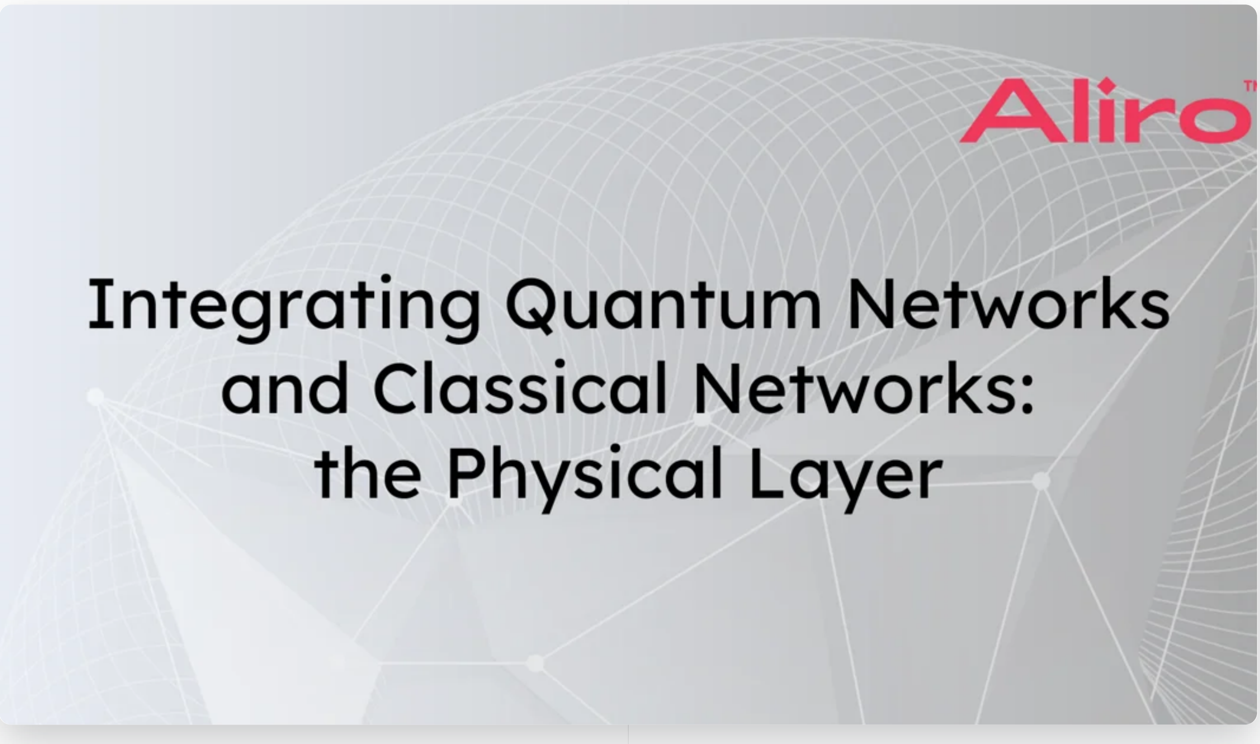
Aliro™

Integrating Quantum Networks and Classical Networks: the Physical Layer

Bruno Rijsman

September 13



Aliro™

Integrating Quantum Networks
and Classical Networks:
the Physical Layer

the control / management / orchestration layers please see our on-demand webinar.

Entanglement-based quantum networks can be used for a variety of applications: clustered quantum computing, distributed quantum computing (also known as the Quantum Internet), distributed quantum sensing, and Quantum Secure Communications.

The most well-known application of quantum networks is Quantum Secure Communications, and this use case is the focus throughout this article. Quantum Secure Communication addresses the problem posed by Q-Day, in which existing encryption protocols such as RSA and Diffie Hellman will be broken by quantum computers capable of implementing Shor's algorithm. Quantum Secure Communication (QSC) refers to the entanglement-based successor to Quantum Key Distribution (QKD) that addresses the weaknesses of QKD.

Quantum Secure Communication uses entanglement-based quantum networking protocols such as E91 and BBM92 that have been studied for many decades, are well understood, and that have security proofs. However, instead of using unsecure trusted relay nodes as QKD does, Quantum Secure Communication uses secure quantum repeaters. Once an quantum network makes use of quantum repeaters, it becomes a general-purpose network, capable of running other applications on the same network, including the other use cases mentioned above.

In some ways, entanglement-based quantum networking is a technology that is quite mature. It is actually more mature than quantum computing. Several companies have been offering commercial QKD products for over 10 years now, and these products have been deployed in operational networks. The components required for the next generation of general-purpose entanglement-based quantum networks are being commercialized. This includes hardware like quantum memories, transducers, and quantum repeaters. The range, speed, and cost of quantum networks will improve over time as a result of further innovations into multi-mode

One of the questions Aliro is frequently asked is, "Will entanglement-based quantum networks replace classical networks?"
The answer is no. We will never watch Netflix or do a Zoom call over a quantum network. Instead, quantum networks will be used in conjunction with classical networks. We can understand this better by looking at what happened with the development of classical computers.

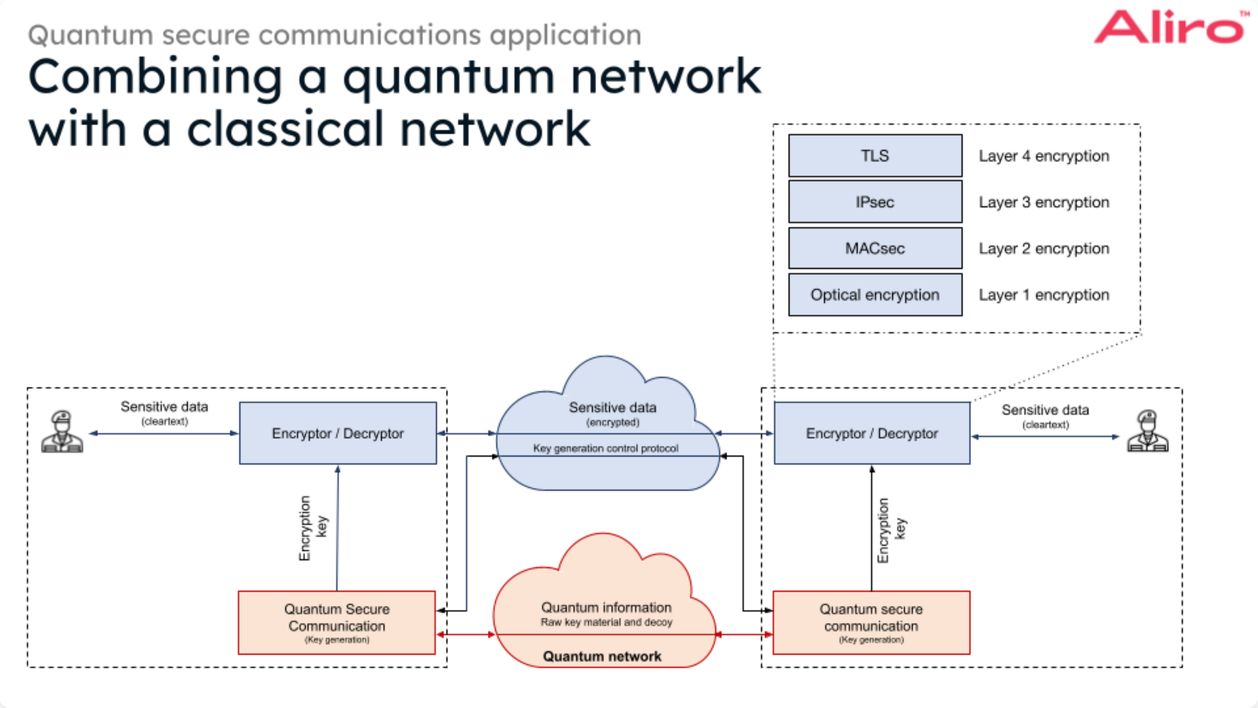
Classical computers have been using co-processors to perform specialized tasks for a long time. Graphical processing units, or GPUs, are used to offload graphics rendering. Tensor processing units, or TPUs, are used to offload machine learning. Data processing units, or DPUs, are used to offload networking tasks. These GPUs, TPUs, and DPUs do not replace the general-purpose CPUs; instead, they augment CPUs by off-loading very specific, specialized tasks.

Similarly, quantum processing units, or QPUs, will not replace classical computers. Just like GPUs, TPUs, and DPUs, quantum processing units will be used to offload very specific tasks that quantum computers are particularly suited for. This includes things like drug design, material design, optimization, simulation, and cryptanalysis. Although quantum computers are much better at certain tasks than classical computers, there are plenty of tasks quantum computers are not well suited for. No one would dream of using a quantum computer to edit an Excel spreadsheet or play a video game. Hence, quantum computers will never fully replace classical computers.

The same is true for entanglement-based networks. Entanglement-based quantum networks will not replace classical networks. Instead, quantum networks will augment classical networks. There are some specific applications that entanglement-based networks are very good at, including secure communications and connecting quantum computers or quantum sensors to each other. Quantum networks are not just better at these applications; some of

Combining a quantum network with a classical network

Below is a concrete example of how a classical network and a quantum network work together. This article focuses on the Quantum Secure Communications use case, as it is the application that is the furthest developed. Similar diagrams could be drawn for clustered and distributed quantum computing and sensing.



Quantum secure communications application

Combining a quantum network with a classical network

At the top, in blue, is the classical network. There are two parties that want to exchange encrypted data over this classical network. Companies including Cisco, Juniper, Fortinet and many others offer hardware encryption devices that do encryption at various layers in the networking stack. The bulk encryption of the data can take place at multiple gigabits or even terabits per second and uses symmetrical encryption protocols such as the advanced encryption standard (AES).

The symmetrical encryption protocols need both parties to agree on a session encryption key.

protocol that is safe against attack by quantum computers. The terms Quantum Secure Communications and post-quantum security specifically refer to this safety from quantum attacks.

One possible way to implement advanced secure key establishment is to use an entanglement-based quantum network. In the diagram above, the quantum network is shown in red at the bottom. The quantum network uses the special properties of quantum physics to establish an encryption key between the two parties in a secure manner. The basic principle behind this security is that the laws of physics guarantee that it is impossible to steal the key without being detected. Thus, the term physics-based security is sometimes used for this approach.

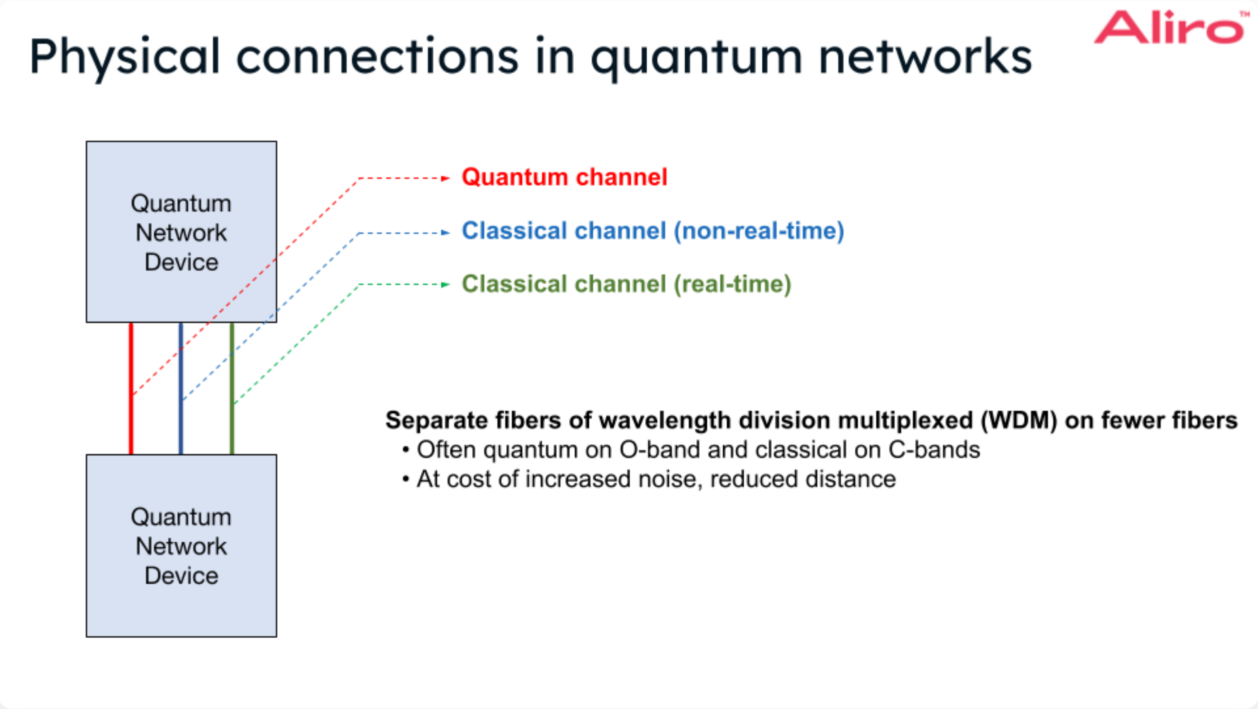
There are two important things to notice in this diagram. The first observation is that the quantum network is not responsible for high-speed bulk data encryption at multiple gigabits per second. The high-speed bulk encryption still happens on the classical side of the network. The quantum network is only responsible for producing the encryption key. Even if the encryption key is rolled over very frequently, the quantum network is more than fast enough to produce the necessary session encryption keys. The quantum network hands over the encryption keys to the classical encryptors using a well-defined interface. The second observation is that the quantum network does not replace the classical network. A forklift upgrade of the classical equipment is not necessary. The quantum network augments the classical network to offload a specific function: in this case, encryption key establishment.

Physical connections in quantum networks

There are three layers to the integration between classical networks and quantum networks: the physical layer, the control layer, and the orchestration and management layer. This article will focus on the physical layer. For additional information, please see the on-demand webinar focused on this integration at all these levels.

quantum routers, quantum sensors, or any other type of device that might be found in a quantum network.

There are three channels: the entanglement channel, the real-time classical channel, and the non-real-time classical channel. Each of these channels can be implemented using optical fiber connections or using free-space connections subject to certain restrictions. When optical fibers are used, each channel can be assigned to a separate optical fiber strand, or multiple channels can be multiplexed onto a single fiber using dense wavelength division multiplexing, or DWDM, once again subject to certain restrictions.



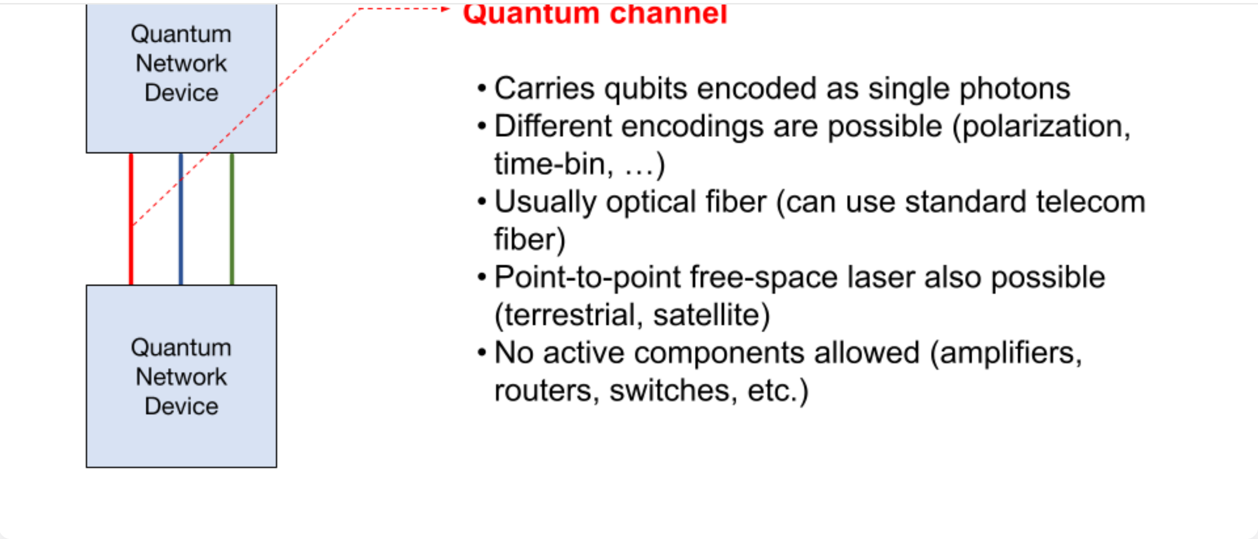
Physical connections in quantum networks

Separate fibers of wavelength division multiplexed (WDM) on fewer fibers

- Often quantum on O-band and classical on C-bands
- At cost of increased noise, reduced distance

Entanglement channel

The first channel is the entanglement channel. This is the channel that carries the qubits, which encode the quantum information typically in the form of individual photons. There are multiple different encoding schemes, including polarization encoding and time-bin encoding, each with their own advantages and disadvantages.



Quantum channel

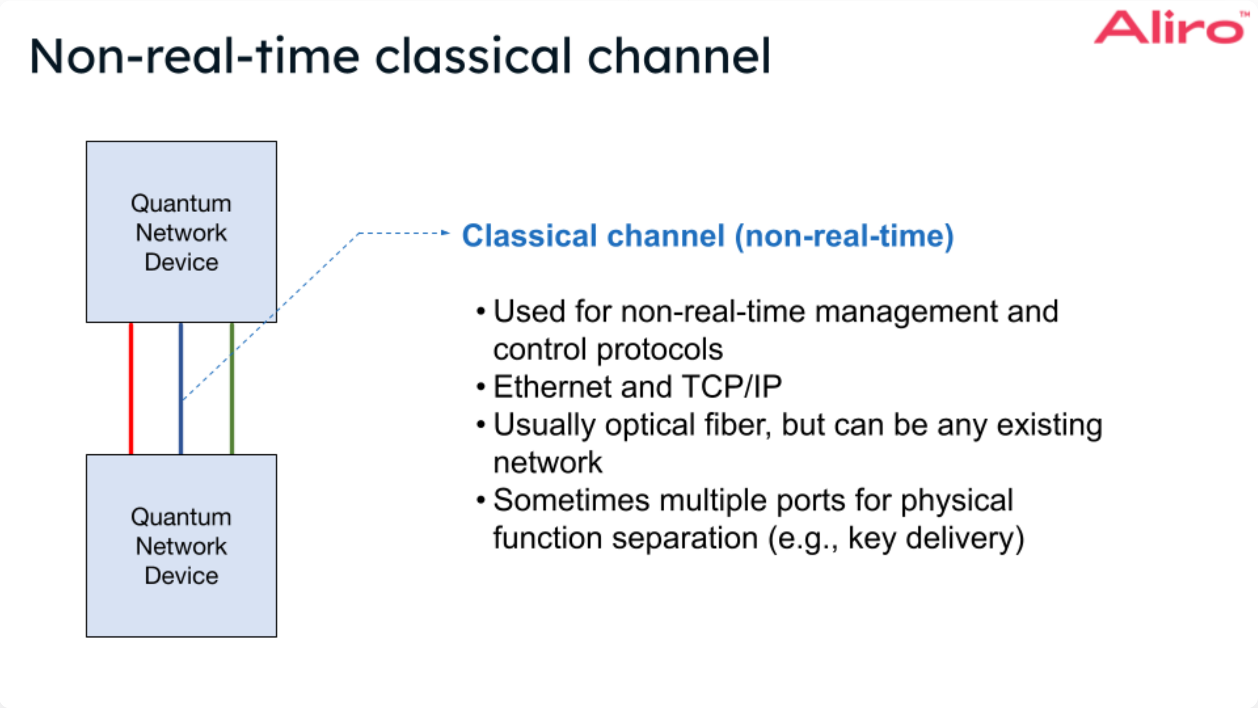
- Carries qubits encoded as single photons
- Different encodings are possible (polarization, time-bin, ...)
- Usually optical fiber (can use standard telecom fiber)
- Point-to-point free-space laser also possible (terrestrial, satellite)
- No active components allowed (amplifiers, routers, switches, etc.)

The entanglement channel is typically carried over optical fibers. It is possible to use typical telco fiber that is already deployed for the entanglement channel. It is not necessary to deploy a new kind of special fiber for the entanglement channel. However, the optical path used for the entanglement channel must not contain any active components. Passive components such as patch panels and optical cross-connects are compatible, but active components such as classical routers or classical switches or even simple classical amplifiers are not compatible with the entanglement channel.

It is also possible to carry the entanglement channel over a free-space connection. This may be a terrestrial point-to-point free-space connection, or it may be a ground-station to satellite free-space connection. Either way, the free-space connection must be implemented using a point-to-point laser. Radio networks such as Wifi networks or cellular networks are currently not suitable for the entanglement channel, and neither are copper links such as DSL links.

Non-real-time classical channel

The second channel is the non-real-time classical channel. This channel is used to carry widely used in classical networks.



Non-real-time classical channel

Classical channel (non-real-time)

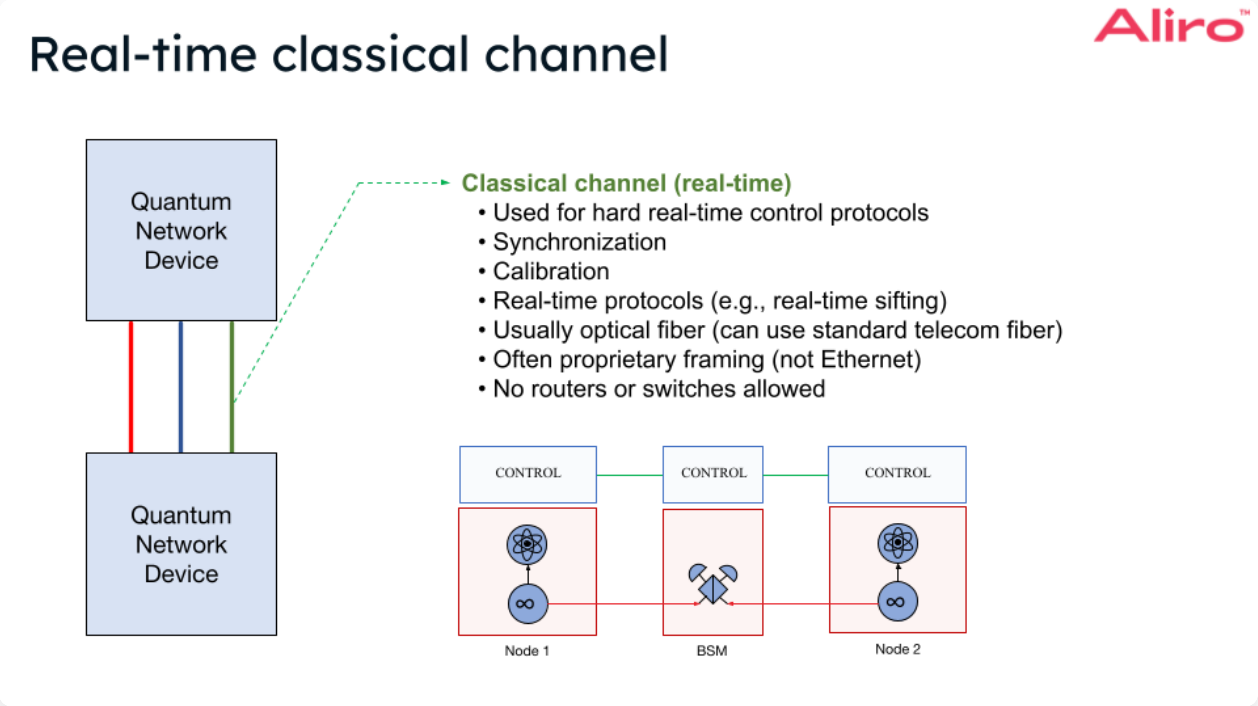
- Used for non-real-time management and control protocols
- Ethernet and TCP/IP
- Usually optical fiber, but can be any existing network
- Sometimes multiple ports for physical function separation (e.g., key delivery)

The control protocols are used to control various aspects of the quantum network. A small subset of these control protocols are extremely hard real-time, in the sense that they must be synchronized down to the nanosecond level. However, most of the control protocols are not hard real-time. Examples of non-hard real-time control protocols include key post-processing (such as information reconciliation and privacy amplification), key delivery, topology discovery, resource discovery, session establishment signaling, and many more.

These non-real-time control protocols can be carried over the non-real-time classical channel along with the orchestration and management protocols. The non-real-time classical channel uses completely normal TCP/IP and Ethernet networks, and thus it is possible to use an existing classical network with existing classical routers and switches.

In practice, there are often multiple non-real-time classical channels using separate ports on the device for security reasons. For example there might be separate physical ports for key

The third channel is the real-time classical channel. This channel is known by many different names including the service channel or the synchronization channel. Examples of hard-real-time control protocols include synchronization, calibration, key sifting, elementary entanglement generation, entanglement swapping, entanglement distribution, and teleportation. These hard-real-time control protocols are carried over a dedicated channel.



Real-time classical channel

Aliro™

Classical channel (real-time)

- Used for hard real-time control protocols
- Synchronization
- Calibration
- Real-time protocols (e.g., real-time sifting)
- Usually optical fiber (can use standard telecom fiber)
- Often proprietary framing (not Ethernet)
- No routers or switches allowed

Above is one possible mechanism for implementing elementary entanglement generation. In this example, the source on the left and the source on the right generate photons that need to arrive at the bell state analyzer in the middle at exactly the same time, down to the nanosecond level. This requires extremely precise clock synchronization protocols. The entanglement generation protocol is non-deterministic in the sense that multiple attempts are needed to get a successful entanglement. For this, a real-time control protocol is needed to track the attempts and retry until success is achieved.

Because of the sheer volume of control messages and because of the very precise timing compatible with the real-time classical channel.

Maximum link distance

One of the challenges in entanglement-based quantum networking is the limited maximum distance for point-to-point links. As a general rule of thumb the maximum loss on a point-to-point entanglement link is around 20 decibels, which translates into a maximum distance of roughly 100 kilometers. The exact limit depends on various technical details - for example what type of sources and what type of detectors are used. The actual distance limit may be higher or lower; but 100 kilometers is typical and this is the number used in examples throughout this article.

Beyond 100 kilometers, a kind of relay mechanism is necessary. This might be a trusted relay node, a quantum repeater, a quantum router, or a satellite. In many real-world deployments it is desirable to use dense wavelength division multiplexing, or DWDM, to multiplex classical and entanglement channels onto the same fiber. This greatly reduces the cost of the network because fewer fibers are deployed.

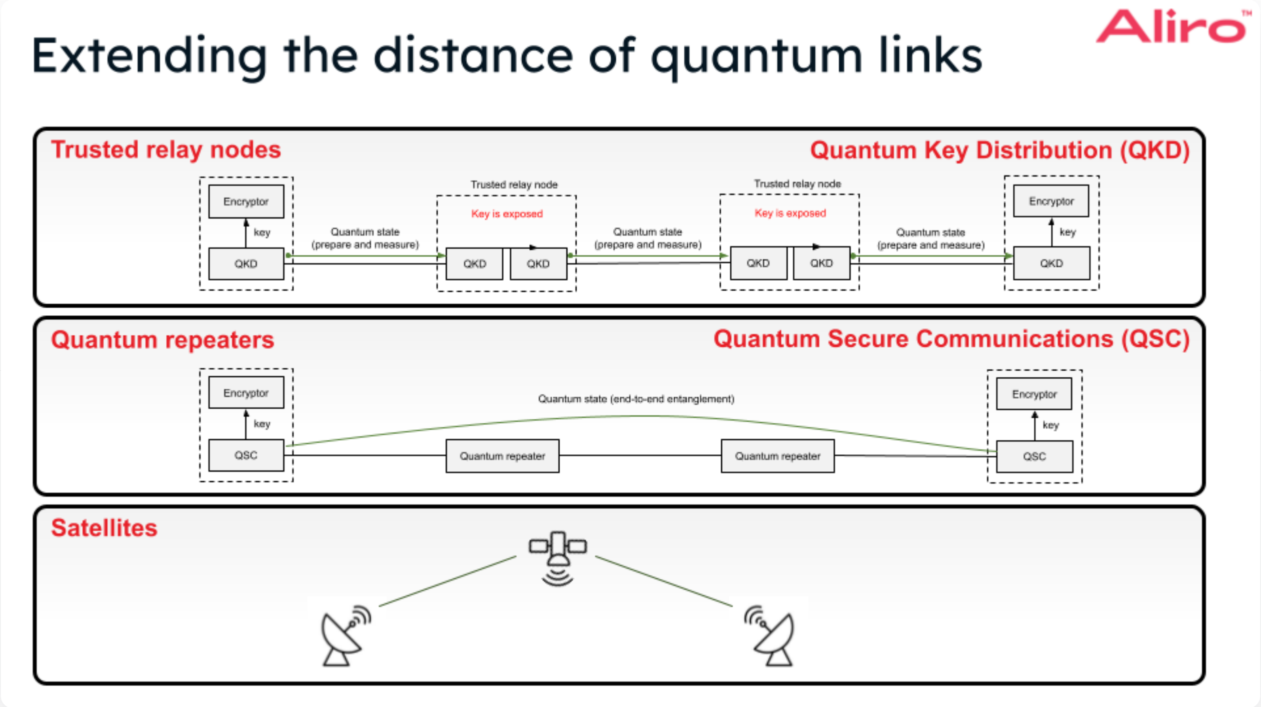
It is customary to put the entanglement channels in the O-band and the classical channels in the C-band to minimize interference between the entanglement and the classical channel. When the entanglement channel is in the O-band, the maximum distance is reduced by about 40% because the optical fiber has more loss in the O-band than in the C-band.

Extending the distance of entanglement links

There are several options for relay nodes to extend the distance of a point-to-point entanglement link exceeding 100 kilometers.

inside each of the trusted relay nodes. The name trusted relay node is somewhat misleading. It is not that the node is trustworthy. It is that trust is forced: the node must be trusted to not leak the exposed key. This need for trusted relay nodes is one of the most important criticisms of current first generation quantum key distribution networks. Another important drawback is that QKD networks are single-purpose: they can only ever be utilized for key distribution alone.

A better method to extend the distance of entanglement links is to use quantum repeaters in place of trusted relay nodes. Quantum repeaters offer two important benefits. The first benefit is that the keys are not exposed at the quantum repeaters. The second benefit is that an entanglement-based quantum network built with quantum repeaters is a general-purpose entanglement network. It can be used not only for Quantum Secure Communications, but also for other applications such as clustered and distributed quantum computing and sensing.



Extending the distance of quantum links

The current first generation of QKD networks are similar to the telephone networks of the 1980s: they can only run one single application. Entanglement-based networks are like the Internet of today, in the sense that they can run any application.

to replace trusted relay nodes over the next few years.

Finally, for intercontinental distances, there is the option to use satellites and ground stations connected by free-space lasers. Because the loss in the vacuum of space is much lower than in fiber, they can cover large distances of up to several thousands of kilometers. The downside to using this method is that satellites and ground stations are expensive to deploy.

Towards universal entanglement-based quantum networks

We have discussed physical interfaces in the context of Quantum Secure Communications. The next step is to generalize these interfaces, as well as the protocols and standards, to multi-purpose entanglement-based quantum networks.

At the physical layer, quantum repeaters and quantum routers will need to be introduced to the network. At the control layer, entanglement generation protocols - including elementary entanglement generation, swapping, purification, and teleportation - need to be implemented. At the management and orchestration layer, the network needs to continue to enable new end-user services such as clustered and distributed quantum computing and sensing and quantum testbed as a service. Finally, at the application interface, it is necessary to support general-purpose entanglement delivery.

Quite a lot can be implemented through software. An entanglement-based network software stack for building general-purpose entanglement-generating quantum networks should have these primary components:

- An orchestrator to implement the orchestration and management layer. This provides an interface to the operator to manage the quantum network and provides an interface to potential hardware and topologies is also recommended, as it can be integral to the design phase of quantum network implementation.

For more detailed information on integrating quantum and classical networks at the physical layer, application layer, and the control / management / orchestration layers please see our on-demand webinar.

Bruno Rijsman

September 13

Aliro™