Designing Large Quantum Key Distribution Networks via Medoid-based Algorithms *

Iván García-Cobo

Doctoral School "Studii Salamantini", Universidad de Salamanca.
C/Espejo, 2 - 37007 Salamanca, Spain.
ivangarciacobo@usal.es

Héctor D. Menéndez[1]

Computer Science Department, Middlesex University London.
Hendon Town Hall, The Burroughs, Hendon, London NW4 4BG, UK.
h.menendez@mdx.ac.uk

Abstract

The current development of quantum mechanics and its applications suppose a threat to modern cryptography as it was conceived. The abilities of quantum computers for solving complex mathematical problems, as a strong computational novelty, is the root of that risk. However, quantum technologies can also prevent this threat by leveraging quantum methods to distribute keys. This field, called Quantum Key Distribution (QKD) is growing, although it still needs more physical basics to become a reality as popular as the Internet. This work proposes a novel methodology that leverages medoid-based clustering techniques to design quantum key distribution networks on commercial fiber optics systems. Our methodology focuses on the current limitations of these communication systems, their error loss and how trusted repeaters can lead to achieve a proper communication with the current technology. We adapt our model to the current data on a wide territory covering an area of almost 100,000 km^2, and prove that considering physical limitations of around 45km with 3.1 error

*Dedicated to the memory of Miltos Petridis, head of the Computer Science Department of Middlesex University London and one of the few people who understood how to give support to researchers. We gratefully acknowledge the support of NVIDIA Corporation with the donation of the Titan V GPU used for this research.

[1]Corresponding Author

loss, our design can provide service to the whole area. This technique is the first to extend the state of the art network's design, that is focused on up to 10 nodes, to networks dealing with more than 200 nodes.
Keywords: Quantum Key Distribution, Medoids, Trusted Repeater QKD, Quantum Network, Partition Around Medoids

1. Introduction

One of the main theoretical challenges facing modern cryptography is its vulnerability to future quantum computers. According to Shor's algorithm [1], once quantum computers raise, most public key encryption algorithms will be decrypted in linear time. This is a major problem, not only affecting secure communication, but also protecting data - both future and current - bearing in mind that encrypted data can be stored.

To face the threats that quantum computing proffers over classical cryptography, we can use applications of quantum mechanics itself to implement new solutions. Quantum cryptography allows us to design algorithms that, on the one hand, manage to overcome the limitations of classical physics [2] and, on the other hand, are not vulnerable to attacks from quantum computers [3]. These protocols are based on sending and measuring light polarization on a fiber optic channel [4]. However, one of the main problems associated with these algorithms is the distribution of the so-called quantum keys, given their physical properties.

There are numerous successful experiments on quantum communication for sending keys at distances above 100 km on fiber optic channels such as those found in [4]. However, a realistic commercial environment requires distances below 50 km based on experiences [5] that can demonstrate that, at such distances with current commercial equipment (such as those manufactured by the company ID Quantique SA), the achieved results are remarkable [2].

[2]This device allows to exchange about 20,000 quantum keys in an hour [6].

Our main goal is to propose a novel methodology to create a distribution network of quantum keys that allows to provide service over a fiber optic network on a given territory (Section 4). The main problem of our network is to decide whether it is possible to set trusted repeaters on the quantum key distribution process, as those proposed by Salvail et al. [7], considering the current features of the provided fiber optic network (Section 2). To this end, this work focuses on a fibre optic network of a commercial operator on the territory of Castilla y León, Spain (Section 5.1). With this information, we propose a methodology based on clustering algorithms to minimize the number of quantum key repeaters on that specific territory, so our methodology does not only create the distribution network but also optimizes it. For the sake of the authors, this is the first work focused on designing large networks and distributing the repeaters inside the networks. With this approach we can extend the current networks, whose size is up to 10 nodes (Section 7) to networks with more than 200 nodes (Section 5).

In order to evaluate this methodology, a series of experiments have been carried out that simulate, on the aforementioned territory, how to create this distribution network (Section 5). In this case, two maximum distances between repeaters based on distances below 50 km have been considered. The first maximum distance is 35 km, and the second 45 km. These distance are boundaries for the theoretical and modulation error of the fiber optic channel (Section 3). The results show that for a network with a limit distance of 35 km, the entire territory of Castilla y León can be served using 100 repeaters. However, it is necessary to place a minimum of five repeaters outside the fiber optic service areas. In the case of a maximum distance of 45 km, it would suffice to use the available network by docking 100 repeaters on it. This would ensure secure communications using quantum encryption over all of Castilla y León, a territory that currently occupies 100,000 km^2 (Section 6).

For reproducibility porposes, we have published the data and the code for the experiments[3].

2. Quantum Communication Protocols and BB84

Quantum key distribution (QKD) mainly makes use of two large families of protocols [8]. These algorithms are based on the transmission of qubits: BB84 and B92. Other families, like E91, work on linked pairs.

The BB84 protocol is considered to be the first quantum key distribution protocol. It was proposed by Bennett and Brassard in 1984 [9]. It is an application of quantum properties. In this protocol four states and two alphabets are used, each of which with two states.

To explain the BB84 protocol, we are going to consider that there is a message exchange between Bob and Alice. Both interlocutors are connected through two communication channels. One quantum and one conventional. When we refer to someone trying to intercept the messages, we will refer to Eve. We also assume that the conventional channel is authenticated so that no spy can perform attacks of impersonation or modifications to the message (integrity). However, Eve can, according to the laws of quantum physics, try to read from the quantum channel, although this will modify the message [9]. Algorithm (1) describes the protocol behaviour.

We will consider a Vernam cipher applied to the encoding and decoding of the message, i.e., the key and the message are considered as vectors of numbers, character by character, and they are added to create the encoded message and subtracted to decode the message [10]. The BB84 protocol creates and exchanges the secure key.

First, Alice will write the message that she wants to transmit and she will transcribe it as a sequence of 0s and 1s. BB84 generates a key of the same size (or larger) as the message to be transmitted. To do this, Alice generates a random sequence of 0s and 1s. Alice will choose the alphabet in which she will

[3]https://github.com/hdg7/QKDNetworks.

Algorithm 1 Protocol BB84 based on 4 quantum states

Alphabet z**:** $\{|0\rangle, |1\rangle\}$

Alphabet x**:** $\{|+\rangle, |-\rangle\}$

1: Alice generates a sequence of random values of zeros and ones that corresponds with the key she wants to exchange with Bob.
2: Alice generates another random sequence, now with the bases she will use for encoding of the key generated in the previous step.
3: For each bit generated, Alice performs the following action: if the bit is zero, Alice codifies it by randomly choosing between $|0\rangle$ (alphabet-z) and $|+\rangle$ (alphabet-x). If the bit is one, she encodes it uniformly at random between $|1\rangle$ (alphabet-z) and $|-\rangle$ (alphabet-x).
4: Alice sends the sequence of qubits to Bob.
5: Bob generates a random sequence with the bases that he uses to decode the sequence of states received from Alice.
6: Bob measures each received state in the base corresponding to the generated sequence.
7: Bob sends Alice the sequence of bases used through an authenticated public channel.
8: Alice compares the sequence of bases used for the key encoding with the sequence provided by Bob in the previous step, remaining only with those measurements for which both bases have coincided.
9: Alice and Bob share a sequence of values formed by those in which the positions where the bases of preparation and measurement have coincided.
10: After the previous points there is a subsequent process aimed at estimating the presence of a spy, correcting errors, and amplifying privacy.

transmit (z or x). Then, she follows the rest of the steps of the BB84 protocol to exchange the key (Algorithm 1). It is important to remark that, in the last step of the BB84 algorithm, the values that do not coincide are discarded.

Once both share a secure single-use key, the message is encoded with that key by Alice and sent it to Bob. He, upon receiving it, will make the binary sum with the key that Alice had previously transferred to him to discover the original text.

After executing the algorithm, and once the key has been generated by BB84, Alice will use the key to encode every new message. Bob will then be able to decode the messages with this shared key. The security is guaranteed because the creation and transmission of the key are based on the fundamentals of quantum mechanics. The presence of a potential spy (Eve) could compromise the exchange of the key, because if she measures the channel, she will produce a state change. However, the security of the protocol lies in the fact that it uses two alphabets with non-orthogonal states, Eve cannot simultaneously measure the polarization on x and on z for the same qubit.

3. Quantum Key Distribution on Networks

Currently, there are different works that aim to implement the distribution of quantum keys through commercial channels [4]. In this work, we aim to construct on the state of the art, focusing on creating an optimum network on commercial optical fiber. Our system aims to optimize the number of repeaters needed on the network based on a known infrastructure.

The fiber optic implementation does not use light polarization as it could be done for high speed systems designed for short distances or laboratories. On the other hand, we consider phase-coding techniques. Moreover, at present, the technology for emitting single photons is not commercially mature, so we consider very attenuated laser pulses [11].

There are two fundamental problems affecting the transmission of photons. The first one refers to the physical properties of the fiber channel itself. Fibre optics is not an ideal channel, so it absorbs part of the photons it tries to transmit. The other problem lies in the receivers, in our case the repeaters [7], located at the ends of the channel: these receivers need a recovery time between the arrest of one photon and the next.

The length of the transmitted wavelength directly affects the quality of the transmission itself. In such a way that the material in which the channel itself is built - the optical fibre - has an absorption probability that varies depending on the wavelength that is transmitted through this channel. The *color* of light is therefore the basis for how much will be lost during transmission. Evidently, the distance -length of the fiber- makes the loss greater as it increases. Starting from a certain distance that cannot be modified –distance to which we want the communication to occur–, the transmission can only be improved by using materials that offer less absorption and/or wavelengths that, in a given material, represent a lower rate of absorption in its transmission. Therefore, if the distance is known, the fiber to be used is already implemented, hence we only have the variable relative to the frequency of light to be transmitted.

As an example, three of the most outstanding relatively recent solutions are currently highlighted:

- In 2017, Toshiba launched a commercial solution for distributing key information at a speed of 13.7 megabits per second [12]. This distribution capacity surpasses any current system, achieving speed improvements up to seven times more powerful than its 1.9Mbps systems developed in 2016.

- In 2006, Hiskett et al. [13] developed a system that extended the distribution of quantum keys to long-distances, in their solution, distances greater than 50 km. These systems are based on ultra-low-noise transition-edge sensors (TESs). These systems were capable of exchanging keys at distances of 67.5 km.

- In 2012, Patel et al. [14] created a system based on the temporary filtering effect to reject noisy photons. It achieved high bidirectional transmission ratio up to Gb/s. This system is capable of transmitting over fiber optics

Fiber Length	Measurement	Theoretical Error (ET)	ET + Mod. Error
0-10 Km	3.6%	0%	3.1%
10-20 Km	3.4%	0%	3.1%
20-30 Km	3.1%	0%	3.1%
30-40 Km	3.5%	0%	3.1%
40-50 Km	3.4%	0%	3.1%
60-70 Km	3.5%	0.2%	3.3%
70-80 Km	5.1%	0.6%	3.7%
80-90 Km	4.0%	1.2%	4.3%
90-100 Km	6.2%	1.7%	4.8%
100-105 Km	7.3%	2.0%	5.0%
105-110 Km	6.9%	2.4%	5.2%
115-120 Km	8.1%	3.1%	6.0%
120-125 Km	8.9%	3.9%	7.0%

Table 1: Quantum error at bit level (Quantum Bit Error or QBER) in percentage to fibre length, extracted from the works of Gobby et al. [15].

.

up to 90 km away. It is one of the systems closest to large-scale transmission.

Apart from these solutions, several papers by Gobby et al. [15] have studied both theoretically and experimentally the efficiency of fiber optic communications with respect to bit-level quantum error in communications. The most relevant results regarding the relationship between distance and error can be found in Table 1. It can be seen, especially in the theoretical error, that from 50 km the growth of the error begins to play a significant role. This information will be used later in the experimental design of this work to establish physical limits of quantum communication (see Section 5.2).

4. Medoid-based Quantum Key Distribution Network

Our methodology employs an existing fiber optic network to create a QKD network on its infrastructure. This requires two main steps: 1) select which nodes of the network will act as repeaters and, 2) optimize the number of repeaters as they are the new infrastructures that need to be added. Considering how fiber optic networks distribute around localities, we consider a municipality as a potential place to set a repeater and, over a given map, our methodology will find those municipalities that are best candidates to host repeaters.

When addressing the problem of repeater distribution, we uses a methodology based on grouping municipalities through a k-medoids algorithm (Section 4.2.1). This algorithm will help, given a set of municipalities, to select those that are physically close to each other. The algorithm will then facilitate the selection of the most central municipality within the set of nearby municipalities. This municipality will be considered as a candidate, within the set, to host a repeater. The methodology, finally, will try to connect the possible repeaters among them to generate a distribution network.

This type of problem is similar to the Travelling Salesman Problem, where the most optimal route has to be selected for a traveller who intends to cover a certain set of places. In this case, "the traveller" would correspond to the set of quantum keys, and "the places" would correspond to the municipalities. The traveller's problem is NP-complete [16], and requires approximation methods in order to find local solutions. Inspired by state of the art solutions applied in this scenario, this paper addresses the problem of creating a quantum key distribution network on two levels. First, a local solution will be sought that reduces the number of municipalities and simplifies the network to a fixed number of repeaters. The distances between them will then be measured in order to generate a communication network between them.

4.1. Basic Network of Municipalities

When selecting municipalities as potential candidates for repeater placement, it is important to bear two factors in mind: the selected municipality must have the rest of the municipalities in its group within the range of distances required in quantum key distribution, and the representative municipality of the group must have, at least, one other representative municipality within the limit distance in order to generate the distribution network.

The first part of the algorithm focuses on finding these representative elements. Considering $X = \{x_1, \ldots, x_n\}$ the set of all potential municipalities, this first part is divided into the following steps:

1. Select the maximum distance D between network repeaters.
2. Calculate the distance matrix $d(\cdot, \cdot)$ for all potential municipalities. This distance matrix can be defined in many possible ways, since the algorithm will not require the metric itself. In Section 5.1, the experiments use the geodetic distance based on the GPS coordinates of municipalities.
3. Select an initial number of repeaters k.
4. Select an initial random set of repeaters $m_1, \ldots, m_k \in X$ following a uniform distribution.
5. Apply the Partition Around Medoids algorithm (Section 4.2.1) to extract a final list of m_j^* repeaters that are a solution to the optimization process.
6. Evaluate each group c_j associated to each repeater to check that for all $x_i \in c_j$, $d(x_i, m_j^*) < D$.
7. If this last condition is not satisfied, increase k and repeat steps 4 to 7.

To understand how this grouping methodology is performed, the following section outlines how to apply the grouping or clustering algorithm to municipalities data.

4.2. Using Clustering to Identify Representative Municipalities

The problem of distribution of quantum keys over a given population requires not only to know the physical limits established by communication between nodes, but also specific methodologies that allow for optimum positioning of repeaters. For this second part our methodology applies clustering, a known unsupervised automatic learning technique [17].

Given a data set $X = \{x_1, \ldots, x_n\}$ where n represents the cardinality of the set –or the total number of elements–, a clustering algorithm divides this set into k groups, or clusters c_j, where $C = \{c_1, \ldots, c_k\}$ represents the total set of clusters [17]. This division is unsupervised, referring to the algorithm's ability to separate data without using any supervised information – usually provided by an expert in the data set – to measure the quality of clusters during the discrimination process. A clustering algorithm only uses a cost function that it tries to minimize, based on the data's own characteristics.

The selection of the cost function is fundamental, not only because it defines the grouping criterion, but also because it will facilitate or hinder the algorithm optimization process. Originally, these functions start from a distance that they try to minimize. The most frequently used distance is the Euclidean distance between each cluster element and its centroid v_j. Thus, a clustering algorithm must find the discrimination that best minimizes this distance for each element and cluster [18]. Formally, the cost function is defined as:

$$J = \sum_{x_i \in X} \min_{v_j \in C} ||x_i - v_j|| \tag{1}$$

In this case, a centroid is defined as the expectation or equidistant distance of all the points of a cluster. This is calculated as:

$$v_j = \frac{1}{|c_j|} \sum_{x_i \in c_j} x_i \tag{2}$$

The best-known clustering algorithm, k-means [18], tries to reduce these distances using an iterative process. Given a fixed number of clusters, k, and assuming that the centroids v_j acquire random values at the beginning of the execution of the algorithm, the process successively performs the following two steps:

1. Assign the x_i points to the nearest centroid.
2. Recalculate the centroids.

One of the main problems with clustering algorithms is finding the optimal number of clusters, k [19]. The choice of this value depends as much on the criteria to be satisfied with the grouping as on the metrics used by the algorithm. In the first case, the analyst decides this value. In the second case, the value is decided through a metric that measures the quality of the clusters. This quality can be measured individually, for example, through a quadratic distance [18];

or collectively, through, for example, the Silhouette [20] or the Dunn Index [21].

Although these clustering techniques generalize the way clustering is usually applied, there are several other varieties of clustering that endorse graph theory [22, 23, 24], bio-inspired algorithms [25, 26, 27, 28], and big data methods [29, 30, 31]. Also, it has multiple applications to several fields, for instance, behavioural models [32, 33], malware analysis [34, 35], social network analysis [36, 37], biomedicine [38, 39], and marketing [40, 41, 42]. In this work, clustering will be applied in order to group municipalities by distance, in such a way that it can be determined in which places quantum key repeaters should be placed. The clustering algorithm will be used to select positions for the repeaters optimally, with the aim of minimizing them while maximizing the connections between them. Each repeater will correspond to one cluster, and the number of repeaters to the number of clusters. However, given that we want to choose the municipality to place the repeaters within the possible municipalities, we can not use a centroid-based strategy. The use of centroids would cause some repeaters to be in marine or inaccessible areas. To correct this potential problem, a clustering strategy based on medoids will be used.

4.2.1. PAM: Partition Around Medoids

Partition Around Medoids, or k-medoids [43], is a variation of k-means where, instead of using centroids, the selected element is the best, within the cluster, minimizing the cost function. In this way, there is a slight modification in the cost function, where:

$$J = \sum_{x_i \in X} \min_{m_j \in X|_{c_j \in C}} d(x_i, m_j) \tag{3}$$

In this case, the optimization follows two directions: the selection of the cluster and the selection of a representative element within it or medoid. The possibility of choosing an element of the cluster avoids the need to use a metric space or, specifically, an Euclidean space. It is enough to define a matrix of distance d between all the elements of X. In equation 3, $d(\cdot, \cdot)$ describes this distance between two elements belonging to X. Thus, since the optimization process only needs information about the distance, and not how to calculate it, there is no need to describe the distance itself.

PAM facilitates the selection of representative municipalities within the municipalities to be connected through the quantum key distribution network, and ensures connectivity between these municipalities and all municipalities belonging to the same cluster. It is still necessary to create a network between the representative municipalities in order to carry out the distribution of quantum keys.

4.3. Repeater's Network

In order to ensure that any municipality within the network can communicate with any other municipality, it is necessary to establish a network of repeaters based on the representative municipalities selected in the previous step. This network will be defined as follows:

1. Each representative municipality will be connected to all the municipalities in its cluster. In this way, all municipalities in the same cluster will be able to exchange quantum keys using the repeater. The previous step ensures that the repeater is less than D km away from each municipality in its cluster.
2. Each repeater will connect with all the repeaters in its environment that are at a distance less than D. In this way, if there is more than one repeater near to another, different routing can be used to reduce the saturation of the key distribution.

These criteria when creating the network not only facilitates better routing, but also makes it easy to identify possible regions isolated from the network. In order to find these regions, it is sufficient to calculate the number of connected components of the network. Formally, the network is a non-directed graph G, divided into vertices V, representing municipalities, and edges E representing those municipalities that are either within a cluster and connected to its repeater, or are repeaters at a distance smaller than D. In this way, the number of connected components of the graph can be calculated in several ways, where the most representative are the multiplicity of its eigen-values, or estimation using random paths [44]. This work uses the second (see Section 5.1). If the number of connected components of the graph is 1, the network is fully connected. Otherwise, the following strategies can be used:

1. Search for intermediate locations between municipalities to place repeaters that reduce the distance between two known repeaters.
2. Increase the number of initial repeaters and re-generate the groupings of municipalities in the first step.
3. Sacrifice part of the quality of key communication, increasing the distance between repeaters.

In the following sections of the work, we simulate, in a practical way, how to generate this type of networks over a known area, taking into account the special cases mentioned above. Besides, it is shown how the distance D, considered in the state of the art of quantum key distribution, could be feasible for specific regions and what kind of measures to take in case of finding isolated regions.

4.4. Complete Algorithm Flow

The complete process flow for creating quantum key distribution networks is summarized in Algorithm 2. This algorithm only needs the coordinates of the different municipalities that will be considered (X) as input data, and a limit distance that will be used to verify that the municipalities comply with the physical restrictions D.

The algorithm starts by defining the array of distances $d(\cdot,\cdot)$ between each pair of data $x_i, x_j \in X$. Since this matrix is symmetrical and its diagonal is 0, by the definition of distance, it is enough to define only its triangular matrix. Once the matrix is defined, the two general steps will be carried out.

The first step starts by setting the initial value of k to 2 (lines 2 and 5). The value of k represents both the number of clusters for the clustering algorithm

Algorithm 2 Quantum Key Distribution Algorithm

Entry: D: Limit physical distance
X: List of municipalities coordinates data

Output: C: Cluster of municipalities
R: Repeater list
G: Network Graph

1: Define $d(\cdot,\cdot)$, the matrix of geographical distances between municipalities, for all par $x_i, x_j \in X$, such that $x_i \neq x_j$.
2: $k = 1$
3: **repeat**
4:     **repeat**
5:         k++
6:         C=PAM($d(\cdot,\cdot)$,k)
7:     **until** (($k \geq |X|$) **OR** (verifyDistance(C,D)== **TRUE**)
8:     R=extractMedoids(C)
9:     G=graphDistanceLimit(R,D)
10: **until** (isConnected(G) == **TRUE**))
11: annexClusters(G, C)
12: **return** C, R, G

(Section 4.2), and the number of repeaters that will finally be selected. The PAM algorithm (line 6) is applied, which groups the data into clusters based on distances. The value of k is increased to continue the loop (line 5), which iterates until it obtains a group discrimination that guarantees that the distances between each representative element –or medoids– of each cluster is at a distance less than D with respect to the rest of elements. This is verified in the loop condition with the verifyDistance function (line 7). If this distance cannot be guaranteed, the algorithm will continue until a cluster is assigned to each element.

If the distance is satisfied, the repeaters' list, R, is extracted from the k representative elements of C (line 8). These elements are then used to build the repeater's network G (line 9). This network is constructed in the following way: the repeaters act as network nodes, and the D distance is used to decide which connections need to be set. If two nodes are physically closer than D, there will be a connection between them. Once the network has been created, the main objective is to guarantee its connectivity, i.e. that it has only one connected component (Section 4.3). If this happens, the network is ready (line 10), it is only necessary to connect the rest of nodes, i.e. the non-representative elements of the clusters (or non-repeaters) to the network (line 11). If this does not happen, the number of repeaters is increased again (line 5), and the execution continues. The result will be a fully connected G network.

5. Experiments

In order to understand the effectiveness of the proposed method for creating a quantum key distribution network, this part performs two simulations on a known territory, in this case Castilla y León. The simulations aim to test the effectiveness of the method and to show how it can be used in a practical way to create a network from scratch in a selected territory.

5.1. Experimental Setup

In order to carry out the experiments, we chose municipalities in Castilla y León with a population of at least 1,000 inhabitants as the data set. These are considered within the plans of Telefónica[4], a Spanish multinational supplier of commercial fibre optics. From the 2,248 municipalities in Castilla y León identified, only 267 comply with the population restriction [5]. This limits the number of repeaters in the experimentation. In order to be able to measure quality, our experiments create different networks between 10 and 250 repeaters.

Although the works of Gobby et al. [15] manage to obtain a distribution of quantum keys over fibre of up to 100 km distance, under the BB84 protocol (see Section 2), the approximate error rate obtained by these authors is around 9% (see Table 1, in the Section 3). For that reason, this simulation uses more conservative approaches when creating the distribution network. According to the work of Gaya et al. [45] on the same protocol, conservative limits are established for the secure transmission of keys between 30 and 50 km. According

[4] `https://www.telefonica.com/es/web/sala-de-prensa/-/telefonica-llevara-la-fibra-al-97-de-los-hogares-en-2020`
[5] Population data obtained from the INE

to these data, a first simulation will be performed considering several potential levels for D (the key communication limit distance) that fall in the 20 to 100 km distance range. Besides, considering the conservative limits, a second experiment has been carried out with two representative mean distances within them: 35km and 45km.

The implementation of the PAM algorithm used has been extracted from the package `cluster` of R[6]. The values of k vary according to the number of repeaters, although all other values of the algorithm have been set by default. The distance metric used was the geographical distance obtained from the GPS positions of the municipalities data set. This distance has been calculated using the R[7] `geosphere` package. For the last part, which calculates the number of related components of the repeater network, the R[8] `igraph` package based on random paths has been used.

5.2. Results

Two experiments have been carried out to measure the quality of the networks in relation to the number of repeaters. In the first case, the limit distance is considered as a parameter and is manipulated together with the number of repeaters. The second case fixes the limit distance, considering two conservative distances, and measures the quality of the network for these distances, specifically, 35 and 45 km.

Figures 1 and 2 show the result of the first experiment. This establishes a grid of distances and number of repeaters that varies between 20 and 100 km for the distances and between 10 and 250 for the repeaters. The main objective of the experiment is to check at which points the entire network is connected, i.e. when the number of connected components of the graph is 1 (see Section 4). The lighter blue of the figures represents the lowest number of components, in this results, a single component. This assumes that service can be provided

[6] `https://cran.r-project.org/web/packages/cluster/index.html`
[7] `https://cran.r-project.org/web/packages/geosphere/index.html`
[8] `https://cran.r-project.org/web/packages/igraph/index.html`

to all municipalities without leaving anyone isolated within the distance ranges established in the state of the art. As it can be seen in both figures, the optimum values of distance would have to be located from 80Km in order to place the least number of possible repeaters (between 10 and 20), however, for distances around 40 km, about 100 repeaters are enough to create the connected network.

When the distance limit falls below 40 kilometres, Figure 2 shows an asymptotic behaviour. In these cases, the algorithm is not able to find a discrimination of repeaters that allows to generate a complete network. It is necessary to place extra repeaters in unpopulated areas in order to complement the service. This phenomenon is most clearly seen in the second experiment.

The second experiment focuses on the state of the art distances: 35 and 45 km. In these cases, represented in Figure 3, the number of related components increases at first. This phenomenon is due to the fact that the clusters have not succeeded in having their internal elements satisfying the D limit distance. This is solved from 50 repeaters in the case of 35km; and 25 repeaters in the case of 45km. In both cases, all clusters satisfy the distance limit (Section 4.1).

For 35 km, it is not possible to get a fully connected network (Figure 3). The components reach an asymptotic behavior in 5 components. From 100 repeaters, 4 of them remain disconnected, and they are connected between them when their number increases, but they are not connected to the main network. These places, as discussed in Section 4.3, could be discarded, annexed through intermediate repeaters or reduce the quality of communication, increasing the limit distance at those particular points, however, the rest of municipalities (specifically 260) would be connected. The municipalities disconnected from the network formed in Castilla y León are 7: 3 of them in Soria, specifically Ágreda, Arcos de Jalón and Ólvega; and 4 of them in Zamora, specifically Alcañices, Galende, Puebla de Sanabria and Trabazos.

The 45 km experiment (see Figure 3) shows more positive results in generating a fully connected network, since it is generated from 100 repeaters. This proves that any quantum key distribution system using at least this type of limit distance can serve all municipalities in Castilla y León that currently fall

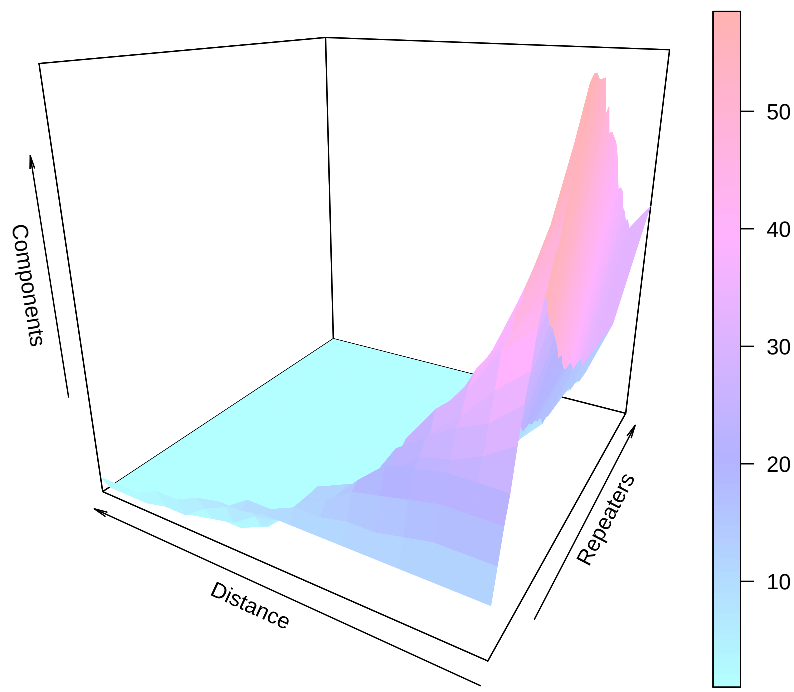

Figure 1: Experimental results considering the two variables of the experiment: the limit distance of the repeaters (D) and the number of repeaters (k). The graph shows the number of connected components that the network has for different values of these parameters. It can be seen that the predominant value is 1 component in most cases, so the network would be connected.

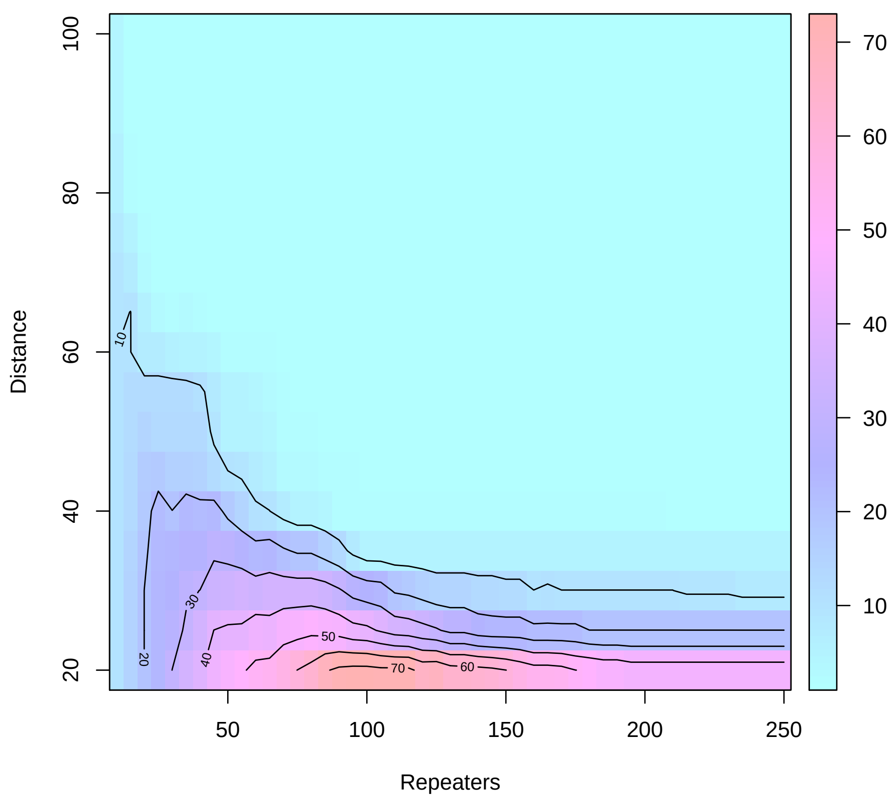

Figure 2: This plot fixes the view of Figure 1 to a given plane and analyzes the contours of the various limits on the number of repeaters relative to the distance.

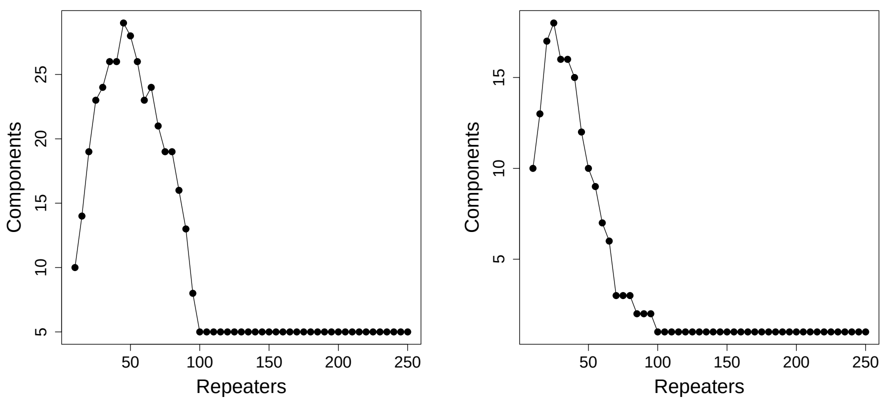

Figure 3: Considering the D distance limit of about 35Km (left), there is an asymptotic behavior in the number of connected components from 100 repeaters. The components do not fall below 5. Considering the distance limit D of about 45Km (right), it can be seen that the connected network is reached from 100 repeaters.

within Telefónica's fibre optic potential range.

Considering the experimental results and the state of the art, it can be seen that it is possible to generate a quantum key distribution network to serve Castilla y León, a territory that covers 94,226 km^2. The next section discusses these results, showing what a potential network based on the proposed algorithm would look like.

6. Discussion

During the experimentation of the previous section, it is shown how the proposed method for creating a quantum key distribution network is able not only to create the network with respect to the parameters established within the physical limitations of the problem, but also to optimize the distribution of repeaters within the network.

In order to visualise the effects of this selection, we have analysed the municipalities in detail. Figure 4 shows all the municipalities of Castilla y León considered for the experiment constraint to a population of 1,000 people. As explained above, these municipalities have the potential to form part of Telefónica's fibre

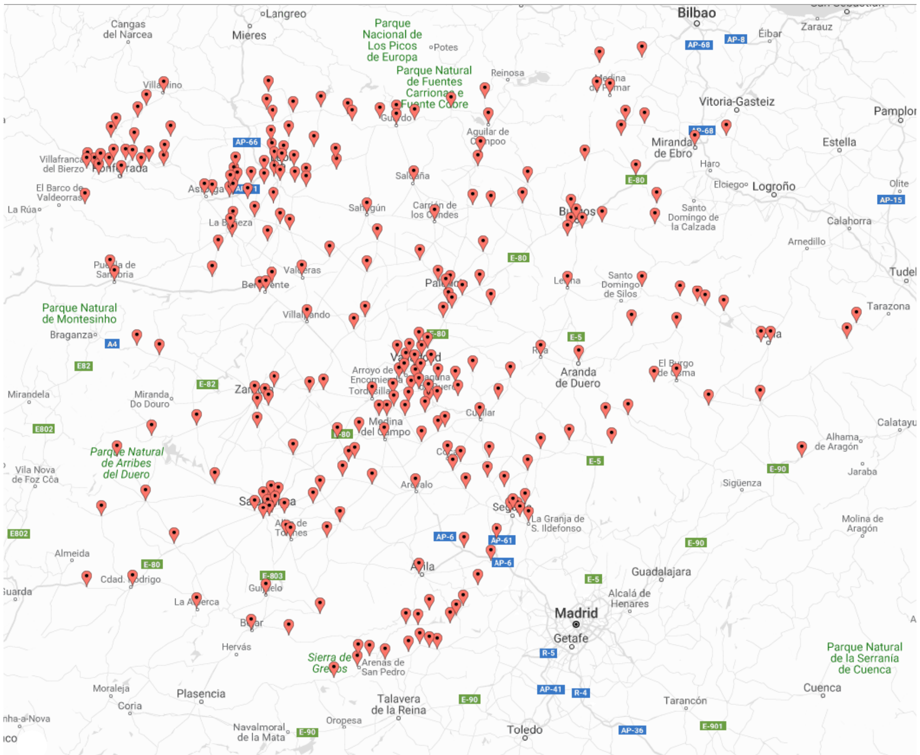

Figure 4: Municipalities of Castilla y León with more than 1,000 inhabitants that have been used during experimentation.

optic networks, where the keys would be distributed. Two effects can be seen in the figure: there are several areas with many nearby municipalities and, at the same time, there are also several isolated points. These isolated points would explain both the high number of repeaters needed and the problem encountered when trying to apply a limit distance of 35 km.

In order to understand the final decisions of the algorithm, Figure 5 shows the position of the repeaters for the experiment with a limit distance of 45 km. These results show how a few repeaters can be placed to serve the areas of higher concentration, while at the points of lower concentration it is necessary to place a repeater directly. Considering the five isolated municipalities is the 35 km experiment, it is enough to see on the map that only a few intermediate

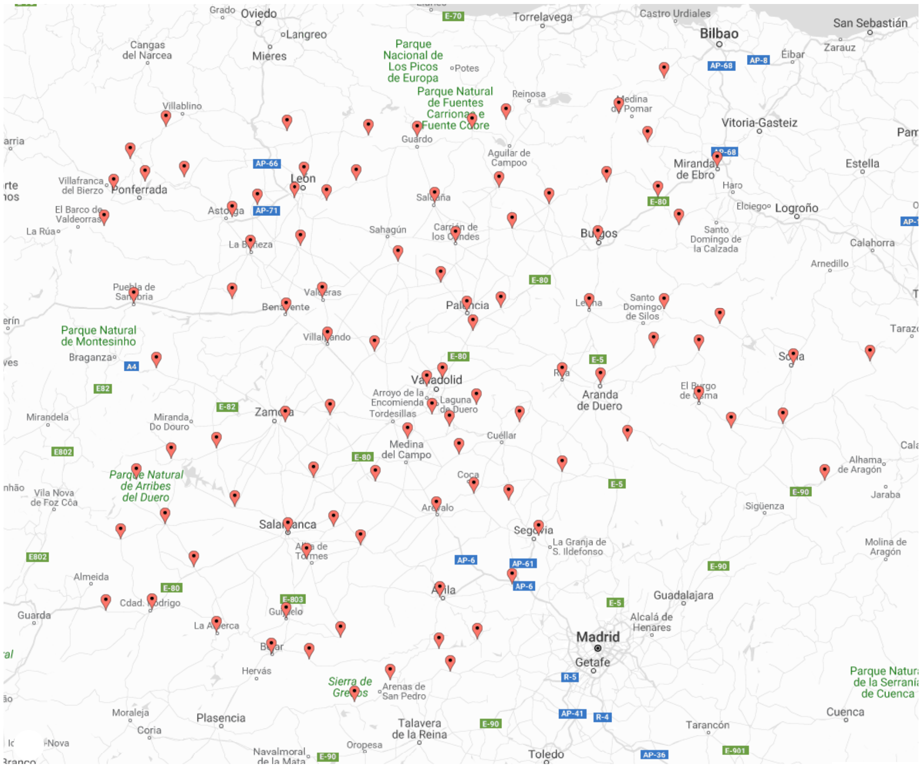

Figure 5: Municipalities of Castilla y León selected by the distribution algorithm to host quantum key repeaters. These one hundred municipalities would complete the network by associating the municipalities of the Figure 4

.

repeaters would be needed, given that these are in the most border areas of the regions considered.

If the results of Gobby et al. [15] were considered, this network could be significantly simplified. Taking into account the results of Experiment 1 (Section 5.2), from 100 km, it is enough to place about 10 repeaters in the whole area of Castilla y León. However, as mentioned in the Section 5.1, the error rate of 9% would mean a cost in the service's quality, the impact of which cannot be measured through simulations. Considering that these networks must provide keys on Internet services in a high population (according to the INE of about 2.5 million inhabitants), it is better to use more conservative limits that the same authors established at 50.6 Km [5], with the guarantee that the error would be limited to 5%.

Apart from the results obtained by the quantum key distribution network creation system, one of the main advantages of the algorithm introduced in this work (Section 4) is its ability to find this selection in a totally unsupervised way, i.e. without requiring any human feedback in the process. As a consequence, either to extend the network or to create a new one in other regions of Spain, it is enough to provide a new list of municipalities. The algorithm will be able to start from this list to obtain another network that will allow a new distribution to be generated without any added effort.

In addition, the algorithm is based only on the distances entered as boundary distances and on the population map, so it is agnostic of the communication protocol used, as long as it has information on its physical limits. This allows to use different communication protocols in different areas to create networks depending on the established demands. In order to extend the network and make it more secure, our algorithm can serve as an input for secure network algorithms, such as the one proposed by Zhou et al. [46], which designs the communication scheme of a given network to guarantee security while reducing the number of intermediate nodes. Their algorithm also design key management and data scheduling schemes to optimize data transmission. Our approach can geographically set a basic network while the approach of Zhou et al. can provide relevant tune-ups to make the network secure. This indeed can extend the algorithm providing an initial solution from our algorithm and using the method proposed by the authors to optimize the connection and the positions of the repeaters locally. Although we will explore this possibility in future work, our algorithms could join following the steps below:

1. Select a region in the map and the municipalities that have fiber optics providers and need to be part of the QKD network.
2. Apply the medoids algorithm having into account the distance to find the initial repeater's position.

3. Based on the medoids, apply Zhou et al.'s algorithm setting weights to the local network and recalculate the position of the medoids based on the Lyapunov network optimization technique [47]. This will also improve the communications of the basic network which is something that our algorithm is not considering at the moment. Providing the first solution will reduce the effort of the Lyapunov optimization process as it would be performed locally.
4. Connect the local areas of the network to provide the general network and measure the components to guarantee the connectivity.

With this idea we could also create a secure network over a given population automatically.

It is important to recall that the main differences between classical networks and QKD networks are the communication physics (Section 3) and the protocols to guarantee a secure communication (Section 2). Moreover, the methods for wireless communication networks normally take into consideration the numbers of users that they need to serve, which is something unknown at the moment for the QKD technology, although we are currently exploring this point by measuring the message exchange rates that different amounts of users can generate, and adjusting it to the current known technology, including the error rates in the exchange of messages. We can see similarities between the network construction processes because we need to adapt our network design to existing fiber optic networks. For that reason, our algorithm is similar to network algorithms. However, in terms of security, our network behaves differently reducing constraints related to potential attacks.

7. Related Work

The problem of creating a quantum key distribution network is divided in two main approaches [7]: 1) quantum channel switching paradigm that creates an end-to-end channel among every agent; and, 2) trusted repeated paradigm that allows intermediate nodes in the network to route keys. The first paradigm is limited by the physical distance limits of the communication process. For instance, on fibre optic, this limit is about 100Km, even though the communication quality starts to suffer significantly for distances over 45/50 km [15]. The second method, which is the target of this work, aims to surpass these physical limitations by adding repeaters to the network.

In terms of nodes, there are several networks that already operate. These networks are DARPA [48], covering a range of 50Km with around 10 nodes, SECOQC [49, 50] that uses 6 nodes around Vienna (on the dependencies of Siemens), the network designed by Wang et al. [51] containing 9 nodes around 3 cities and covering 200km (this network extends a former one containing 5 nodes and covering 150Km [52]), and the Tokyo network [53] with 6 nodes and covering 90Km, among others. Even if these networks are working experimental prototypes on specific dependencies, their design on the existing territory has not been optimized to follow a specific criteria. Our approach aims to automatize the design of the network, which, for the sake of the authors, is the first methodology that any researcher has proposed to quantum key distribution approaches. Also, our methodology is focused on the design of larger networks were we can have hundreds of nodes, and to select which nodes will act as repeaters that, again, is also novel.

As we state in Section 3, there is a significant amount of research measuring the limits on direct communications. These experiments focuses on understanding how the physical limitations affect the communication abilities. Researchers focus on different protocols where the most famous are the BB and E families [8]. For the BB ones, the distance has significantly be increased. Starting with distances of 30 Km using interferometric quantum cryptography schemes [54], to a distance of 120Km with an improvement on the technology focused on optimization of the interferometer and single photon detection [15]. Current technologies pay more attention to the transmission rate using single photon detection systems [55]. Although these distances, related to quantum channel switching, are reasonable for communication, they have loss problems. For that reason, we chose the conservative method, provided by Gobby et al. [15], because this methodology can also guarantee a low error rate (3.1% in the distances that we are considering).

In terms of security, this depends on the properties of quantum mechanics, as long as it behaves as the postulates defined in [56]. According to these principles, when an attacker interacts with the key that is distributed, it causes a disturbance in the communication that could be detected by the communication agents. To guarantee the security of the communication, the attacker must not have access to the devices that the agents use for quantum key exchange. In addition, until now, it has been assumed that the classic channel was authenticated and that Alice and Bob were really who they claimed to be. Nevertheless, there are some quantum channel attacks to consider.

Suppose that Eve has taken individual samples of each qubit and measures them one after the other. She can perform a beam splitter attack, probably the most damaging that can be done to quantum key distribution systems over fiber optics. This attack uses an optical coupler on the quantum channel to extract part of the key without Bob noticing Eve's presence [57]. Another known attack is the photon number division attack [58], where Eve performs a non-destructive measurement of the number of photons on each pulse. If it detects more than one photon in each pulse, it will store one of them to measure it. The rest will be sent to Bob [59]. Finally, another attack Eve can perform is the intercept and resend attack [60]. Assuming Eve has access to the repeaters, she can intercept the photons, measure them using a random basis and forward the photons to Alice.

8. Conclusions

The application of quantum physics to computation implies a paradigm shift. The transition from classical to quantum computing is the starting point for finding solutions to historical problems that have been unresolved for some time. Quantum systems can perform mathematical operations that invert one-way functions with a low computational cost, breaking most designs of secure communication systems based on these functions. Therefore, it is necessary to strengthen current communication systems by implementing algorithms resistant to such possible attacks while new quantum applications are designed to achieve faster and more efficient secure communications.

In this context, our work has reviewed different quantum key distribution (QKD) works to understand their physical properties and limitations. After analyzing the results of laboratory tests of different research groups, we focused our effort on implementing an optimized quantum key distribution network, since the maximum distance at which these systems work is relatively low. Together with the latter, we have found the need for the designed system to be operated over a commercial (general purpose) fibre optic network.

Our experimentation finds the optimum way to deal with the distribution of repeaters to cover a wide area. Specifically, the surface area occupied by Castilla y León, one of the biggest regions in the Spanish territory. The municipalities considered on these experiments are those with 1,000 or more inhabitants within the selected territory. The experimentation shows how the number of repeaters needed varies depending on the distance as well as the minimums needed to cover the whole territory, interconnecting it entirely.

From this work there are several lines that can be continued in the future. The most relevant are: extending the application territory, apply different algorithms to design the network and new ones to connect existing ones. Another interesting line, as we highlighted in Section 6, is to extend the algorithm to create secure networks. Finally, we will also study other physical features that may affect the quality of the quantum key distribution network.

References

[1] P. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proceedings 35th Annual Symposium on Foundations of Computer Science, IEEE Comput. Soc. Press, 1994, pp. 124–134. doi:

10.1109/SFCS.1994.365700.
URL http://ieeexplore.ieee.org/document/365700/

[2] E. National Academies of Sciences, Medicine, et al., Quantum computing: progress and prospects, National Academies Press, 2019.

[3] D. Gottesman, H.-K. Lo, N. Lutkenhaus, J. Preskill, Security of quantum key distribution with imperfect devices, in: International Symposium on-Information Theory, 2004. ISIT 2004. Proceedings., IEEE, 2004, p. 136.

[4] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, A. J. Shields, Long-distance quantum key distribution secure against coherent attacks, Optica 4 (1) (2017) 163. doi:10.1364/OPTICA.4.000163.
URL http://arxiv.org/abs/1701.07252http://dx.doi.org/10.1364/OPTICA.4.000163https://www.osapublishing.org/abstract.cfm?URI=optica-4-1-163

[5] G. Gobby, Z. L. Yuan, A. J. Shields, Unconditionally secure quantum key distribution over 50km of standard telecom fibre, Electronics Letters 40 (25) (2004) 1603–1605. arXiv:0412173, doi:10.1049/el:20045038.
URL http://arxiv.org/abs/quant-ph/0412173http://dx.doi.org/10.1049/el:20045038

[6] IDQuantique, Cerberis QKD Blade (2015).
URL https://www.idquantique.com/quantum-safe-security/products/cerberis-qkd-blade/http://marketing.idquantique.com/acton/attachment/11868/f-00d1/1/-/-/-/-/2015IDQDatasheetCerberisQKDBlade.pdf

[7] L. Salvail, M. Peev, E. Diamanti, R. Alléaume, N. Lütkenhaus, T. Länger, Security of trusted repeater quantum key distribution networks, Journal of Computer Security 18 (1) (2010) 61–87.

[8] A. Cabello, Quantum key distribution without alternative measurements, Physical Review A 61 (5) (2000) 052312.

[9] C. H. Bennett, G. Brassard, Quantum Cryptography: Public Key Distribution, and Coin-Tossing, in: Proc. 1984 IEEE International Conference on Computers, Systems, and Signal Processing, 1984, pp. 175–179. doi:10.1016/j.tcs.2011.08.039.

[10] G. S. Vernam, Cipher printing telegraph systems: For secret wire and radio telegraphic communications, Journal of the AIEE 45 (2) (1926) 109–115.

[11] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, Quantum cryptography, Reviews of Modern Physics 74 (1) (2002) 145–195. doi:10.1103/RevModPhys.74.145.
URL https://cdn.journals.aps.org/files/RevModPhys.74.145.pdf

[12] Toshiba : Press Release (15 Sep, 2017): Toshiba Pushes Quantum Key Distribution Speed Beyond 10Mbps (2017).
URL https://www.toshiba.co.jp/about/press/2017_09/pr1501.htm

[13] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, J. E. Nordholt, Long-distance quantum key distribution in optical fibre, New J. Phys. 8 (9) (2006) 193. doi:10.1088/1367-2630/8/9/193.
URL https://arxiv.org/pdf/quant-ph/0607177.pdfhttp://stacks.iop.org/1367-2630/8/i=9/a=193

[14] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, A. J. Shields, Coexistence of high-bit-rate quantum key distribution and data on optical fiber, Physical Review X 2 (4) (2012) 041010. doi:10.1103/PhysRevX.2.041010.
URL https://link.aps.org/doi/10.1103/PhysRevX.2.041010

[15] C. Gobby, Z. Yuan, A. Shields, Quantum key distribution over 122 km of standard telecom fiber, Applied Physics Letters 84 (19) (2004) 3762–3764.

[16] E. L. Lawler, The traveling salesman problem: a guided tour of combinatorial optimization, Wiley-Interscience Series in Discrete Mathematics.

[17] D. T. Larose, C. D. Larose, Discovering knowledge in data: an introduction to data mining, John Wiley & Sons, 2014.

[18] J. MacQueen, et al., Some methods for classification and analysis of multivariate observations, in: Proceedings of the fifth Berkeley symposium on mathematical statistics and probability, Vol. 1, Oakland, CA, USA, 1967, pp. 281–297.

[19] E. Rendón, I. Abundez, A. Arizmendi, E. M. Quiroz, Internal versus external cluster validation indexes, International Journal of computers and communications 5 (1) (2011) 27–34.

[20] P. J. Rousseeuw, Silhouettes: a graphical aid to the interpretation and validation of cluster analysis, Journal of computational and applied mathematics 20 (1987) 53–65.

[21] J. C. Dunn, A fuzzy relative of the isodata process and its use in detecting compact well-separated clusters.

[22] D. Menendez, J. L. Llorente, The combination of graph theory and unsupervised learning applied to social data mining, Graph Theory: New Research, Nova Science Publishers Inc.

[23] H. D. Menéndez, D. F. Barrero, D. Camacho, A multi-objective genetic graph-based clustering algorithm with memory optimization, in: 2013 IEEE Congress on Evolutionary Computation, IEEE, 2013, pp. 3174–3181.

[24] H. D. Menéndez, D. F. Barrero, D. Camacho, A genetic graph-based approach for partitional clustering, International journal of neural systems 24 (03) (2014) 1430008.

[25] H. D. Menéndez, D. F. Barrero, D. Camacho, A co-evolutionary multi-objective approach for a k-adaptive graph-based clustering algorithm, in:

2014 IEEE congress on evolutionary computation (CEC), IEEE, 2014, pp. 2724–2731.

[26] H. D. Menéndez, F. E. Otero, D. Camacho, Macoc: a medoid-based aco clustering algorithm, in: International Conference on Swarm Intelligence, Springer, 2014, pp. 122–133.

[27] H. D. Menéndez, D. Camacho, Mogcla: A multi-objective genetic clustering algorithm for large data analysis., in: Proceedings of the Companion Publication of the 2015 Annual Conference on Genetic and Evolutionary Computation, 2015, pp. 1437–1438.

[28] H. D. Menéndez, F. E. Otero, D. Camacho, Medoid-based clustering using ant colony optimization, Swarm Intelligence 10 (2) (2016) 123–145.

[29] H. D. Menéndez, D. Camacho, Gany: A genetic spectral-based clustering algorithm for large data analysis, in: 2015 IEEE Congress on Evolutionary Computation (CEC), IEEE, 2015, pp. 640–647.

[30] H. Menendez, F. E. Otero, D. Camacho, Extending the sacoc algorithm through the nystrom method for dense manifold data analysis, International Journal of Bio-Inspired Computation 10 (2) (2017) 127–135.

[31] H. D. Menéndez, Varmog: A co-evolutionary algorithm to identify manifolds on large data, in: 2019 IEEE Congress on Evolutionary Computation (CEC), IEEE, 2019, pp. 3300–3307.

[32] V. Rodríguez-Fernández, H. D. Menéndez, D. Camacho, Automatic profile generation for uav operators using a simulation-based training environment, Progress in Artificial Intelligence 5 (1) (2016) 37–46.

[33] V. Rodríguez-Fernández, H. D. Menéndez, D. Camacho, Analysing temporal performance profiles of uav operators using time series clustering, Expert Systems with Applications 70 (2017) 103–118.

[34] H. D. Menéndez, S. Bhattacharya, D. Clark, E. T. Barr, The arms race: Adversarial search defeats entropy used to detect malware, Expert Systems with Applications 118 (2019) 246–260.

[35] H. D. Menéndez, J. L. Llorente, Mimicking anti-viruses with machine learning and entropy profiles, Entropy 21 (5) (2019) 513.

[36] G. Bello, H. Menéndez, S. Okazaki, D. Camacho, Extracting collective trends from twitter using social-based data mining, in: International Conference on Computational Collective Intelligence, Springer, 2013, pp. 622–630.

[37] G. Bello-Orgaz, H. Menéndez, S. Okazaki, D. Camacho, Combining social-based data mining techniques to extract collective trends from twitter, Malaysian Journal of Computer Science 27 (2) (2014) 95–111.

[38] H. D. Menéndez, L. Plaza, D. Camacho, A genetic graph-based clustering approach to biomedical summarization, in: Proceedings of the 3rd International Conference on Web Intelligence, Mining and Semantics, 2013, pp. 1–8.

[39] H. D. Menéndez, L. Plaza, D. Camacho, Combining graph connectivity and genetic clustering to improve biomedical summarization, in: 2014 IEEE Congress on Evolutionary Computation (CEC), IEEE, 2014, pp. 2740–2747.

[40] S. Okazaki, A. M. Dìaz-Martìn, M. Rozano, H. D. Menendez-Benito, How to mine brand tweets: Procedural guidelines and pretest, International Journal of Market Research 56 (4) (2014) 467–488.

[41] S. Okazaki, A. M. Díaz-Martín, M. Rozano, H. D. Menéndez-Benito, Using twitter to engage with customers: a data mining approach, Internet Research.

[42] S. Okazaki, K. Plangger, D. West, H. D. Menéndez, Exploring digital corporate social responsibility communications on twitter, Journal of Business Research.

[43] L. Kaufman, P. J. Rousseeuw, Finding groups in data: an introduction to cluster analysis, Vol. 344, John Wiley & Sons, 2009.

[44] U. Von Luxburg, A tutorial on spectral clustering, Statistics and computing 17 (4) (2007) 395–416.

[45] A. R. A. Gaya, D. C. Díaz-Aldagalán, V. G. Muñoz, A. M. García, W. A. A. Ocampo, J. G. R. CHICUE, J. M. Almerich, J. C. Francoy, Practical quantum key distribution based on the bb84 protocol, in: Waves, Vol. 1, Instituto de Telecomunicaciones y Aplicaciones Multimedia (iTEAM), 2011, pp. 4–14.

[46] H. Zhou, K. Lv, L. Huang, X. Ma, Security assessment and key management in a quantum network, arXiv preprint arXiv:1907.08963.

[47] L. Georgiadis, M. J. Neely, L. Tassiulas, Resource allocation and cross-layer control in wireless networks, Now Publishers Inc, 2006.

[48] C. Elliott, The darpa quantum network, in: Quantum Communications and cryptography, CRC Press, 2018, pp. 91–110.

[49] A. Poppe, M. Peev, O. Maurhart, Outline of the secoqc quantum-key-distribution network in vienna, International Journal of Quantum Information 6 (02) (2008) 209–218.

[50] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, et al., The secoqc quantum key distribution network in vienna, New Journal of Physics 11 (7) (2009) 075001.

[51] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, et al., Field and long-term demonstration of a

wide area quantum key distribution network, Optics express 22 (18) (2014) 21739–21756.

[52] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, et al., Field test of wavelength-saving quantum key distribution network, Optics letters 35 (14) (2010) 2454–2456.

[53] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, et al., Field test of quantum key distribution in the tokyo qkd network, Optics express 19 (11) (2011) 10387–10409.

[54] C. Marand, P. D. Townsend, Quantum key distribution over distances as long as 30 km, Optics Letters 20 (16) (1995) 1695–1697.

[55] J. Zhang, M. A. Itzler, H. Zbinden, J.-W. Pan, Advances in ingaas/inp single-photon detector systems for quantum communication, Light: Science & Applications 4 (5) (2015) e286.

[56] M. Fox, Quantum optics: an introduction, Vol. 15, OUP Oxford, 2006.

[57] J. Calsamiglia, S. M. Barnett, N. Lütkenhaus, Conditional beam-splitting attack on quantum key distribution, Physical Review A. Atomic, Molecular, and Optical Physics 65 (1) (2002) 123121–1231212. arXiv:0107148v1, doi:10.1103/PhysRevA.65.012312.
URL http://arxiv.org/abs/quant-ph/0107148http://dx.doi.org/10.1103/PhysRevA.65.012312

[58] C. F. Sabottke, C. D. Richardson, P. M. Anisimov, U. Yurtsever, A. Lamas-Linares, J. P. Dowling, Thwarting the Photon Number Splitting Attack with Entanglement Enhanced BB84 Quantum Key Distributiondoi:10.1088/1367-2630/14/4/043003.
URL http://arxiv.org/abs/1111.4510http://dx.doi.org/10.1088/1367-2630/14/4/043003

[59] J. Yao, Microwave photonics, J. Lightwave Technol. 27 (3) (2009) 314–335. doi:10.1109/22.989971.
URL https://www.osapublishing.org/jlt/abstract.cfm?URI=jlt-27-3-314http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=989971http://www.scopus.com/inward/record.url?eid=2-s2.0-0036500370&partnerID=tZOtx3y1

[60] M. Curty, N. Lütkenhaus, Intercept-resend attacks in the Bennett-Brassard 1984 quantum key distribution protocol with weak coherent pulsesdoi:10.1103/PhysRevA.71.062301.
URL http://arxiv.org/abs/quant-ph/0411041http://dx.doi.org/10.1103/PhysRevA.71.062301