum repeater is in charge of many functions in the network, such as:

- Entanglement distribution between neighbor repeater nodes,

- Entanglement purification improves the quality of entanglement.
- Entanglement swapping linking neighbor-entangled links together to create large quantum networks.

If the elementary entangled pairs have non-unit fidelity or the entanglement swapping procedures are noisy, only a small number of pairs may be connected with entanglement. So, it will be necessary an extra procedure, which is entanglement **purification** (also named distillation). It allows us to copy an entangled state from a few noisy copies of them since that is probabilistically possible; we will review this later. Another option is to utilize a mechanism for **error control**. While implementing error control could be complex, it must guarantee a minimum **fidelity** level at the very least.

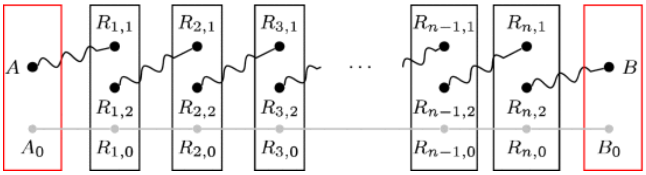


Fig. 11. *Sequence of teleportation and entanglement swapping performed by quantum repeaters, Source:* [30].

The next example from Figure 11 is based on a sequence of quantum swapping and teleportation among consecutive nodes until to reach the destination.

Two entangled nodes are connected by a wavy line and the gray lines are classical channels. Imagine that A want to send a quantum state to B through two quantum repeaters. We notice that each quantum repeater consists of at least two qubits. These qubits may be both atom qubits for swapping entanglement and/or storage.

Once A shares an entangled qubit with the first repeater (R1), R1 can apply the entanglement swapping with its other qubit (R1,2), which is entangled with the second repeater (R2). Thus, A and R2 can establish an entangled state. Furthermore, A sends the binary outcome (m1) obtained from Bell State Measurement (BSM) to R1 as well, for the teleportation. And then R1 applies the necessary correction based on m1. The correction result is then applied to another BSM in R1 with its two entangled qubits, resulting in a second (m2) that is sent to R2. R2 apply the BSM again with its 2 qubits, and the outcome (m3) is finally sent to B.

To recover the transmitted qubit from A, the receiver node B needs to know all the outcomes generated (m1, m2, and m3) by each repeater. There will be as many outcomes as entangled pairs have.

- Quantum memories

For the quantum repeaters-based quantum network it is mainly needed 2 elements: a source of entangled states, which are more advanced and are already available today, and quantum memory, which store qubits and currently are in development.

Such a memory must be capable of correctly storing qubit strings (pure or mixed quantum state) and releasing them as needed. But the storage does not have to be ideal. The storage of photons is a challenging task, and it can only be accomplished for brief periods of time utilizing, for example, loops of fibers. Delay loop lengths and storage time of memories are constrained by absorption and dephasing. One technic applied is electromagnetically induced transparency (also known as slow light), which can cause light speed to be slowed or even stopped in some materials.

Another strategy is the use of quantum memories based on atomic ensembles, in which photonic states (light) are converted to atomic excitations (solid) and vice versa. The downside is if we need to manipulate the quantum information that has been stored, there are better options such as interfaces between photons and trapped ions, NV centers, and superconducting interference devices [28]… because they allow high-fidelity manipulation of the electronic states of trapped ions.

3.4 Challenges

Now we will comment on some parameters and challenges to consider that prevent the development of a complete quantum entanglement network. First, in order to establish a distributed entangled state, we need the transmission of qubits keeping their entangled state by quantum channels. However, due to some features like the no-cloning theorem or quantum measurement, and the fact that any physical channel will always be lossy, linking nodes inside a quantum entangled network is a challenging task.

We will mention two of these parameters:

- Decoherence

One of the existing constraints is decoherence [31], which affects quantum hardware and also impedes the advancement of long-distance communication. During transmission and preservation, quantum states frequently lose information since qubits are extremely delicate and any contact between a qubit and its environment results in decoherence. A totally isolated qubit must maintain its quantum state, but isolation is challenging to establish in practice considering the quantum technology available today. Additionally, it is not ideal to have absolute isolation since computation and communication involve interacting with the qubits, so isolation and communication are incompatible.

Thus, the decoherence of long-distance entanglement could make entanglement connections unstable and lossy. In order to combat decoherence, an option that could reduce its effect is the use of wireless communication channels (free space) instead of fiber. In comparison to optical fibers, wireless transfer of quantum states is meant to be more beneficial since there are several high transmission windows in the environment. Another alternative is the quantum repeater using quantum teleportation. Unfortunately, we know it is not maturely available nowadays.

- Fidelity

We must remember errors can come from several factors. Due to defects and unpredictable fluctuations, errors almost always occur while performing any action in a quantum state. So if during teleportation (for an entangled network) some data is lost, it will be permanent (no-cloning theorem). But, even if we lose the data, we can quantify the amount of data lost with a parameter that is fidelity.

Quantum fidelity is a key measure of quality, which enables us to know how much noise from some sources, or even any operation, has impacted the quantum state. The fidelity, which ranges in value from 0 to 1, is a measurement of the capacity to differentiate between the quantum state and the desired state. Lower fidelity results from bigger implementation imperfections of any quantum process, and higher fidelity is better regarding quality.

Nevertheless, it is not necessarily a perfect fidelity to run a network, we just need to be above some specific threshold. In this way some applications will set a minimal fidelity threshold, and the network will do its best to achieve it.

3.5 Error control

As we see, generating Bell pair is the main issue for quantum teleportation and any entangled application. In order to keep the qubit safe in the communication we must take into consideration all the effects that worsen the decoherence. Therefore, once there are enough entangled pairs, we need to ensure their fidelity and get it better by purification. Since long-distance quantum communication networks must satisfy a minimal fidelity. The entangled states that are created could not have the same characteristics because of the losses of decoherence in quantum memory, in quantum gates, in any local operation, or even in the channels. Hence, we need to employ error detection or correction codes under strict constraints on the initial fidelity of entangled states and the quality of quantum gates. Now we will see some examples of error management.

- Entanglement Purification

The creation of Bell pairs and swapping operations are both noisy processes. Thus, the integrity of the state decreases with each link and each exchange and once we lose the state it will be forever. Nevertheless, it is probabilistically possible to produce fewer copies with higher fidelity from multiple identical copies of noisy Bell pairs (which, for example, can be produced by continuously distributing elementary entangled pairs).

This technique is called purification (also known as distillation) [28] which combines two or more lower-fidelity Bell pair states to produce higher-fidelity Bell pair states.

A second (and occasionally third) quantum state is used as a "test tool" to evaluate a proposition about the first state, in order to distill a quantum state. When the test is successful, the state's fidelity increases. When purification is utilized, resource needs significantly increase because are destroyed in the process. The tested state must likewise be deleted if the test is unsuccessful. In comparison to QEC, distillation places less demand on fidelity and resources, although distributed protocols have round-trip delays because of traditional communication.

- Quantum error correction (QEC)

Decoherence and errors are unavoidable, so we need a plan to correct such errors and we must consider that network's design will be affected by the choice of how to handle errors [33].

Similar to classical error correction, QEC protects a logical qubit from errors by encoding them using a great number of physical qubits. Moreover, QEC can also account for missing qubits, in addition to correcting state mistakes. Besides, if all physical qubits that encode a logical qubit are located at the same node, the correction procedure can be executed locally, even if the logical qubit is entangled with remote qubits.

Even though QEC was initially a plan to shield a qubit from noise, it may also be used for entanglement purification.

There are quantum communication technologies that can correct mistakes. Yet, QEC has very strict criteria for both the initial quality of the resources and the physical qubit needs. Given how challenging it is to implement, QEC is not expected to be used until further generations of quantum networks are practical.

3.6 Architecture model of the quantum Internet

In a quantum network, quantum nodes can take different forms, depending on their role and location in the network. Figure 12 is an example of the general architecture of the quantum internet taken from [32].

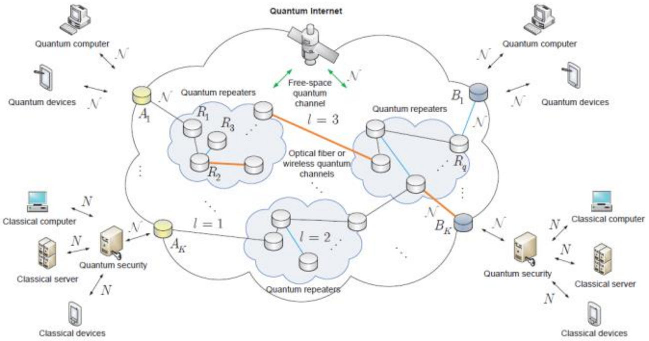


Fig. 12. *General entangled network structure of a quantum Internet, Source:* [32]

In this quantum internet network structure, we can identify different nodes and links.

If we look closely, we have several users, with quantum and classical devices. Classical machines can only access the quantum internet if they use **quantum security protocols**, like QKD or similar applications. Therefore, the quantum network must identify which type of user is entering the network and which application want to apply.

There are **source end quantum nodes** (denoted as yellow “Ai” representing Alice) that provide access to the quantum internet cloud. The network also includes numerous intermediate nodes, especially because of quantum repeaters due to the instability that a qubit can suffer in lossy and noisy communication channels in long-distance communications *[46].*

The figure represents the quantum internet as a white cloud that encompasses all the repeaters. But within this white cloud, there are other networks represented as gray clouds, which are considered as the **metropolitan networks** that cover a specific region, such as a country for example, or can even be smaller. And within this network, it can be further subdivided. But the matter is that within a metropolitan network, the links can be perfectly established through **wireless** quantum channels or **fiber optics**, they can even take advantage of the existing classic networks already established to transmit the qubits. However, these channels do not allow long distances beyond the metropolitan area, even with the use of repeaters. Therefore, when connecting two continuous metropolitan networks, **quantum satellites** are typically used, involving **free-space** quantum channels. The use of quantum satellites with quantum repeaters allows the quantum internet to span much more area and eventually establish it worldwide.

But obviously, the technology is not yet precise enough to achieve this accomplishment, there are many challenges and uncertainties to solve until having reliable and efficient quantum hardware.

In the image, it also includes receiver end quantum nodes (denoted as blue Bi representing Bob). In reality, all the links of fiber optics, wireless, or free space channels consist of entangled connections at several levels. Figure 13 from *[46]* provides a visual representation of the different levels of entangled connections of nodes.

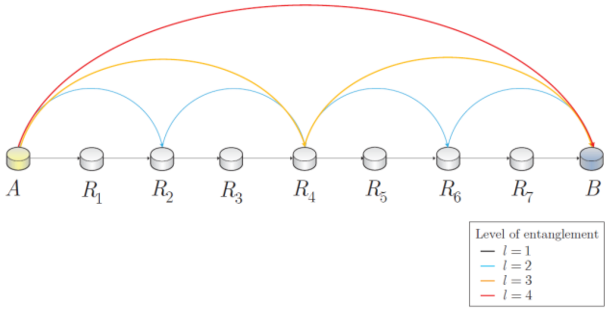


Fig. 13. *Entanglement distribution in multi-hop links depends on the level of entanglement. Source:* [32]

This architecture defines different levels of entangled connections. The goal is to establish an entanglement distance between quantum nodes A and B through a series of repeaters in the network. The first level (l=1) has a direct entangled connection with each repeater. In this case, a great entangled connection could be achieved with entanglement swapping applied to the repeaters.

For the higher levels, the entanglement distribution will be generated by the repeaters in the **middle**. For example, level l=2 of entangled connections is generated by R1, R3, R5, and R7. Level l=3 is generated by R2 and R6; and for l=4, the entangled connection is generated by only R4. This last one would be the most challenging case to achieve since the qubit has to travel the longest distance.

Even so, we see in some cases that sometimes quantum repeaters perform as entanglement generators. This allows for an efficient way to distribute entangled pair.

3.7 Entanglement experiments

To have a certain order when showing the experiments, we will classify them into the following sections: Lab experiments, Metropolitan/Intercity entanglement experiments, and Initiatives.

3.7.1 Labs experiments

In [34], they found the idea to realize the entanglement distribution for the Quantum Internet, but this one uses an opportunistic model through quantum repeaters (Figure 14).

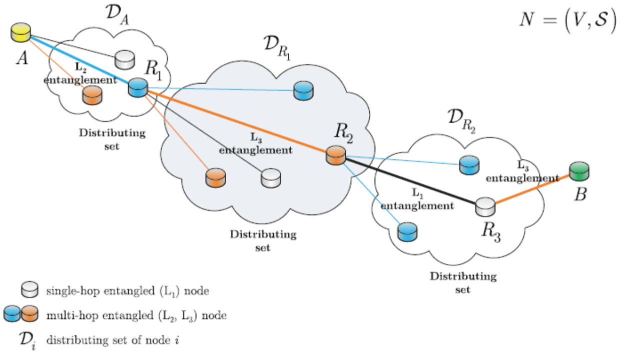
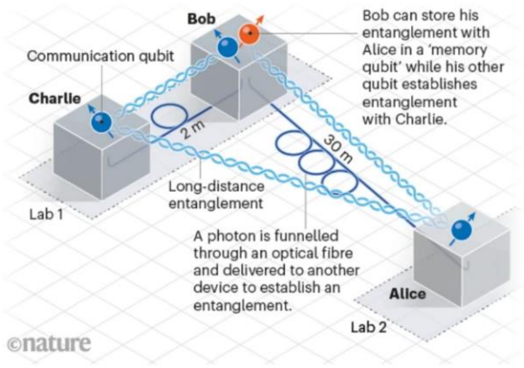


Fig. 14. *Opportunistic entanglement distribution in a quantum Internet setting. Source:* [34].

As we have seen, for very distant quantum nodes, we distribute entanglement with their "neighbors" until getting receiver B. For this, it is necessary the quantum repeaters to send entangled states in order to extend the quantum communication distance. These repeaters need one more element to store their entangled states, its quantum memory. But these (imperfect) memories add noise to the distribution process, where the probability of error evolves over time and is predictable. Hence, their objective for opportunistic entanglement distribution is to select those quantum nodes of which the cost function reaches a local minimum. This cost function uses the error patterns of local quantum memories and the prediction of the evolution of entanglement fidelities.

In [35], the Detch University of Technology achieved to connect 3 quantum machines thanks to quantum memory (Figure 15)



Bob can store his entanglement with Alice in a 'memory qubit' while his other qubit establishes entanglement with Charlie.

A photon is funnelled through an optical fibre and delivered to another device to establish an entanglement.

Fig. 15. *Entangled network with 3-quantum devices. Source:* [35]

This method uses synthetic diamonds in each quantum device with nitrogen atoms. In Charlie's diamond device, the researchers stimulate the nitrogen atom to emit a photon, so that the photon will be entangled with the state of the nitrogen atom. So, they can funnel the entangled photon through a fiber channel and send it to Bob's device. It stores information about the entanglement with Charlie in a quantum memory, which is the key to establish 3-way entanglement.

Bob's quantum memory consists of carbon13 where the Charlie's nitrogen's quantum state is stored. This release an additional nitrogen qubit which will be entangled with Alice node. In reality, quantum memories slow down, so that they can keep their quantum states for a minute or more, which in the subatomic world is enough.

Thus, the 3rd node Alice does the same procedure as Charlie and entangles with the additional nitrogen qubit from the central node Bob. Thereby, the central device has an entangled qubit with the 1st node and another with the 3rd node at the same time. This technique uses the same principles as entanglement swapping but adding the quantum memory.

Even so, it requires more years of improvement, since problems such as having the carbon qubit well isolated from its environment and, at the same time, accessible to be programmed, involve a great challenge to carry out.

In [36], it is discussed how a quantum frequency converter (QFC) was used to successfully distribute entangled photons over a 20-kilometer distance. QFC uses the difference frequency generation to convert a single photon from 780 nm to the telecom S-band at 1522 nm. The method employs a single rubidium-87 atom to create entanglement with a photon and, over the 20 km optical cable, they could obtain a conversion efficiency of 57% and an entanglement fidelity between the atom and the telecom photon of >78.5 ± 0.9%, which was mainly constrained by the atomic state's decoherence. The trial is a significant step in distributing quantum information widely.

In [37], called "FENDI: High-Fidelity Entanglement Distribution in the Quantum Internet", they offer a solution for High-Fidelity Remote Entanglement Distribution (HF-RED) in a multi-hop quantum network. They discussed the design of a remote entanglement distribution protocol for a future quantum internet, evaluating it with a quantum network simulator and demonstrating its superior performance compared to other existing solutions such as ORED, E2E-F, and QPASS. This solution has better features on fidelity while optimizing the maximum entanglement distribution rate. It involves quantum repeaters generating and swapping entangled qubits to establish high-fidelity qubits between source-destination pairs.

Apart from formulating the HF-RED issue, they demonstrated its hardness before deriving an end-to-end fidelity model for the worst-case noise called isotropic.

3.7.2 Metropolitan / intercity entanglement experiments

In [38], scientists from the U.S. Department of ESnet have built a quantum network testbed that connects various buildings on the Brookhaven Lab campus using unique portable quantum entanglement sources and an existing communications fiber-optic network. This was a significant step towards building a large-scale quantum network that can transmit information over long distances. The most achievement was that the entanglement sources used in the experiment were portable and could be easily launched in standard data center computer server racks that are connected to regular fiber distribution panels. They accomplished entanglement over 16 km, but this experiment has now expanded to include a 128 km quantum network testbed.

In [39], a new testbed for quantum communication experiments has been developed by researchers from the University of Chicago and Argonne National Laboratory. It features two linked 42 km fiber-optic cables connecting Argonne and Illinois Tollway. It is one of the longest ground-based quantum communication lines in the US with a total reach of 84 kilometers. A loop will be used to explore the science underlying quantum engineering systems and the principles of quantum entanglement, which links two particles so that they are in a shared state. The loop can help identify and address challenges in operating a quantum network and can be scaled to test and demonstrate communication over longer distances to help lay the foundation for a quantum internet.

Scientists are using the 84 km quantum loop as a testbed to transmit signals from photons emitted from ensembles of ions, which can be used as a quantum memory for the network. Before using this technology on a bigger scale, researchers will be able to test and improve it thanks to the quantum loop.

In [40], they kept the project updated and thought about the new quantum loop to be a significant development for the scientific field of quantum physics, communications, and computing.

A 56 km extension was added to the Chicago network, making it one of the longest in the United States with six nodes and 200 km of optical fiber. The extended Chicago network provides a significant increase in the scale of quantum networks for larger interstate systems.

In [42], Chinese researchers distributed entangled photon pairs over 1,200 km using the Micius satellite. This was one of the first implementations of Micius, which connected Delingha and Lijiang. The experiment proved the survival of two-photon entanglement and developed the satellite-based technology, but it is not used for any application, just offered new opportunities for studies at distances that were previously not possible on the ground.

In [41], in return, without the need for trusted relays, they used the same satellite for entanglement based QKD application between two ground stations that are 1,120 kilometers away (Figure 16)

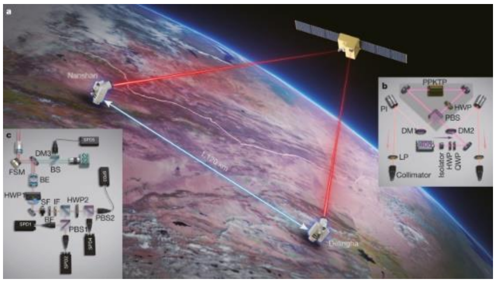


Fig. 16. *Micius Satellite over 1120 km, the set-up of entanglement based QKD. Source:* [41]

Using two bidirectional downlinks from the Micius satellite, entangled photon pairs were sent towards two ground observatories in China between Delingha and Nanshan. This was a significant advancement at that time providing secure communications over great distances without the necessity of trusted nodes.

The creation of a high-efficiency telescope significantly increased the link efficiency. To optimize the link efficiency, they developed cascaded multistage acquiring, pointing and tracking systems both in the satellite transmitters and the ground station receivers. Entanglement-based QKD is naturally source-independent, which guarantees that the system is secure against imperfections in the source. To ensure security on the detection sides, they utilized the BBM92 protocol with a QBER average of 4.51% ± 0.37%.

This research has almost quadrupled the link efficiency than without entanglement and reached a low-key secret key rate of 0.12 bits per second, despite surpassing the mark of 1000km. It is possible to brighten our space-based entangled photon source which would improve the average final key to tens of bits per second or tens of kilobits per orbit. This is a significant step towards a fully resilient and unbreakable cryptographic approach for distant users across arbitrarily long distances, increasing the safe distance of practical QKD on the ground by more than 1,000 km.

3.7.3 Initiatives

In [43], they present the Euro – Quantum Communication Infraestructure (Euro-QCI), an initiative from 2019 whose objective is to guarantee the security of secure communications in Europe, with an additional quantum security layer. In the long term, they want more complex quantum repeater entanglement technologies.

This project wants to strengthen security between present and future cyber threats. They bet that each member of the EU must develop their own infrastructure to avoid dependence on other countries. So, particularly EuroQCI-Spain wants to demonstrate use cases between Madrid and Barcelona. With assistance from the Commission's Digital Europe Plan, the EuroQCI's first implementation phase officially started in January 2023 with a focus on the following areas:

- A group of commercial initiatives to create and advance the EuroQCI's major technology pillars in order to advance the European quantum communication ecosystem and industry.
- National initiatives enable Member States to develop and construct the national quantum communication networks that will serve as the structure for the terrestrial section, testing various technologies and protocols and customizing them to meet the requirements of each nation.
- PETRUS, a coordination and support initiative that will serve as a connector between all initiatives, promote collaboration, and identify areas in need of standardization.

In [44], they present a 7-year program to build an advanced European CI ecosystem. The European Commission supports this project, which is led by QuTech. This program called Quantum Internet Alliance began one year ago (2022) and aims to develop a prototype network that connects distant cities throughout Europe.

In order to accomplish long-distance quantum communication in the future, QIA built the foundation for its prototype network, which included the first multiprocessor quantum network in the lab, the first quantum software and network stack, and a cutting-edge quantum repeater system.

The goal is to build two metropolitan-scale networks containing quantum processors and photonic clients, connected by a long-distance fiber backbone using quantum repeaters. This network will be fully programmable to allow the realization of any application supported by the hardware using software independent of the platform (full stack).

In [45], they present the Quantum Internet Research Group (QIRG), which already has support from throughout the world and researcher collaboration. This group aims to build a quantum network worldwide in 2019. QIRG established a roadmap with capability milestones to develop the quantum internet. The proposal seeks to address potential engineering issues with the quantum Internet, including those related to designing an application programming interface (API), defining the application level of the quantum Internet, and defining a standardized architectural framework. Another problem that can be tackled is the multi-party state and multi-party transfers such as network coding.

In [46], they present another initiative called the AWS Center for Quantum Networking (AWS-CQN), a new quantum department that Amazon has such as the AWS Center for Quantum Computing (AWS-CQC). They already had services in the cloud where they offered simulations or quantum computing resources. But now they want to extend it to quantum networks as well, which will mean a lot for the growth of quantum computing. The center will focus on developing quantum network technologies, tools, and applications that are expected to transform the way communications and computing are done...Collaboration with scientists and companies is essential to advance this technology, and the AWS center will seek to establish partnerships to accelerate the development of quantum solutions.

3.8 Conclusions

In conclusion, after seeing quite a few numbers of quantum network experiments, we realize that the worldwide implementation of quantum QKD networks constitutes the most advancement in the use of quantum technology to communication. For instance, currently there are already several functional quantum QKD networks in the eastern part, such as in China, Japan and Vienna, that reach max distance of 4600 km.

This development of quantum technology is due to have sufficiently mature for creating QKD networks. In Europe, initiatives such as Qutech or Euro-QCI have deployed test or metropolitan QKD networks among different cities, but they are not larger than the China network, therefore we must take the China QKD network as a reference.

Now we will see some points as a conclusion taken from the QKD experiments:

- At short distances it is possible to transmit a secure key at a fairly high rate (SKR), but as we increase the distance between nodes, this SKR is lower. Therefore, we must well compensate for the distance with the secure key rate that it will generate, also taking into account the QKD protocol used.
- Maximum SKR commented is 10Mbps at only 10km in the metropolitan area and (-the minimum SKR is 0.25bps at 421km)
- Most of the protocols used in the experiments are from Decoy-state with BB84 and can be polarization or time-bin encoded.
- Quantum communication can coexist with classical communications as long as the quantum links have much less power or use QKD with continuous variables.
- Twin-field achieves fiber point-to-point distance records with connections greater than 500km, but it is the most difficult approach to implement in practice because of all the hardware involved.
- Trusted nodes allow the distance to be extended and are more efficient if we use satellites.
- The most developed and larger network, a backbone network is used that connects different metropolitan networks and with satellites.

However, for even longer distances that enable the connection around the world, there are still certain areas that need to be developed, such as improving the effectiveness of the channel, accelerating quantum (post)processing, and putting more complex quantum protocols into practice.

As we commented, the quantum internet is not only all QKD networks, but the quantum internet spans a greater concept that contains distributed quantum computing, quantum teleportation, and other quantum technologies that make use of entanglement. The entanglement is the core network of the quantum internet.

Now we will see some points as a conclusion taken from the entangled experiments.

- For teleportation we need to establish an entangled state between two nodes. The most common form of entanglement is the Bell-pair, which constitutes its maximum level of entanglement.
- Entanglement is just a resource, which can be used for several applications, such as Distributed quantum computing, data teleportation, QKD, sensors, clocks, ...
- Repeaters are a key element for the creation of a large-scale quantum internet, together with quantum memory.
- The repeaters will usually offer a process of entangled distribution, purification, and swapping.
- The whole process of the entangled qubit throughout the communication will be affected by decoherence, reducing its entangled state.
- An important aspect when distributing entanglement is fidelity, which we must always keep high, but it does not need 100% to be functional, it depends on the error correction protocol.
- In the US, they managed to use portable entanglement sources that could be launched on another standard computer server. They also achieved a quantum loop for the test benches.
- The entanglement with QKD is implemented through satellites. In China the Micius satellite allows non-dependence on trusted nodes, it can exceed a distance of 1000km, the downside is that SKR is still quite slow, at 0.12 bps.

However, regarding entangled networks, we realize that is still a technology that needs to mature, there are still several crucial challenges, especially when it comes to extending the distances of connections worldwide, with the specific hardware for the necessary components, its errors management, and the standardization.

We can say that considerable progress has been made in the development of quantum networks in recent years. But even so, it is not enough to implement a large quantum network compared to the classical Internet, for this there is a long way to go. In fact, quantum repeaters still lack enough maturity to achieve a practical application. We only have the theory of how they would work, but scientists and researchers are still working to develop the best implementation of the ideal quantum **hardware**. Even on a practical level, quantum memories, repeaters, and error-correcting teleportation are still ambitious goals nowadays.

Apart from the necessary hardware, we must also study the best network model to find the best route among the nodes (**routing**). This is an issue to consider for these new types of quantum networks; we must find through the engineering of services and high-performance routing protocol for the quantum internet, offering services such as resources and interoperability. However, since each entangled link has a probability of transmitting successfully, routing paths are also probabilistic and unpredictable. This is what makes quantum so complicated in the field of communications.

That is why in the few applications of entanglement at metropolitan level they are from QKD and not from distributed quantum computing, since **QKD applications** are more practical because an entangled link is only created when it is necessary. Once the teleportation is done the link will collapse and then we would need quantum routers to give us effective routing paths based on repeaters, but this is where we go out of practice again. That is why the entanglement in satellites is made by end-to-end link with only 2 nodes connected, for more nodes is still a challenge.

This leads, in turn, to the problem of how to organize and design quantum internet standards for all future quantum networks. Many experiments have been developed in the quantum internet field but all of them own different characteristics, since this is a new technology in progress, there is not any background, and researchers are working on it. But once we go achieving certain milestones of quantum internet, we must establish a **standard communication** for the future worldwide quantum network. The standardization will help define a platform for the global quantum network.

So, apart from the decoherence and repeaters, I consider that an important impediment to the development of the entanglement quantum networks is the standardization and routing of the path, especially when we have multipartite connections.

4 Study Case (Entanglement Assisted Classical Capacity)

4.1 Shannon theory

As we mentioned, entanglement distribution is the main goal in a quantum network. Thereby entangled pairs can be utilized for various applications, such as quantum secure information, distributed quantum computing, QKD, quantum sensing, etc. Nevertheless, in this context, we will focus on one specific application: a boost to classical communication rates thanks to the **Entanglement-Assisted Classical Capacity** (EACC).

In classical networks, the communication channels are in charge of transmitting information while achieving the best possible properties. For example, the capacity of a communication channel takes into consideration the maximum rate at which information can be transmitted through it. That is why the Shannon theory is employed in communication channels.

The Shannon theory provides a framework for understanding the requirements for information communication in the presence of noise and perturbations, as well as analyzes the capacity of a channel to reliably transmit information [47]

The capacity of a channel is represented as the maximum rate at which information can be transmitted without errors or failures. Shannon represents the capacity as follows:

$$C = B \cdot log_2(1 + SNR)$$

Where B represents the bandwidth, and SNR (Signal to Noise Ratio) determines the presence of noise in the channel. A higher SNR is desirable because it means that the signal power is higher than the noise power.

If we transpose this concept to the quantum world, the Quantum Shannon theory arises [48]. It extends Shannon's theory to a quantum system, where quantum communication channels are employed instead. Quantum Shannon takes into account the quantum mechanics within the quantum channel, determines the manipulation of qubits, as well as the quantum error correction, and quantum communication protocols.

The most applicable feature of quantum Shannon theory is entanglement. It determines the utilization of entangled states for various purposes, including security, encoding information, efficient communication…

In that way, there is an effective operation of entanglement to improve classical capacity. However, first it is essential to explain the scenario for a further understanding of this concept.

4.2 Scenario

Throughout this research, our goal has been to understand the functionality of the Quantum Internet and the crucial role of entanglement. In this scenario, we assume the existence of quantum internet (or a basic quantum network) that provides entanglement between two endpoints, namely Alice and Bob. The entanglement distribution can even be achieved by just a satellite based on free space communication as we see in Figure 17, but the most important is to establish entanglement between different users.

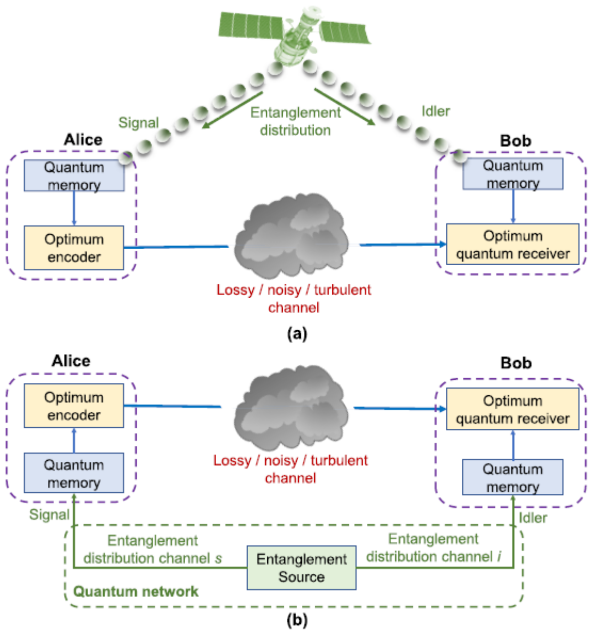


Fig. 17. *Entanglement-assisted classical communication provided by a satellite or by certain quantum network. Source:* [49]

In this situation we will have two channels coming from the entanglement source, one is known as the **signal mode** and is headed to Alice, and the other channel corresponds to **idler mode** and remains in Bob's memory. They both consist of entangled pairs, but the signal mode places the main function in this process. We assume throughout this project that the entanglement is pre-shared before implementation of the Entanglement-Assisted (EA).

The process starts with Alice receiving the signal photon from the entanglement source, in order to store it in the quantum memory for future use when needed. Then, Alice encodes classical information onto the entangled signal photon thanks to Optimum encoder, which converts any properties of the signal photon, such as wavelength or phase, to carry the encoded information.

Next, Alice sends the converted signal to Bob through a lossy, noisy, and turbulent Bosonic channel. Upon receiving the converted signal mode, Bob employs an optimum quantum receiver to later measure it jointly with the idler mode, that was stored in Bob's quantum memory. This joint measurement enables the decoding of the classical information from Alice.

As we will see later, we will demonstrate that Entanglement Assisted communication techniques will provide a significant advantage regarding the achievable classical capacity over noisy and lossy bosonic channel.

Since many years it is known that pre-shared entanglement improves the classical capacity against those without entanglement. However, it is usually assumed that entanglement distribution is perfect: lossless, noiseless, and unlimited. But many effects occur in any quantum channel that is not ideal, such as dispersion, attenuation, decoherence and noise, and additional factors when employing satellite-to-ground links.

Regarding quantum hardware, there is still much progress to be performed. Moreover, whether the optimum quantum receiver or quantum transmitter designs have not been achieved for optimal EA capacity yet; even quantum memory is still imperfect to be used.

Despite these challenges, afterward, we will discuss the cases where EA capacity remains achievable and is better than the classical channel capacity in the environment of imperfect entanglement distribution.

4.3 Background

Before delving into the details, it is useful to introduce some concepts of the transmission of quantum information.

Homodyne detection is a measurement technique that utilizes a single photon source and a detector in order to measure a specific property, such as phase or amplitude. It works by mixing the quantum signal of interest with a coherent reference state at a beam splitter. The goal is to extract information about the property of the quantum signal from this mixture at the detector. [50]

On the other hand, **heterodyne detection** uses two photon source and a detector to measure the interference between two optic signals. One source provides the desired quantum information to be measured, while the other source is the local laser or local oscillator with a different frequency. These two signals are mixed in the detector in order to obtain the amplitude and phase of its quantum state

Bosonic Channel refers to any transmission channel that allows the propagation of photons, especially in our case refers to a standard optical channel. It is usually affected by noise, attenuation, and loss effects.

Now, it is necessary to clarify the distinction between certain types of quantum light states that can exit.

- **Coherent state:** These states are quite common in practice as they can be classically modeled as waves, closely resembling the classical states. It is characterized by having an indefinite number of photons at each instant, but it follows a certain probability governed by the Poisson statistic. Instead, these states do have a precisely defined phase. [51]
- **Thermal state:** These states have neither a well-defined phase nor a well-defined number of photons. An example of such states could be sunlight, which can be described by black-body radiation and follow the super-Poissonian statistics.
- **Squeezed state**: These states are based on **Heisenberg's uncertainty principle**, which dictates that if the number of photons at each instant is well defined, there will be uncertainty in their phase. On the contrary, if the phase is well-defined, the number of photons will be clearly undefined. Apart from the number of photons or phases, this Heisenberg principle can also be applied to other features. Heisenberg principle allows a precise measurement in one aspect that could be enough to reduce the noise ef-

fect, despite having uncertainty in the other aspect, this is regarded as the term "squeezed" [52]

- **Two-Modes Squeezed Vacuum (TMSV) state**: It goes within the concept of "squeezed state" but this is regarded specifically for quantum entanglement. It reduces the noise as well but in just one of the modes compared to the normal vacuum state. The modes are referred to the number of entangled qubits.

These are not the only quantum light state, it exits further but, in our project, these are the most useful.

4.4 Performance

As we mentioned, most researchers referring to EACC typically just consider the attenuation effect, while assuming ideal or perfect conditions for other properties, such as the pre-shared entanglement distribution. Therefore, we consider a more realistic scenario where the noise and no-idealities will be modeled and taken into account in each step, with the exception of the idler channel and quantum memory.

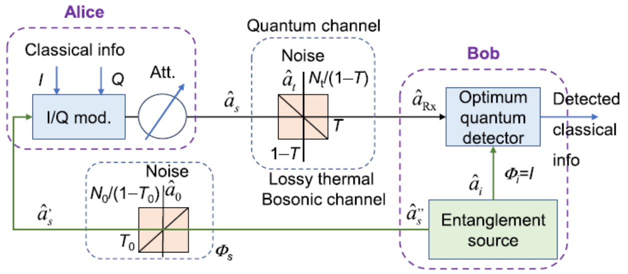


Fig. 18. *Entanglement assisted classical communication with its components depicted in detail. Source:* [49]

For this study case, we have decided to follow the paper [49] and use the expressions derived by the author. In this realistic situation (Figure 18), the Entanglement Source is located on Bob's side. Thereby, Bob just obtains his entangled idler signal $\hat{a}_i$ by his idler channel ϕ_i. Due to the built-in Entanglement Source on Bob, this channel is considered as id, that is $\phi_i = I$ where "I" is the identity operator. The idler photon should remain stored in a quantum memory until receiving the corresponding result from Alice.

Then, the other channel from the entanglement source is the signal channel ϕ_s, which is responsible for transmitting the signal photon $\hat{a}_s''$ through the Single-Mode Thermal Lossy Bosonic Channel. This implies that entanglement distribution is not perfect, there is certain thermal noise that reduce the transmissivity of Bob-to-Alice channel T_o. This is interpreted as a beam splitter that allows only the part that was not affected by the noise to pass through, which is $\hat{a}_s'$ tis are part of the TMSV state. The part affected by noise transforms the signal photon into a thermal state, which is separated from the channel by the beam splitter since it is not functional, and this thermal state follows a mean photon number of $N_o/(1-T_o)$.

Next, Alice receives the attenuated signal photon $\hat{a}_s'$, depending on the transmissivity and prepares to modulate this signal using the I/Q modulator. The modulator applies certain transformations to the signal, performing In-phase (I) or/and Quadrature (Q) modifications, performing the Gaussian Modulation (GM).

Apart from In-phase or Quadrature modulation, it is possible to use different modulations in order to encode classical information into the signal state. For example, the polar modulator is great for phase encoding [53] accomplishing EA capacity as well, or even the utilization of the I/Q modulator can be used for a different modification, such as the displacement of the signal photon state. Having precise modulation provides better properties related to capacity in the channel, as well as performance.

Then, once the signal photon is modulated, the signal $\hat{a}_s$ has to be transmitted through the same type of channel as the entanglement distribution channel, which is modeled as a Single-Mode Thermal Lossy Bosonic channel. In this case, it is considered the main channel since it carries the signal from Alice to Bob.

The noise effects are also represented as a beam splitter with the same characteristic: It reduces the transmissivity of the main channel (T), being less than or equal to the transmissivity of the distribution channel (To), that is $T \leq T_o$.

Therefore, the beam splitter removes the thermal state $\hat{a}_t$ resulting from noise, with a mean photon number of $N_t/(1-T)$, which is higher than the mean photon number in the distribution channel (No), that is, $N_t \geq N_o$.

Finally, the signal received by Bob is $\hat{a}_{Rx}$. This is the signal that Bob needs to decode, using also his idler photon stored in the quantum memory to extract the modulated information from the I/Q modulator. To achieve this, Bob performs a joint measurement on the idler and signal pair in order to decode classical information.

4.5 Classical capacity

It was already known that Entanglement-Assisted communication has an advantage in improving the classical communication capacity, especially over lossy and noisy bosonic channels. This is evident in the same prior example of [49], where the main channel is, in reality, a **quantum** noisy bosonic channel. In this case, the precision of the measurement of the signal photon is improved by the Heisenberg principle since it defines a modulated basis while reducing certainty on another basis. It is a reason why EA communication provides a greater capacity advantage in the weak signal and strong noise channel than classical communication.

Despite having the quantum channel, the entangled signal is modulated to encode classical information and is then considered as classical bits (or, in our case, when using Gaussian Modulation, we transform the TMSV state into the Gaussian state) conveying through the quantum channel.

This allows the maximum rate of reliable communication, known as classical capacity. However, there is something that has not been considered so far, which is the entanglement distribution channel, which, in the example, is a quantum noisy and lossy bosonic channel as well. This slightly changes our perspective since it is not always the case that the capacity is better with EA, it will depend on something else.

First, we will look at the case without EA, where the classical capacity is as follow:

$$C_{without\ \ EA} = g(T * N_s + N_t) - g(N_t)$$

This capacity is also known as the Holevo capacity because Holevo designed this capacity expression [54] , wherein.

$$g(x) = (x+1) * log_2(x+1) - x * log_2(x)$$

represents the entropy of a thermal state. This capacity without EA was achieved using coherent states modulated by the Gaussian method, as well as it is utilized TMSV state modulated the by Gaussian method for EA communication [49]. In both cases, coherent or TMSV states are transformed into Gaussian states, which are the keys to provide nonclassical resources in the channel, such as entanglement and squeezing states. That is why this capacity is also referred to as the quantum limit of the classical capacity. This resulting Gaussian state features the mean and the covariances of the real quadrature field.

In the example of [49], after analyzing certain covariance of the TMSV state, the covariance of the noisy thermal state, and the covariance for the zero-mean Gaussian state, it results in "symplectic eigenvalues":

$$v_{\pm} = \sqrt{\left(N_s + N_s' + 1^2 - 4T_o * T * N_s(N_s+1)\right)} \pm (N_s' - N_s)$$

Where

$$N_s' = (N_s * T_o + N_o) * T + N_t$$

and

$$N_s'' = N_s * T_o + N_o$$

We can obtain the final expression of the **EA classical capacity from [49]**:

$$C_{EA} = g(N_s) + g(N_s') - \left[g\left((v_+ - 1)/2\right) + g\left((v_- - 1)/2\right)\right]$$

This EA capacity is in the case we have an ideal receiver for EA communication, but there is no structured receiver specifically designed for EA capacity. Therefore, we consider existing detection modes used for classical capacity. For homodyne detection, the encoded information is realized in only one quadrature, and its classical capacity is given by [49]:

$$C_{hom} = 0.5 * log_2[1 + 4T * N_s/(2N_t + 1)]$$

where 4TNs represent the mean of the received photon, and 2Nt+1 is the mean of the noise photon.

Regarding the heterodyne detection, both quadrature are used for encoding, and the classical capacity that [49] give us is:

$$C_{het} = log_2[1 + T * N_s/(N_t + 1)]$$

Where TNs represents the mean of received photon and Nt+1 is the mean of noise photon per quadrature

In reality, the EA capacity has already been demonstrated considering a perfect pre-shared entanglement (without noise), and its expression [55] is as follows:

$$C_E = g(N_S) + g(N_S') - g(A_+) - g(A_-)$$

Where

$$A_{\pm} = (D - 1 \pm (N_s' - N_s)/2$$

and

$$D = \sqrt{(N_S + N_S' + 1)^2 - 4TN_s(N_s+1)}$$

Once we remark the different classical capacity expressions for each case, now we can further analyze the expression in detail, especially when taking into consideration the imperfect entanglement distribution, and determining which case the EA communication is still beneficial for classical capacity.

In this section, my goal was to analyze the previous expressions in the context of classical capacity. The expressions mentioned above are derived from the papers [49] [54] and [55] and while I may not completely understand all the aspects of the expressions or neither their origin, I aim to analyze these expressions numerically.

4.6 Simulation on Matlab

Once we have reviewed the expressions for the EA capacity in different cases, let's put them into practice using Matlab.

In every case, the noise and loss in the main channel are considered as the parameters T and Nt. However, the case we will study is when the loss and noise affect to entanglement distribution channel, which is represented by the parameters To and No. This case is referred to as the **imperfect or real case**, which will be compared to EA communication without loss and noise in the entanglement distribution channel, which will be referred to as the **perfect case**.

Additionally, we will explore three other cases where EA communication is not applied: the **Holevo capacity, the homodyne capacity, and the heterodyne capacity**.

The main goal is to study the imperfect case in comparison to the perfect, Holevo, homodyne and heterodyne cases, and determine in which aspect the real case is more optimal than the others.

It is crucial to remark that the main channel must have higher loss and noise according to [53] and [49]. This means that transmissivity in the main channel is lower than the entanglement channel ($T \leq T_o$), which implies that the number of noise photons (thermal noise) in the main channel is larger than the entanglement channel ($N_t \geq N_o$).

Thus, we use arbitrary values of transmissivity and mean noise photon number, but satisfying the previous requirement: T=0.20 , Nt=10 , To=0.50 , No=2

Firstly, we visualize these five cases depicted in Figure 17

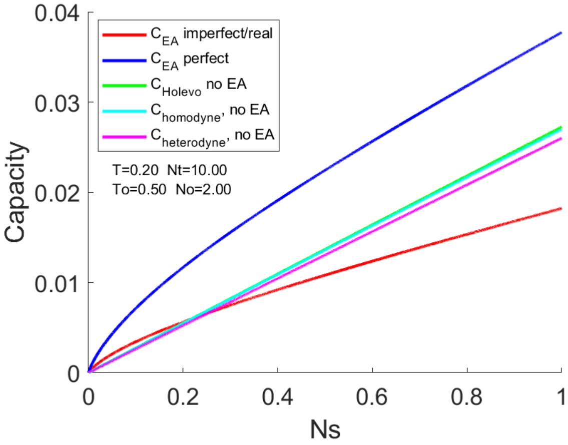


Fig. 17. *Capacity with and without EA vs. mean number of the signal photon in the main channel*

We can notably observe the difference between each capacity in the plot. The capacities achieved without Entanglement-Assisted (Holevo, homodyne, and heterodyne) follow almost the same trend, although Holevo achieves a little more capacity. However, the imperfect EA capacity provides the lowest capacity among them as the Ns increase. In fact, imperfect EA capacity just reaches a higher level of capacity at the beginning of the signal, but starting from Ns=0.22, the "no EA" capacity becomes higher.

On the other hand, if we observe the perfect EA capacity, we notice a big difference compared to the no EA capacity and imperfect EA capacity. In fact, as Ns keep increasing, the perfect EA capacity remains higher.

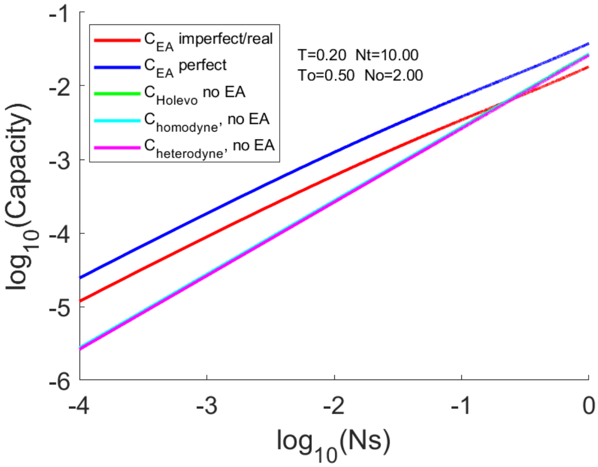


Fig. 18. *Capacity in logarithmic vs. mean number of the signal photon in logarithmic*

As we observed, the imperfect EA becomes optimal just for Ns<<1. In another perspective (Figure 18), we transform the axes to log10 scale since the values are very small.

In a nutshell, when the entanglement distribution is perfect and only the main channel has noise and loss (perfect case), the EA capacity achieves the highest classical capacity in the transmission from Alice to Bob.

On the contrary, when the entanglement distribution is performed over the noisy thermal bosonic channel (real case), the EA capacity is greatly reduced and only provides better functional capacity when Ns<<1, in other words, when the transmitter provides low brightness using single photons source.

However, we must take into account that as Ns becomes smaller, the value of capacity decreases. Hence, we cannot choose a way too small Ns.

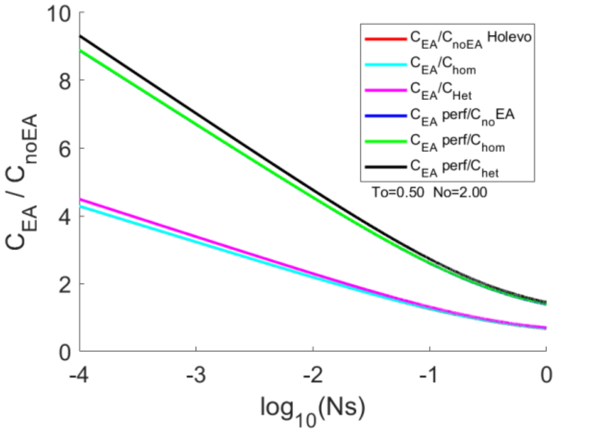


Fig. 19. I*mprovement proportion of EA Capacity compared to "no EA" vs. logarithmic mean number of the signal photon.*

For a better comparison, let's look at Figure 19.

To have an overview of the capacities, in Figure 19 we calculate the proportion of the imperfect and perfect EA capacity compared to each "no EA" capacity as a reference in order to see the percentage of improvement between them. The idea of Figure 18 and Figure 19 was borrowed from [49], but I also compare the perfect EA capacity in a standard value of T and Nt.

Indeed, when Ns is low, the imperfect EA capacity is up to 4 times better, and the perfect EA capacity can reach up to 9 times better than "no EA" capacity. However, at this high improvement, the capacity values are very small regardless.

As we can see in Figures 17, 18, and 19, the "no EA" capacities are quite similar, especially the Holevo capacity with the homodyne capacity. The heterodyne capacity is slightly lower and that is why in Figure 19 the comparison with heterodyne capacity shows a slightly higher improvement.

Now, we set a fixed value of the main channel at T=0.2 and Nt=10, while we vary the values of the entanglement distribution channel: T0 and No; starting from the perfect EA capacity (To=1 and No=0).

We note in Figure 20 that when To=1 and No=0 (perfect entanglement distribution), the capacity is identical to the perfect EA capacity. However, once the transmitivity (To) starts to decrease due to imperfections, and simultaneously the number of noise thermals (No) increases, the EA capacity decreases providing less range of functional EA capacity.

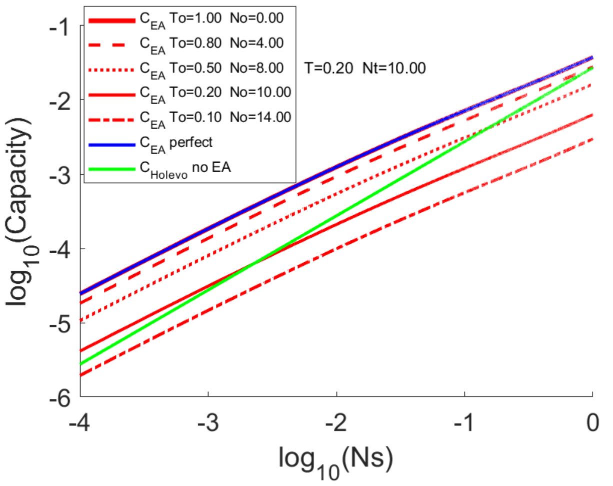


Fig. 20. *EA capacity and Holevo capacity with different characteristics (To and No) in the entanglement distribution channel. These changes do not affect the perfect EA capacity.*

In fact, when No=Nt and To=T, in other words, when both channels have the same lossy bosonic channel, we can see that the EA capacity is only higher for very less Ns and small capacity. Furthermore, when the entanglement distribution channel is more lossy and noisier than the main channel (last case of Figure 20) EA capacity will always be lower than "no EA" capacity.

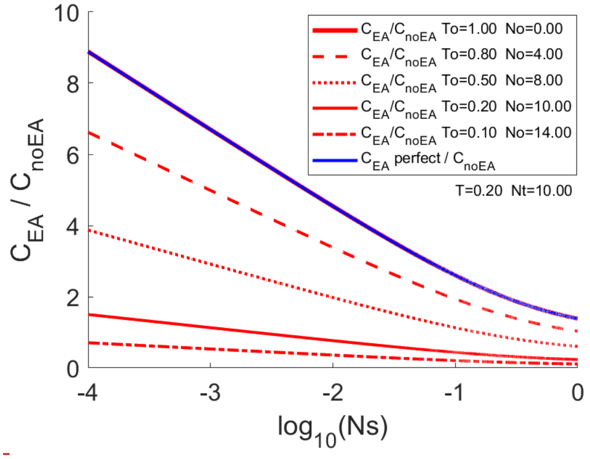


Fig. 21. *Improvement proportion of EA capacity compared to Holevo capacity, with different characteristics (To and No) in the entanglement distribution channel.*

In Figure 21 we observe the same but with improvement proportion of EA capacity compared to only Holevo capacity as a reference.

We conclude the same, the more lossy and nosier the entanglement channel, the worse the EA capacity. In fact, we observe that when the entanglement channel is noisier than maim channel, there is no improvement since it does not reach 1.

Now, we set fixed values of the entanglement channel at an intermediate value, like No=0.6 and To=2, and we vary the transmitivity (T) and mean thermal photon (Nt) at the main channel.

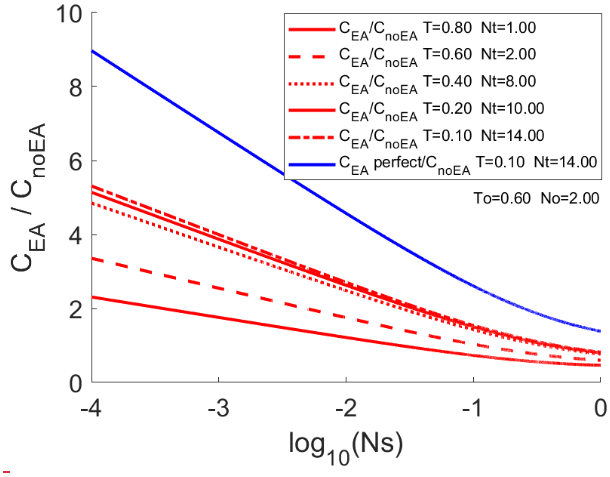


Fig. 22. *Improvement of EA capacity compared to Holevo capacity, with different characteristics (T and Nt) in the main channel.*

Hence in Figure 22, we start having more loss and noise in the entanglement channel instead of the main channel, and we observe that it exits an improvement proportion of up to 2 instead of not even reaching 1. But we should note that the variation in the main channel affects Holevo capacity as well. Hence both EA and Holevo capacity worsen their capacities as noise and loss increase, but when comparing the improvement shows a value of 2.

The second case is when both main and entanglement channels have the same noisy bosonic channel characteristics (same values of N and T). When the noise starts to further affect the main channel, the capacity proportion increases as well. But no matter how much we increase the Nt or decrease the T, it will never reach the proportion of perfect EA capacity, since this just depends on the entanglement channel.

Nevertheless, we do notice that if the main channel is noisy, it can be an advantage for the EA capacity, since we observe that the noisier the main channel is, the better results the EA capacity achieves.

4.7 Conclusion

In this study case, we analyze the Entanglement-Assisted classical capacity in the presence of imperfect shared entanglement between Alice and Bob.

If we consider perfect entanglement distribution, the EA capacity will always remain an advantage compared to the Holevo, homodyne, and heterodyne capacities. However, if we consider the same lossy and noisy bosonic channel of the main channel for the entanglement channel, the achieved imperfect EA capacity gets greatly reduced and only surpasses the "noEA" capacity for Ns<<1. This implies that the transmitter needs to send single photons for low brightness. That is why an attenuator is used before sending any photon through the main channel (figure 16). In fact, quantum communication relies on single photon sources every time since it is crucial to the confidentiality, management, and control of the qubits [56] , in applications such as QKD, teleportation, …

Unfortunately, an actual optimum receiver to achieve this EA capacity has not been completely designed.

We also observed that the improvement in EA capacity, even with imperfect entanglement distribution, is especially effective in the presence of high noise and loss in the main channel. Even within the range where the imperfect EA capacity is better, it still is viable when there is high thermal noise in the main channel: Nt>>1.

Conversely, EA communication is not appropriate for high loss in the entanglement channel, since EA capacity will never even reach the "no EA" capacity. In fact, the first condition mentioned earlier is met: $T \leq T_o$, and $N_t \geq N_o$ is a crucial requirement to employ imperfect EA capacity. If we do not meet this requirement, the entanglement distribution channel would have more noise and loss, which implies that the communication rate in the main channel is ineffective since there would be no functional entangled pairs to use. The higher the entanglement level, the more efficient transmission of information in the main channel. That is why we consider less noise in the entanglement channel since it is still possible to perform imperfect entanglement.

5. Conclusion

Throughout my work, we have seen the current state of QKD networks as the most advanced so far. However, it is proposed that entanglement networks will be the core of the future Quantum Internet. Nevertheless, further research and development are still required.

One application of entanglement networks is the boost of classical capacity, especially in bosonic channels. If the distribution of entanglement is perfect, it will provide an advantage. However, in the case of imperfect distribution, the advantage will only hold for a low number of mean photons in the transmission channel.

Even so, it is expected to implement Bell pairs for entanglement distribution, which are fully entangled states. If a future Quantum Internet can reach a high level of entanglement between two distant points, the capacity improvement for EA communication would be evident, especially for noisy and lossy channels.

Acknowledgment

I wish to thank my tutor Angeles Vasquez Castro, for her guidance and support throughout my TFG. She offered me a Matlab function that helped me understand the expressions used in the study case.
I also wish to thank Andreas Winter, who was the first contact person for my research on quantum tech and connected me with my tutor Angeles.

References

[1] C. Q. Choi, «AN IBM QUANTUM COMPUTER WILL SOON PASS THE 1,000-QUBIT MARK,» 24 December 2022. [En línea]. Available: https://spectrum.ieee.org/ibm-condor.

[2] A. Cho., «IBM promises 1000-qubit quantum computer—a milestone—by 2023,» *Science,* 15 September 2020.

[3] Angela Sara Cacciapuoti, Marcello Caleffi, Francesco Tafuri, Francesco Saverio Cataliotti, Stefano Gherardini, and Giuseppe Bianchi, «Quantum Internet: Networking Challenges in Distributed Quantum Computing,» *IEEE Network,* nº nº 0890-8044, 2020.

[4] Parisa, Surya Teja Marella and Hemanth Sai Kumar, «Introduction to Quantum Computing,» IntechOpen, 29 October 2020. [En línea]. Available: https://www.intechopen.com/chapters/73811.

[5] C. Warke, «Introduction to quantum computing part -1 Representation of qubit using Bloch sphere,» 20 March 2019. [En línea]. Available: https://medium.com/random-techpark/introduction-to-quantum-computing-part-1-representation-of-qubit-using-bloch-sphere-c6830d6ac240.

[6] S. Amyx, «Quantum Computing Series, Part 4: Superposition in Quantum Mechanics,» 20 Jul 2017. [En línea]. Available: https://medium.com/@ScottAmyx/quantum-computing-series-part-4-superposition-in-quantum-mechanics-381b98180f62.

[7] F. Zickert, «Quantum Computing is Different. The No-Cloning Theorem,» 1 Dec 2020. [En línea]. Available: https://towardsdatascience.com/quantum-computing-is-different-2178fba922cd.

[8] C. Wood, «Quantamagazine,» Pioneering Quantum Physicists Win Nobel Prize in Physics, 4 October 2022. [En línea]. Available: https://www.quantamagazine.org/pioneering-quantum-physicists-win-nobel-prize-in-physics-20221004/#:~:text=Alain%20Aspect%2C%20John%20Clauser%20and,groundbreaking%20experiments%20with%20entangled%20particles.&text=From%20left%3A%20John%20Clauser%2C%20Anton.

[9] A. Nellis, «The quantum internet, explained,» uchicacgo news, 8 Dic 2022. [En línea]. Available: https://news.uchicago.edu/explainer/quantum-internet-explained.

[10] A. Mukherjee, «Quantum Key Distribution: The Future Of Secure Communication,» 14 Jun 2022. [En línea]. Available: https://www.electronicsforu.com/technology-trends/quantum-key-distribution-future-secure-communication.

[11] MR.Asif, «Medium,» Quantum Key Distribution and BB84 Protocol, 24 Jun 2021. [En línea]. Available: https://medium.com/quantum-untangled/quantum-key-distribution-and-bb84-protocol-6f03cc6263c5.

[12] «The classical One Time Pad,» Qutech, 2019. [En línea]. Available: https://www.qutube.nl/quantum-

algorithms/the-classical-one-time-pad.

[13] G. Ribordy, «From Quantum Networks to the Quantum Internet,» IDQ, 25 March 2022. [En línea]. Available: https://www.idquantique.com/from-quantum-networks-to-the-quantum-internet/.

[14] H. Qin, «Towards large-scale quantum key distribution network and its applications,» ITU (workshop), 5 June 2019. [En línea]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019060507/Documents/Hao_Qin_Presentation.pdf.

[15] B. S. Anil Lamba, «QUANTUM CRYPTOGRAPHY (QKD) – A RESEARCH-BASED FUTURE SECURITY TECHNOLOGY,» *International Journal For Technological Research In Engineering,* vol. 5, nº 2347 - 4718, 2018.

[16] Bruno Huttner, Romain Alleaume, Eleni Diamanti, Hugo Zbinden, et la, «Long-range QKD without trusted nodes is not possible with current technology,» *Nature,* nº 108, p. 8, 9 Sep 2022.

[17] Louis Salvail, Mamtchil Peev, Eleni Diamanti, Romain Alleaume, Thomas Langer, «Security of Trusted Repeater Quantum Key,» *Cornell University,* nº 0904.4072, 2009.

[18] Fadri Grunenfelder, Alberto Boaron, Davide Rusca, Anthony Martin, Hugo Zbinden, «Performance and security of 5 GHz repetition rate polarization-based Quantum Key Distribution,» *arXiv,* vol. 2007, nº 15447, p. 5, 2020.

[19] Z. L. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, et la, «10 Mb/s quantum key distribution,» *arXiv,* vol. 1807, nº 04484, p. 7, 2018.

[20] BI-XIAO WANG, Yingqiu Mao, Lei Shen, Lei Zhang, et la, «Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber,» *Optics Express,* vol. 28, nº 9, p. 8, 2020.

[21] Teng-Yun Chen, Xiao Jiang, Shi-Biao Tang, Lei Zhou, Xiao Yuan, Hongyi Zhou, Jian Wang, Yang Liu, Luo-Kan Chen, Wei-Yue Liu, Hong-Fei Zhang, Ke Cui, Hao Liang, Xiao-Gang Li, Yingqiu Mao, Liu-Jun Wang, Si-Bo Feng, Qing Chen, Qiang Zhang, Li Li, Nai-Le Liu,, «Implementation of a 46-node quantum metropolitan area network,» *npj,* vol. 7, nº 134, 2021.

[22] Alberto Boaron, Gianluca Boso,1 Davide Rusca, Cedric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, et la, «Secure quantum key distribution over 421 km of optical fiber,» *arXiv,* vol. 1807, p. 5, 2018.

[23] M. Lucamarini, Z. L. Yuan, J. F. Dynes & A. J. Shields, «Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,» *Nature,* vol. 557, 2018.

[24] Jiu-Peng Chen, Chi Zhang, Yang Liu, Cong Jiang,v Dong-Feng Zhao, Wei-Jun Zhang,, *arXiv,* nº 11671, 2022.

[25] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, A. Tanaka, et la, «Field test of quantum key distribution in the Tokyo QKD Network,» *arXiv (Cornell University),* vol. 19, nº 11, p. 21, 2011.

[26] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, Feng-Zhi Li, Xia-Wei Chen, Li-Hua Sun, Jian-Jun Jia, Jin-Cai Wu, Xiao-Jun Jiang, Jian-Feng Wang, Yong-Mei Huang, Qiang Wang, Yi-Lin Zho, «Satellite-to-ground quantum key distribution,» *Nature,* nº 549, 2017.

[27] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, Sheng-Long Han, Qing Yu, Ken Liang, Fei Zhou, Xiao Yuan, Mei-Sheng Zhao, Tian-Yin Wang, Xiao Jiang, Liang Zhang, Wei-Yue Liu, Yang Li, «An integrated space-to-ground quantum communication network over 4,600 kilometres,» *Nature,* nº 589, 2021.

[28] Rohit K. Ramakrishnan, Aravinth Balaji Ravichandran, Ishwar Kaushik, Gopalkrishna Hegde, Srinivas Talabattula & Peter P. Rohde, «The Quantum Internet: A Hardware Review,» *Springer Link,* p. 37, 2022.

[29] Ting, Qiao Ruihong and Meng, «Research Progress Of Quantum Repeaters,» *Journal of Physics,* nº 1237, 2019.

[30] N. Yu, C. Y. Lai and L. Zhou., «Protocols for Packet Quantum Network Intercommunication,» *IEEE,* 2021.

[31] Zebo Yang, Student Member, Maede Zolanvari, Member, and Raj Jain, Life Fellow, «A Survey of Important Issues in Quantum Computing and Communications,» *IEEE,* nº 00378, 2022.

[32] S. I. Laszlo Gyongyosi, «Advances in the Quantum Internet,» *Ommunication of ACM,* 2022.

[33] Simon J Devitt, William J Munro and Kae Nemoto, «Quantum error correction for beginners,» *iopscience,* vol. 76, nº 7, 2013.

[34] Imre, Laszlo Gyongyosi & Sandor, «Opportunistic Entanglement Distribution for the Quantum Internet,» *Scientific Reports (Nature),* nº 9:2219, 2019.

[35] D. Castelvecchi, "Davide Castelvecchi. "Quantum network is step towards ultrasecure internet," *Sprinter Nature,* vol. 590, 2021.

[36] Tim van Leent, Matthias Bock, Robert Garthoff, Kai Redeker, Wei Zhang, «Long-distance distribution of atom-photon entanglement at telecom wavelenght,» *arXiv,* vol. 124, nº 3, 2019.

[37] Huayue Gu, Zhouyu Li, Rouzhou Yu, Xiaojian Wang, Jianqing Liu, «FENDI: High-Fidelity Entanglement Distribution in the Quantum Internet,» *IEEE,* vol. 2, p. 13, 2023.

[38] P. Charity, «Quantum goes the distance,»

Brookhaven, 8 April 2019. [En línea]. Available: https://www.bnl.gov/newsroom/news.php?a=214491.

[39] U. D. o. Energy, «New quantum loop provides testbed for quantum communication technology,» Argonne National Laboratory, 10 Jan 2020. [En línea]. Available: https://www.anl.gov/article/new-quantum-loop-provides-long-national-testbed-for-quantum-communication-technology.

[40] M. Fore, «Chicago expands and activates quantum network, taking steps toward a secure quantum internet,» Chicago Quantum Exchange, 16 Jun 2022. [En línea]. Available: https://chicagoquantum.org/news/chicago-expands-and-activates-quantum-network-taking-steps-toward-secure-quantum-internet.

[41] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Tuan Cao, Liang Zhang, Jian Wei Pan, et la, «Entanglement-based secure quantum cryptography over 1,120 kilometres,» *Nature,* nº 501-505, 2020.

[42] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi, Jian Wei Pan, «Satellite-Based Entanglement Distribution Over 1200 km,» *arXiv,* p. 17, 2017.

[43] Marmol, Veronica Fernandez, "Tecnologías Cuánticas y 5G || ¿Estamos listos para la nueva Infraestructura de Comunicación Cuántica Europea?," 20 Dec 2022. [Online]. Available: https://www.youtube.com/watch?v=ngfe5j16f_w&list=PLGzM5-D_mzhbs004UNehnKcdpx0O75vaD&index=16&t=2s.

[44] «Quantum Internet Alliance,» [En línea]. Available: https://quantum-internet.team/about.

[45] «IRTF,» Quantum Internet Research Group QIRG, [En línea]. Available: https://irtf.org/qirg.

[46] D. S. a. M. Bhaskar, «Announcing the AWS Center for Quantum Networking,» Amazon AWS, 21 Jun 2022. [En línea]. Available: https://aws.amazon.com/es/blogs/quantum-computing/announcing-the-aws-center-for-quantum-networking/.

[47] J. Markowsky, «Britannica,» Information theory, 25 March 2023. [En línea]. Available: https://www.britannica.com/science/information-theory/Discrete-noisy-communication-and-the-problem-of-error.

[48] J. Eisert, «Quantum information theory,» Physik, 2011.

[49] I. B. DJORDJEVIC, «On Entanglement Assisted Classical Optical Communications,» *IEEE,* p. 6, 2021.

[50] D. R. Paschotta, «Optical Heterodyne Detection,» RP Photonics, 2021. [En línea]. Available: https://www.rp-photonics.com/optical_heterodyne_detection.html.

[51] «KTH,» 2014. [En línea]. Available: https://www.kth.se/social/files/6065a79d8c7acdbcfe184f14/lecture-2.pdf.

[52] D. R. Paschotta, «RP Photonics,» Squeezed States of Light, 2022. [En línea]. Available: https://www.rp-photonics.com/squeezed_states_of_light.html.

[53] Haowei Shi, Zheshen Zhang, and Quntao Zhuang, «Practical route to entanglement-assisted communication over noisy bosonic channels,» *arXiv,* vol. 4, p. 16, 2020.

[54] Werner, A. S. Holevo and R. F., «Evaluating capacities of bosonic Gaussian channels,» *APS,* 2001.

[55] Saikat Guha, Quntao Zhuang, and Boulat Bash, «Infinite-fold enhancement in communications capacity using pre-shared entanglement,» *arXiv,* 2020.

[56] L. Zyga, «Phys.org,» Single-photon source may meet the needs of quantum communication systems, 2006. [En línea]. Available: https://phys.org/news/2006-11-single-photon-source-quantum.html.