optics

MDPI

Article

Quantum Network Intelligent Management System

Iván García-Cobo

Department of Applied Mathematics, IUFFyM, MOMACyT, Universidad de Salamanca, 37008 Salamanca, Spain; ivangarciacobo@usal.es

Abstract: Quantum network materializes the paradigm change caused by the depletion of classical computation. Quantum networks have been built gathering reliable quantum repeaters connected by optical fiber networks. The need to build robust and resilient networks against hacking attacks is fundamental in the design of the future quantum Internet, detecting structural security as the major issue in the current development of the technology. A network management method is proposed to achieve its real-time adaptation and to protect itself against sabotage or accidents that render part of the network or its nodes useless.

Keywords: Dijkstra algorithm; intelligent quantum network; QKD; quantum key distribution; quantum network

Citation: García-Cobo, I. Quantum Network Intelligent Management System. *Optics* **2022**, *3*, 430–437. https://doi.org/10.3390/opt3040036

Academic Editor: Thomas Seeger

Received: 4 July 2022
Accepted: 7 November 2022
Published: 15 November 2022

1. Introduction

Current asymmetric key cryptography systems are based on algorithms whose mathematical operations are trivial in a direction, but their corresponding reverse operations are practically unsolvable in low computational times [1]. Several algorithms in public-key (asymmetric-key) cryptography base their security on the assumption that the discrete logarithm problem has no efficient solution [2,3]. P. Shor proposed a quantum algorithm that allows solving the problem of factoring large integers and computing the discrete logarithm [4,5]. The emergence of quantum computing drives the need for a paradigm shift. Quantum communication could protect sensitive data and digital infrastructure in the future. For this, it is necessary to design and deploy quantum networks protected from hacking attacks and other security lacks.

There are numerous successful experiments on quantum communication at distances over 100 km on fiber optic channels [6,7]. However, trying to put a realistic approach orienting to a commercial implementation into real conditions, distances below 50 km have been considered based on the experiences [8]. It is demonstrated that at those distances with current commercial equipment such as those manufactured by the ID Quantique SA company achieve remarkable results. This device makes it possible to exchange around 100,000 quantum keys in one hour [9]. We can find methodologies to design commercial quantum networks through the distribution of quantum repeaters, such as the one proposed by I. García-Cobo and H. D. Menéndez (2021) [10].

2. Challenges, Scope, and Contributions

The implementation of commercial fiber optic quantum networks requires management. In a commercial exploitation scenario, the needs for network availability, service quality assurance, and ability to recover from unforeseen incidents arise. This article aims to respond to the needs derived from the use of commercial fiber optic networks for use in the creation of a quantum network. It is based on previous work carried out for the design of the network, focusing on methods that are resilient to attacks or degradation due to its use or accidents. We propose a method to achieve a robust and reliable quantum network model. A network management method is presented, which allows its continuous work

with the lesser possible impact. This method could face possible sabotage to any node or channel.

3. Distribution of Nodes in the Quantum Network

To build a network that connects all the inhabitants to each other, a distributed network of repeaters must be designed. To carry out this distribution, a methodology based on grouping of municipalities is used, through a k-medoid algorithm [10]. This algorithm will help to select those that are physically closer to each other. Afterward, the algorithm will facilitate the selection of the central or main municipality within the group. This municipality will be considered as a candidate to host a repeater. The methodology, finally, will try to connect the possible repeaters between them to generate a distribution network by using the described method again.

Repeaters Network

To guarantee that any municipality within the network can communicate with any other, it is necessary to establish a repeater network based on the representative municipalities selected in the previous step and organized by clusters and environments. A cluster is a group of municipalities with at least one repeater and an environment is a group of repeaters. This network is defined as follows:

1. Each representative municipality will connect with all the municipalities in its cluster. In this way, all the municipalities of the same cluster will be able to exchange quantum keys using the repeater. It is guaranteed that the repeater is at a lower distance than D (where D is the maximum acceptable distance—we considered 50 km) with respect to each municipality in its cluster.
2. Each repeater will connect to all repeaters in its environment that are within a distance lower than D. Thus, if various repeaters are close to one another, different routing can be used to reduce key distribution cluster.

These criteria when creating networks not only facilitate the achievement of better routing, but also identify possible isolated regions. To be able to find these regions, it will be enough to calculate the number of connected components of the network. Formally, the network is an undirected polygonal graph (G), divided into vertices (V), which represent the municipalities and edges (E) that represent those municipalities that either are within a cluster and are connected to its repeater, or are repeaters to a distance lower than D, between them. 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 their eigenvalues, or the estimation using random paths [11]. If the number of connected components of the graph is at least one, the network is totally connected.

4. Security in Quantum Communications

The security of the channels on which quantum communication protocols are implemented reside in the properties of quantum mechanics—as long as it behaves as postulated by Fox (2006) [12]. Considering these principles, when an attacker named Eve interacts with the key that is distributed, it causes a disturbance in the communication that could be detected by Alice and/or Bob. In this concept, Eve must not have access to the devices that Alice and Bob use for exchanging quantum keys, which will obtain a secure communication. In addition, up until now, the classic channel was authenticated by recognizing what Alice and Bob claimed to really be. Here are some of the attacks on the quantum channel that need to be considered.

4.1. Beam Splitting Attack

This attack is probably the most damaging that can be carried out on fiber optic quantum key distribution systems. As described by Calsamiglia et al. (2002) [13], there are losses associated with the channel itself. In this attack, this circumstance is used to extract

part of the key by means of an optical coupler on the quantum channel without Bob being aware of Eve's presence.

4.2. Photon Number Splitting Attack

As described by Sabottke et al. (2012) [14] in a Photon Number Splitting Attack (PNS), Eve will perform a non-destructive measurement of the number of photons in each pulse. If she detects more than one photon in each pulse, she will store one of them to measure. The rest will be sent to Bob [15].

4.3. Intercept and Resend Attack

Finally, we find the easiest attack we can carry out [16]. Eve intercepts the photons, measures them using a random basis, and returns the photons to Alice.

5. Approach to a Network Management System

The repeaters (network nodes) must recognize the complete topology of the network, as well as some instructions to know where to redirect their messages in case they are not themselves the destination of these.

A related network has been designed on the territory under study (Spain) as an application case. All repeaters are interconnected in such a way that this objective is achieved. The next step is to implement the logic to establish the optimal path for a message to arrive between any pair of points on the network. Every municipality must be able to communicate with the rest.

5.1. Network Topology

The first of the features is based on a network topology map. This map identifies the complete network, its different nodes, and the networks that relate these nodes. The information of the designed network must be housed in the management element for each node and in each final element of the network. An abstraction of the physical implementation of the network can be established, in such a way that this topology, based on the fiber network itself and the repeaters, constitutes a true logical topology. It serves each part of the network. These topology files provide the necessary instructions so that an end user can route the request to first point. In the same way, based on these defined paths, the quantum repeaters will know the next nodes to be (subsidiary network) and where to transmit the information.

5.2. Cost Matrix

The population distribution in the territory is not homogeneous. There is an atomizing effect on demographic distributions. In the application of the node distribution, exclusive distance criteria have been considered (although the premise of municipalities with more than 1000 inhabitants has been taken into account in previous work [10]). This constitutes an in-homogeneous configuration of the network load. Initially, a cost matrix is defined according to the target population served by each node. Each node is signaled by an identifier and a number that link with the population served. We add complexity to the matrix by indicating the distance between each of the connected nodes. In this way, we have created the first matrix.

5.3. Node and Channel Health Check

Each node can continuously verify its saturation status, the requests that it is attending, and other variables that can be defined linked to its specific status. That information is transmitted to the rest of the elements of the network, thus obtaining global status information of the system, which is known by every element of the system.

5.4. Searching the Optimal Path

One of the objectives of this research consists of introducing a novel element in the management of the quantum network. Considering for each repeater: its dimension (the target population of each node), the distance between them and their instantaneous health, the packet routing process can be given intelligence. The method consists of building a dynamic matrix that can be used for obtaining a cost algorithm to determine the optimal way to deliver the messages. At the beginning of the simulation, the nodes start from the defined network topology and the initial cost matrix. In the moment when a user sends a message through the quantum network, the system can route that message. The automatic sending of quality data (health information) between nodes for the network and its nodes will modify the routing of the message between Alice and Bob. This method is proposed based on the algorithm introduced by Dijkstra (1959) [17]. If problems are detected in a channel, its weight will increase, then the path will be modified consistently.

5.5. Justification Based on Previous Research

There are previous works in which the usefulness of the application of the Dijkstra algorithm for the intelligent management of fiber optic networks is discussed and tested [18]. We found comparisons of the use of the chosen algorithm—Dijkstra—versus others—Heuristics, Yen KSP, and some others—on large networks with random node generation tests [19], showing the prevalence of Dijkstra use. Its usefulness to guarantee the quality of the service provided QoS in network management is also analyzed [20].

6. Simulation

To test the method, the sudden inoperability of one of the nodes or the disconnection of a part of the network due to a problem in one of the segments is simulated. The simulation starts from an ideal network in which the different nodes and their connections are shown in the Figure 1. An initialization state with no network element saturation is supposed.

Figure 1. Representation of a network of quantum repeaters distributed over dark fiber nodes on the peninsular territory of Spain and the connection with its territories outside the European continent.

In this representation of the network (Figure 2), the nodes—vertices—(marked with pentagons) are quantum repeaters. They are assigned a *name* identifier to mark each node. The network that links the nodes—edges—has an assigned dimension (weight), which is ideal and equal to 0.

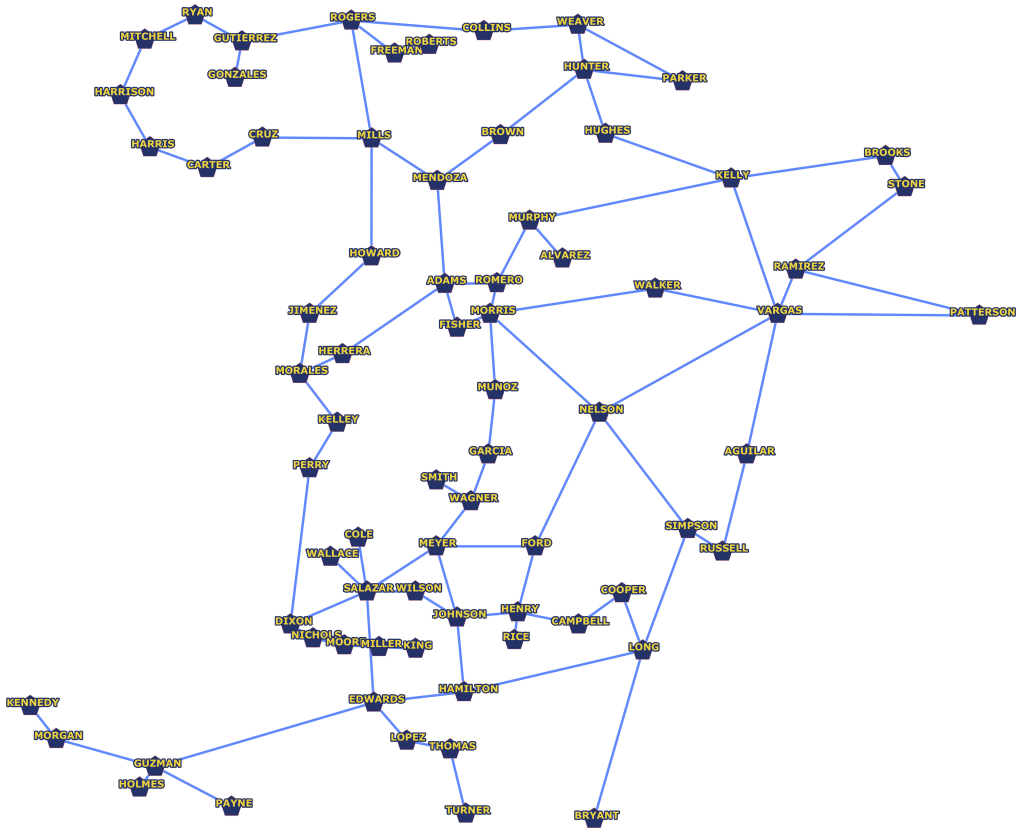

Figure 2. General schematic diagram of the network of quantum repeaters.

In our simulation (Figure 3), we start from the node identified as *Howard* and go to the one identified as *Patterson*. We apply Dijkstra's algorithm to calculate the initial optimal path. The initial optimal path whose length is 8 is: $HOWARD \Longrightarrow MILLS \Longrightarrow MENDOZA \Longrightarrow BROWN \Longrightarrow HUNTER \Longrightarrow HUGHES \Longrightarrow KELLY \Longrightarrow VARGAS \Longrightarrow PATTERSON$.

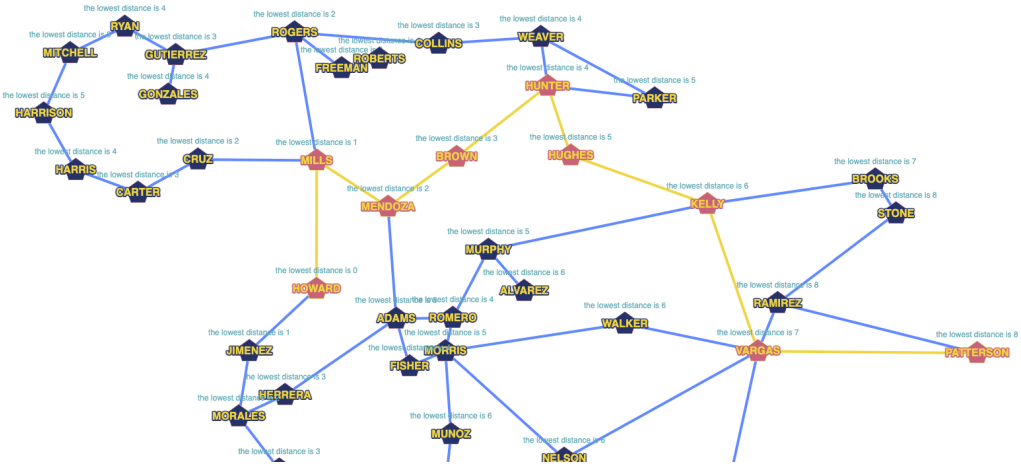

Figure 3. Detail of the optimal path between nodes *Howard* and *Patterson* at the initial moment of the simulation by applying Dijkstra's algorithm.

6.1. Deleting a Node

When eliminating a node from the network, it cannot send its status to the rest of the nodes, so they will stop managing the distribution of packets. Consequently, there will be unavailability in that node and in those channels that link the node with its neighbors, but alternative paths can be traced, solving the interruption. As an example, in Figure 4, the node identified with *Kelly* is eliminated and the algorithm is calculated again.

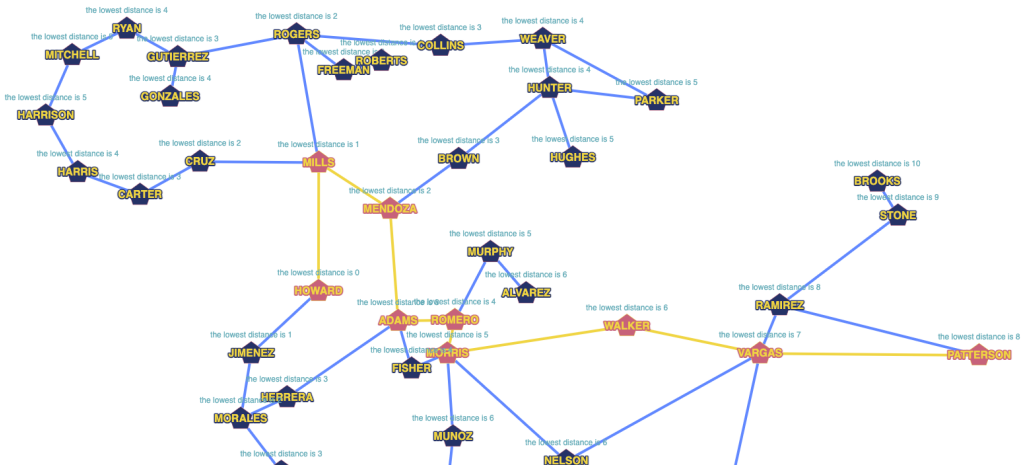

Figure 4. Detail of the result of the optimal path between nodes *Howard* and *Patterson* after eliminating node *Kelly* by applying Dijkstra's algorithm.

After deleting *Kelly*, the optimal path is: $HOWARD \Longrightarrow MILLS \Longrightarrow MENDOZA \Longrightarrow ADAMS \Longrightarrow ROMERO \Longrightarrow MORRIS \Longrightarrow WALKER \Longrightarrow VARGAS \Longrightarrow PATTERSON$.

6.2. Canceling a Segment

If a segment that links a pair of nodes becomes unused, the nodes will stop using that channel. By using Dijkstra algorithm's calculation, a new path will be traced to be able to route the messages accordingly. In that simulation, from initial state, the segment that linked node *Howard* and node *Mills* was eliminated (Figure 5):

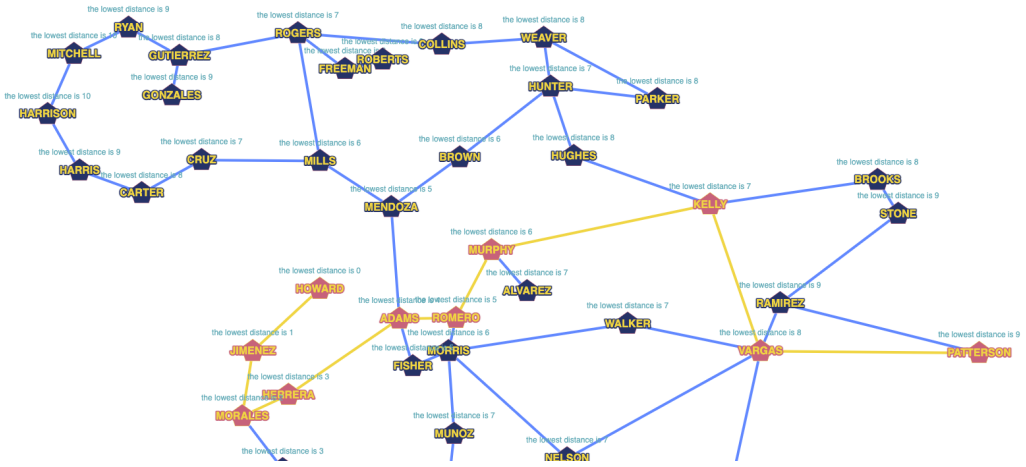

Figure 5. Detail of the result of the optimal path between nodes *Howard* and *Patterson* after eliminating segment that linked node *Howard* and node *Mills* by applying Dijkstra's algorithm.

When segment connecting *Howard* and *Mills* is invalidated new optimal path is: $HOWARD \Longrightarrow JIMENEZ \Longrightarrow MORALES \Longrightarrow HERRERA \Longrightarrow ADAMS \Longrightarrow ROMERO \Longrightarrow MURPHY \Longrightarrow KELLY \Longrightarrow VARGAS \Longrightarrow PATTERSON$.

7. Conclusions

The main contribution of this article consists of the dynamic calculation of the optimal routes in two concurrent scenarios:

- In situations of a saturation of a node and an element of the network, the algorithm will dynamically create a new route, guaranteeing the delivery of the message.
- At the time of sabotage or incident that renders an element of the quantum network useless, the algorithm will isolate the possible attacked node—or segment of the network, depending on the case—and will redirect the traffic using alternative routes to guarantee the best possible performance of the network.

We managed to provide robustness and reliability to our quantum network. We introduced a network management method that allows its continuity with the least possible impact, in the face of an imponderable event, whether voluntary or derived from the use of the nodes and the channel.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results

References

1. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
2. Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]
3. Omura, J.K.; Massey, J.L. Computational Method and Apparatus for Finite Field Arithmetic. U.S. Patent US 4,587,627, 6 May 1986.
4. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134. [CrossRef]
5. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
6. Plews, A.; Shields, A.J.; Sharpe, A.W.; Fröhlich, B.; Dynes, J.F.; Comandar, L.C.; Lucamarini, M.; Tam, W.W.S.; Yuan, Z. Long-distance quantum key distribution secure against coherent attacks. *Optica* **2017**, *4*, 163–167. [CrossRef]
7. Wang, B.X.; Mao, Y.; Shen, L.; Zhang, L.; Lan, X.B.; Ge, D.; Gao, Y.; Li, J.; Tang, Y.L.; Tang, S.B.; et al. Long-distance transmission of quantum key distribution coexisting with classical optical communication over a weakly-coupled few-mode fiber. *Opt. Express* **2020**, *28*, 12558–12565. [CrossRef] [PubMed]
8. Gobby, C.; Yuan, Z.L.; Shields, A.J.; Gobby, G.; Yuan, Z.L.; Shields, A.J. Unconditionally secure quantum key distribution over 50 km of standard telecom fibre. *Electron. Lett.* **2004**, *40*, 1603–1605. [CrossRef]
9. IDQuantique. Clavis XG QKD System. Available online: https://www.idquantique.com/quantum-safe-security/products/clavis-xg-qkd-system/ (accessed on 7 November 2022).
10. García-Cobo, I.; Menéndez, H.D. Designing large quantum key distribution networks via medoid-based algorithms. *Future Gener. Comput. Syst.* **2021**, *115*, 814–824. [CrossRef]
11. Von Luxburg, U. A tutorial on spectral clustering. *Stat. Comput.* **2007**, *17*, 395–416. [CrossRef]
12. Fox, M. *Quantum Optics: An Introduction*; Oxford University Press: Oxford, UK, 2006; Volume 15,
13. Calsamiglia, J.; Barnett, S.M.; Lütkenhaus, N. Conditional beam-splitting attack on quantum key distribution. *Phys. Rev. A At. Mol. Opt. Phys.* **2002**, *65*, 012312. [CrossRef]
14. Sabottke, C.F.; Richardson, C.D.; Anisimov, P.M.; Yurtsever, U.; Lamas-Linares, A.; Dowling, J.P. Thwarting the Photon Number Splitting Attack with Entanglement Enhanced BB84 Quantum Key Distribution. *New J. Phys.* **2012**, *14*, 043003. [CrossRef]
15. Seeds, A.J. Microwave photonics. *IEEE Trans. Microw. Theory Tech.* **2002**, *50*, 877–887. [CrossRef]
16. Curty, M.; Lütkenhaus, N. Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses. *Phys. Rev. A* **2005**, *71*, 062301. [CrossRef]
17. Dijkstra, E.W. A note on two problems in connexion with graphs. *Numer. Math.* **1959**, *1*, 269–271. [CrossRef]

18. Szcześniak, I.; Jajszczyk, A.; Woźna-Szcześniak, B.; Szczesniak, I.; Jajszczyk, A.; Wozna-Szczesniak, B. Generic Dijkstra for optical networks. *J. Opt. Commun. Netw.* **2019**, *11*, 568–577. [CrossRef]
19. Shang, J.; Li, H.; Man, X.; Wu, F.; Zhao, J.W.; Ma, X. A Dynamic Planning Algorithm based on Q-Learning Routing in SDON. In Proceedings of the 2020 Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC), Beijing, China, 24–27 October 2020; p. 4A.194. [CrossRef]
20. Varvarigos, E.; Sourlas, V.; Christodoulopoulos, K. Routing and scheduling connections in networks that support advance reservations. In Proceedings of the 5th International Conference on Broadband Communications, Networks, and Systems, BROADNETS, London, UK, 8–11 September 2008; pp. 536–543. [CrossRef]