DOI: https://doi.org/10.14201/0AQ0315105116

GESTIÓN INTELIGENTE DE RED CUÁNTICA

INTELLIGENT QUANTUM NETWORK MANAGEMENT

Iván García-Cobo[1] and Ángel Martín del Rey[2]

[1] *Grupo de Investigación en Modelización Matemática en Ciencia y Tecnología (MoMaCyT), University of Salamanca, 37007 Salamanca, Spain*
ivangarciacobo@usal.es

[2] *Departamento de Matemática Aplicada, University of Salamanca, 37007 Salamanca, Spain*
delrey@usal.es

Resumen: Las redes cuánticas materializan el cambio de paradigma provocado por el agotamiento de la computación clásica. Hasta ahora, se han construido redes cuánticas agrupando repetidores cuánticos confiables unidos por redes de fibra óptica. La necesidad de construir redes robustas y resilientes ante ataques se hace fundamental en el diseño del futuro Internet cuántico. Proponemos un método de gestión de la red que permita a esta adaptarse en tiempo real y protegerse frente a sabotajes o accidentes que inutilicen parte de la red o de sus nodos.

Palabras clave: QKD; quantum key distribution; quantum network; intelligent quantum network; dijkstra algorithm.

Abstract: Quantum networks materialize the paradigm shift caused by the exhaustion of classical computation. So far, networks have been built Quantum Clustering Reliable Quantum Repeaters Linked by Fiber Networks optics. The need to build robust and resilient networks against attacks becomes fundamental in the design of the future quantum Internet. We propose a method of network management that allows it to adapt in real

Ediciones Universidad de Salamanca / cc by-nc-nd Proceedings of the IV Workshop on Disruptive Information and Communication Technologies for Innovation and Digital Transformation, pp. -116

time and protect itself against sabotage or accidents that disable part of the network or its nodes.

KEYWORDS: quantum key distribution; quantum network; intelligent quantum network; dijkstra algorithm.

1 Introducción

La aparición de la computación cuántica impulsa la necesidad de un cambio de paradigma. La comunicación cuántica podría proteger datos sensibles y la infraestructura digital en los próximos años. Para ello, es necesario diseñar e implementar redes cuánticas que sirvan a este respecto.

Existen numerosos experimentos exitosos sobre comunicación cuántica en distancias por encima de 100 sobre canales de fibra óptica como entre otros los que encontramos en [6]. No obstante, tratando de poner un enfoque realista orientando a una implementación comercial en condiciones reales, se han considerado distancias por debajo de 50 basándonos en las experiencias [8] que consigue demostrar que en esas distancias con equipos comerciales actuales como los fabricados por la empresa *ID Quantique SA* se consiguen resultados destacables. Este dispositivo [9] permite intercambiar del orden de 20000 claves cuánticas en una hora.

Podemos encontrar metodologías para diseñar redes cuánticas comerciales mediante la distribución de repetidores cuánticos como la que se propone con detalle en [7].

1.1 Retos, alcance y contribuciones

La implantación de redes cuánticas sobre redes comerciales de fibra óptica lleva acompañada la necesidad de la gestión de las mismas. En un escenario de explotación comercial, surgen las necesidades de disponibilidad de la red, garantía de calidad de servicio y capacidad de recuperación frente a incidencias sobrevenidas.

Este artículo pretende dar respuesta a las necesidades derivadas del uso de las redes de fibra ópticas comerciales para su uso en la creación de una red

cuántica. Parte de la base de trabajos previos para el diseño de la red, centrándose en métodos para ser resiliente frente a ataques o degradaciones por su uso o provocados por accidentes.

Proponemos un método para conseguir dar robustez y fiabilidad a nuestra red cuántica. Ante un posible sabotaje de alguno de los nodos o de alguno de los canales, introducimos un método de gestión de la red que permita su continuidad con el menor impacto posible.

Proponemos un método para conseguir dar robustez y fiabilidad a nuestra red cuántica. Ante un posible sabotaje de alguno de los nodos o de alguno de los canales, introducimos un método de gestión de la red que permita su continuidad con el menor impacto posible.

1.2 Organización

El resto del artículo está organizado del siguiente modo. En la sección segunda se muestra el esquema de distribución de los nodos en la red. En la sección tercera se presentan cuestiones fundamentales sobre seguridad en la red cuántica, así como sus posibles ataques. En la sección cuarta introducimos la línea de trabajo sobre el sistema de gestión de red basándonos en trabajos previos relacionados.

Por último, en la sección sexta se indican las principales observaciones de este documento y las correspondientes recomendaciones.

2 Distribución de los nodos de la red cuántica

Para construir una red que conecte todos los municipios entre sí, se debe diseñar una red distribuida de repetidores. Para realizar dicho reparto, se utiliza una metodología basada en agrupación de municipios, a través de un algoritmo de k-medoides como se realiza en el trabajo previo [7]. Este algoritmo ayudará, dado un conjunto de municipios, a seleccionar aquellos que se encuentran físicamente cerca entre ellos. Después, el algoritmo facilitará la selección del municipio más céntrico, dentro del conjunto de municipios cercanos. Este municipio será considerado como candidato, dentro del conjunto, para albergar un repetidor. La metodología, finalmente, tratará de conectar los posibles repetidores entre ellos para generar una red de distribución.

2.1 Red de Repetidores

Para poder garantizar que cualquier municipio dentro de la red pueda comunicarse con cualquier otro, es necesario establecer una red de repetidores basada en los municipios representativos seleccionados en el paso anterior. Esta red se definirá de la siguiente manera:

1. Cada municipio representativo se conectará con todos los municipios de su clúster. De este modo, todos los municipios de un mismo clúster podrán intercambiar claves cuánticas utilizando el repetidor. En el paso anterior se garantiza que el repetidor queda a una distancia menor que D respecto a cada municipio de su clúster.
2. Cada repetidor se conectará con todos los repetidores de su entorno que se encuentren a una distancia menor D. De este modo, si hay más de un repetidor cerca de otro, se podrán utilizar distintos enrutamientos para reducir la saturación de la distribución de claves.

Estos criterios a la hora de crear la red no sólo facilitan la consecución de un mejor enrutado, sino que además permite fácilmente identificar posibles regiones aisladas de la misma. Para poder encontrar estas regiones, basta con calcular el número de componentes conexas de la red. Formalmente, la red es un grafo G no dirigido, dividido en vértices V, que representan los municipios, y aristas E que representan aquellos municipios que, o bien se encuentran dentro de un clúster y están conectados a su repetidor, o bien son repetidores a una distancia menor que D, entre ellos. De esta forma, el número de componentes conexas del grafo se puede calcular de varias formas, donde las más representativas son la multiplicidad de sus autovalores, o la estimación utilizando caminos aleatorios [14]. Si el número de componentes conexas del grafo es al menos uno, la red es totalmente conexa.

3 Seguridad en comunicaciones cuánticas

Como se ha mencionado en las secciones anteriores, la seguridad de los canales sobre los que se implementan los protocolos de comunicación cuántica reside en las propiedades de la mecánica cuántica –siempre y cuando esta se

comporte como dicen los postulados que la definen [5]–. Atendiendo a dichos principios, cuando un atacante denominado Eve interacciona con la clave que se distribuye provoca una perturbación en la comunicación que podría ser detectada por Alice y/o Bob.

Para que la comunicación sea segura, Eve no debe tener acceso a los dispositivos que Alice y Bob utilicen para el intercambio de claves cuánticas. Además, hasta ahora se ha supuesto que el canal clásico era autenticado además de que Alice y Bob eran realmente quién decían ser. A continuación, se introducen algunos de los ataques al canal cuántico que deben considerarse.

3.1 Ataques individuales

En los ataques que se describen a continuación Eve ha tomado muestras individuales de cada qbit y las va midiendo una tras otra.

Ataque de divisor de haz

Conocido como *Beam splitting attack* este ataque es probablemente el más dañino que se pueden realizar a los sistemas de distribución de claves cuánticas sobre fibra óptica. Como se describía, existen unas pérdidas asociadas con el propio canal. En este ataque [2] se utiliza esa circunstancia para mediante un acoplador óptico sobre el canal cuántico extraer parte de la clave sin que Bob se percate de la presencia de Eve.

Ataque de división de número de fotones

Como se describe en [10] *Photon Number Splitting Attack, PNS*, Eve realizará una medida no destructiva del número de fotos en cada pulso. Si detecta más de un fotón en cada pulso, almacenará uno de ellos para medirlo. El resto lo enviará a Bob [1].

Ataque de interceptación y reenvío.

Por último, encontramos el ataque más sencillo que podemos realizar. En *Intercept and resend attack* [3] Eve intercepta los fotones, los mide utilizando una base aleatoria y reenvía a Alice los fotones.

4 Aproximación a un Sistema de Gestión de red

Los repetidores –los nodos de nuestra red– han de conocer la topología completa de la red, así como unas instrucciones para saber hacia dónde redirigir sus mensajes en caso de que no sean ellos mismos el destino final de estos.

Se ha diseñado una red conexa sobre el territorio objeto de estudio. Todos los repetidores están conectados entre sí de tal modo que se consigue dicho objetivo. El siguiente paso consiste en implementar la lógica que permita establecer el camino óptimo para que un mensaje llegue entre cualquier par de puntos de la red. Todo municipio debe poder comunicarse con el resto.

4.1 Topología de red

La primera de las características se basa en un mapa de topología de red. En dicho mapa se identifica la red completa, los distintos nodos de esta y las redes que relacionan dichos nodos.

La información de la red que hemos diseñado debe estar albergada en el elemento de gestión de cada nodo y en cada elemento final de la red. Podemos establecer una abstracción de la implementación física de la red, de tal manera que esta topología aún basándose evidentemente en la propia red de fibra y los repetidores, constituya una verdadera topología lógica que sirva a cada parte de la red.

Estos ficheros de topología darán las instrucciones necesarias para que un usuario final sepa a quién encaminar la petición en primer lugar. De igual manera en base a esos caminos definidos los repetidores cuánticos conocerán cuáles pueden ser los siguientes nodos –subsidiariamente qué redes– a los que transmitir la información.

4.2 Matriz de costes

El reparto poblacional en el territorio no es homogéneo. Se produce un efecto atomizador en los repartos demográficos. De tal manera que, en la aplicación del reparto de nodos, se han considerado exclusivamente criterios de distancia (si bien se ha partido de la premisa de municipios de más de 1000 habitantes basándose en el trabajo anterior referenciado [7]). Esto constituye una configuración no homogénea de la carga de la red.

Se define en un primer momento una matriz de costes atendiendo a la población objeto que da servicio cada nodo. De tal manera que cada nodo estará ahora señalizado por un identificador del nodo, y un número que podemos vincular con el grosor de población objeto de servicio. Añadimos complejidad a la matriz indicando la distancia entre cada uno de los nodos conectados. De esta forma hemos creado una primera matriz.

4.3 Chequeo de sanidad del nodo y del canal

Cada nodo podrá saber en todo momento su estado de saturación, las peticiones que está atendiendo y otras variables que pueden definirse vinculadas con su estado de salud puntual. Dicha información debería ser transmitida al resto de elementos de la red, consiguiendo así una información de estado global del sistema conocida por todos y cada uno de los elementos de este.

4.4 En búsqueda del camino óptimo

Vamos a tratar de introducir un elemento novedoso en la gestión de la red cuántica. Teniendo en cuenta por cada repetidor: su grosor (la población objeto de cada nodo), la distancia entre ellos y su salud instantánea se puede dotar de inteligencia al proceso de encaminado de los paquetes. Se trata de construir una matriz dinámica que pueda servir para un algoritmo de costes determine el camino óptimo para realizar la entrega de los mensajes en cada momento.

En el inicio del experimento los nodos parten de la topología de red definida y de la matriz de costes inicial. De tal manera que en el momento en que un usuario envía un mensaje a través de la red cuántica, el sistema es capaz de encaminar dicho mensaje.

Se define el envío automático de datos de calidad entre los nodos tal y como se describía en la subsección anterior. Esta información de salubridad de la red y de sus nodos va a modificar el encaminamiento del mensaje entre Alice y Bob. Se propone un método basándonos en el Algoritmo introducido por Dijkstra [4] some or all pairs of which are connected by a branch; the length of each branch is given. We restrict ourselves to the case where at least one path exists between any two nodes. We now consider two problems. Problem 1. Constrnct the tree of minimum total length between the n nodes. (A tree is

a graph with one and only one path between every two nodes.. Si se detectan problemas en un canal, su peso aumentará. Por ello, al aplicar dicho algoritmo el camino se modificará consistentemente.

4.5 Justificación en base a investigaciones previas

Existen trabajos previos en los que se discute y se prueba la utilidad de la aplicación del algoritmo de Dijkstra para la gestión inteligente de redes de fibra óptica [12]. Encontramos comparativas de uso del algoritmo escogido –Dijkstra– versus otros –Heurísticos, Yen KSP y algunos otros– sobre grandes redes con pruebas de generación de nodos de forma aleatoria [11] resultando demostrado la prevalencia en el uso de Dijkstra. También se analiza su utilidad para garantizar la calidad del servicio prestado QoS en la gestión de la red [13].

5 Experimentación

Sobre nuestra red vamos a simular la inoperatividad sobrevenida de alguno de los nodos o bien la desconexión de una parte de la red por un problema en alguno de los segmentos de la red.

Partimos de una red ideal en la que los distintos nodos de la red y sus conexiones se muestran como en el gráfico que se muestra a continuación. Entendemos que el estado de partida en el que no tenemos saturación en ningún elemento de red. En esta representación de la red, los nodos –vértices– (marcados con círculos) son repetidores cuánticos. Tienen asignados unos números para identificar cada nodo. La red que une los nodos –aristas– tiene un peso asignado que como se decía es ideal e igual a 1.

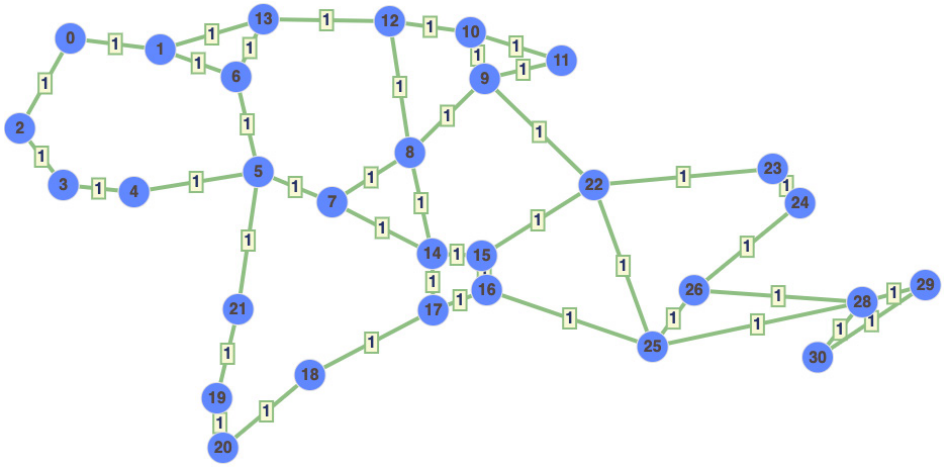

Fig. 1. Situación de partida de la red.

En nuestra simulación partimos del nodo identificado como 0 y nos dirigimos al identificado como 30. Aplicamos el Algortimo de Dijkstra para calcular el camino óptimo inicial:

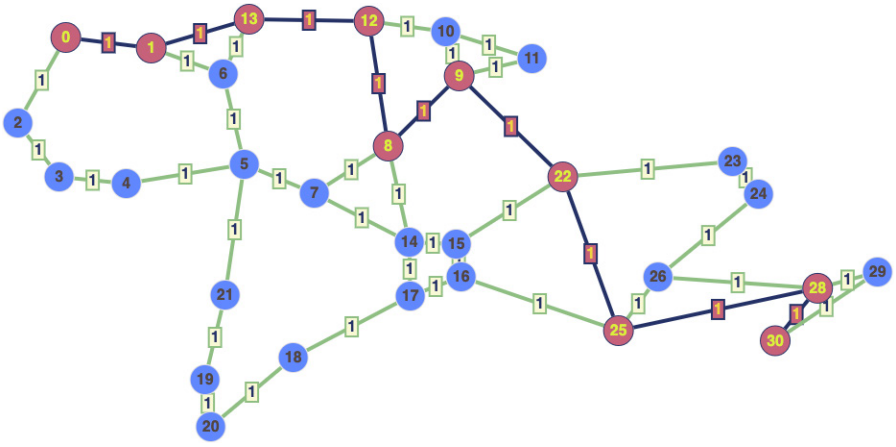

Fig. 2. Camino óptimo entre los nodos 0 y 30 tras aplicar el Alrgoritmo de Dijkstra.

5.1 Eliminación de un nodo

Al eliminar un nodo de nuestra red conexa, este no será capaz de mandar su estatus al resto de nodos, por lo que estos dejaran de tenerlo en cuenta para el reparto de paquetes. Se producirá consecuentemente una inoperatividad en dicho nodo y en aquellos canales que unan el nodo con sus vecinos, pero se podrán trazar caminos alternativos.

En el gráfico mostrado se elimina el nodo identificado con el 8 y se calcula de nuevo el algoritmo:

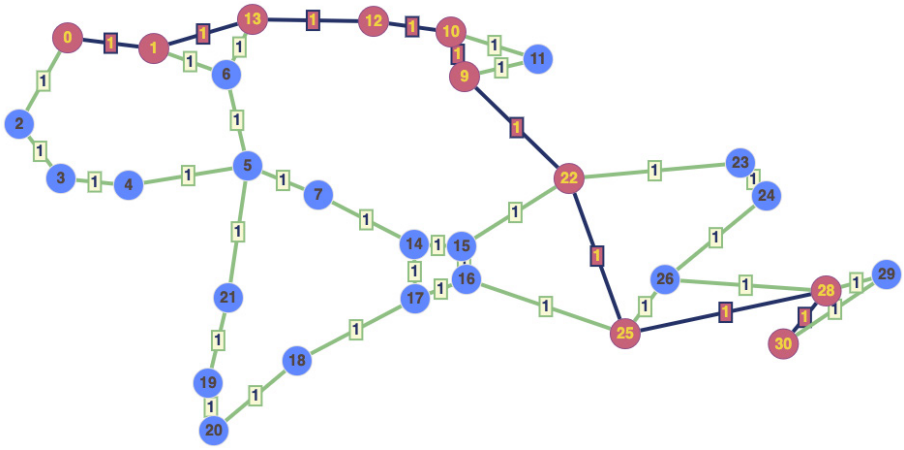

Fig. 3. Camino óptimo entre 0 y 30 tras eliminar el nodo 8.

5.2 Anulación de un segmento

Si un segmento que une una pareja de nodos queda inutilizado, los nodos dejarán de utilizar ese canal. Gracias al cálculo del algoritmo de Dijkstra se trazará un nuevo camino para poder encaminar los mensajes consecuentemente.

En el experimento se eliminó el segmento que unía el nodo 11 y el nodo 22:

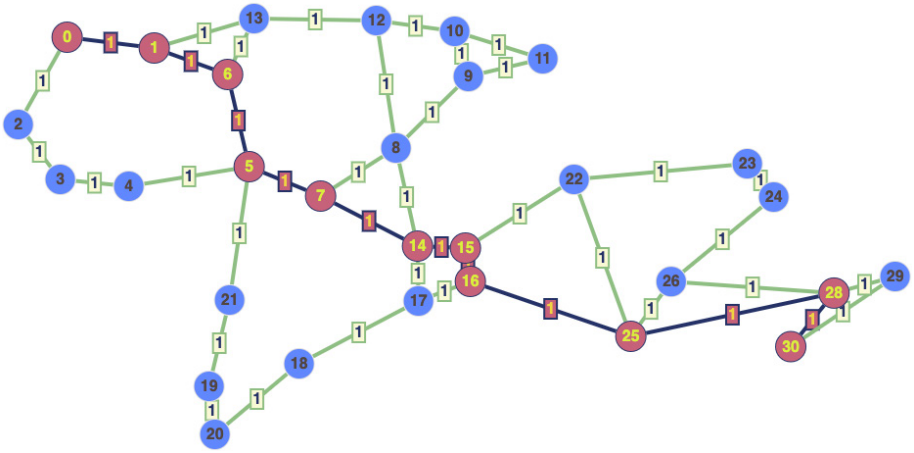

Fig. 4. Camino óptimo entre 0 y 30 tras eliminar el segmento entre el 11 y el 22.

6 Conclusiones

La aportación principal de este artículo consiste en el cálculo dinámico de las rutas óptimas en dos escenarios concurrentes:

1. en situaciones de saturación de un nodo y de un elemento de la red. En ese caso, el algoritmo creará dinámicamente una nueva ruta garantizando la entrega del mensaje.
3. en el momento en que se produzca el sabotaje o incidente que inutilice un elemento de la red cuántica, el algoritmo aislará el posible nodo atacado –o segmento de la red, según el caso– y reencaminará el tráfico utilizando rutas alternativas para garantizar el mejor funcionamiento posible de la red.

Conseguimos dotar a nuestra red cuántica de robustez y fiabilidad. Introducimos un método de gestión de la red que permita su continuidad -con el menor impacto posibleante un imponderable, bien sea voluntario o derivado del uso de los nodos y el canal.

References

1. Alwyn, J.: Seeds, microwave photonics. IEEE Trans. Microwave Theory, Tech 50(3), 877–887 (2002)
2. Calsamiglia, J., Barnett, S.M., Lütkenhaus, N.: Conditional beam-splitting attack on quantum key distribution. Physical Review A 65(1), 012312 (2001)
3. Curty, M., Lütkenhaus, N.: Intercept-resend attacks in the bennett-brassard 1984 quantum-key-distribution protocol with weak coherent pulses. Physical Review A 71(6), 062301 (2005)
4. Dijkstra, E.W., et al.: A note on two problems in connexion with graphs. Numerische mathematik 1(1), 269–271 (1959)
5. Fox, M.: Quantum optics: an introduction, vol. 15. OUP Oxford (2006)
6. Fröhlich, B., Lucamarini, M., Dynes, J.F., Comandar, L.C., Tam, W.W.S., Plews, A., Sharpe, A.W., Yuan, Z., Shields, A.J.: Long-distance quantum key distribution secure against coherent attacks. Optica 4(1), 163–167 (2017)
7. Garcia-Cobo, I., Menéndez, H.D.: Designing large quantum key distribution networks via medoid-based algorithms. Future Generation Computer Systems 115, 814–824 (2021)
8. Gobby, C., Yuan, Z., Shields, A.: Unconditionally secure quantum key distribution over 50 km of standard telecom fibre. Electronics Letters 40(25), 1603–1605 (2004)
9. IDQuantique: cerberis qkd blade (2015), https://www.idquantique.com/quantum-safe-security/products/cerberis-qkd-blade/
10. 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 Journal of Physics 14(4), 043003 (2012)
11. Shang, J., Li, H., Man, X., Wu, F., Zhao, J., Ma, X.: A dynamic planning algorithm based on q-learning routing in sdon. In: Asia Communications and Photonics Conference. pp. M4A–194. Optical Society of America (2020)
12. Szczésniak, I., Jajszczyk, A., Wózna-Szczésniak, B.: Generic dijkstra for optical networks. Journal of Optical Communications and Networking 11(11), 568–577 (2019)
13. Varvarigos, E.M., Sourlas, V., Christodoulopoulos, K.: Routing and scheduling connections in networks that support advance reservations. Computer Networks 52(15), 2988–3006 (2008)
14. Von Luxburg, U.: A tutorial on spectral clustering. arxiv, cs. DS, November (2007)