Towards Scalability in QKD Networks

Joel Ansbro
dept. of Computing and Mathematics
Manchester Metropolitan University
Manchester, UK
joel.ansbro@stu.mmu.ac.uk

Daniel Smith
dept. of Computing and Mathematics
Manchester Metropolitan University
Manchester, UK
daniel.smith@stu.mmu.ac.uk

***Abstract*—Quantum Key Distribution offers a level of security, for communications, that is only governed by the laws of physics and isn't based on any assumptions of computing power or time constraints. With ever increasing research into different computing architectures, such as quantum computing, many cryptographic methods are coming under threat; a threat that QKD promises to alleviate completely. Current commercially available QKD machines work only between two nodes, about 100km apart; providing widely available QKD, which everyone can access, requires a scalability of those commercially available devices, to much larger geographical areas, with an associated scale up in connectivity. In this paper, we provide an insight into the current architecture of QKD, describe some of the perceived faults and look to provide a path forward.**

***Index Terms*—Quantum Networks QKD Trusted Repeaters Entanglement Scalability Satellites Drones MDI-QKD**

I. Introduction

Quantum Computing promises to provide great advancements in computational capabilities compared to even the best classical super computers. Harnessing the quantum phenomena known as superposition, quantum computing utilises qubits and the amount of data a qubit can contain scales exponentially with the number of available qubits – according to Microsoft [1] "Information that 500 qubits can easily represent would not be possible with even more than 2500 classical bits."

Applications range from accelerating drug development[2], to market prediction [3], to fluid modelling [4]. Cyber Security will see a notable breakthrough, as Quantum Computers' calculation power threatens to break many classical encryption algorithms with ease [5]. The time limit barrier that currently secures many classical encryption ciphers will be overcome easily, potentially compromising huge amounts of sensitive data.

Notably – quantum computers cant break all encryption methods due to their limited range of functionality, and many encryption methods are already considered to be quantum safe; however developments in classical computing, such as research being conducted on the use of Josephson Junctions[6] has the potential to threaten even those.

Fortunately, Quantum Key Distribution (QKD) serves as a practical solution to all these issues; generating quantum cryptographic keys that are uncopiable and cannot be hijacked by a third-party intruder. QKD can be said to be central to establishing secure channels for global communications in the future.

Several roadblocks exist before we can implement Quantum Key Distribution on a large scale. Firstly, the distance that we can transmit qubits is limited due to the surrounding noise within a system. Secondly, classical methods for amplifying a photonic signal are unsuitable for quantum networks due to the no-cloning theorem rendering them impossible.

This paper will be split into two parts;

1) Investigating the recent most developments in QKD; exploring experimental networks using fibre channels across a high-traffic network, and looking at technology beyond the use of fibre in the form of satellites and drones.
2) A discussion of some of the key drawbacks of the current implementation of QKD as trusted node networks, a vision of the way forward, and investigation into what is needed to be done to make that a reality.

A. Background

Throughout this paper, we will use some quantum mechanical terminology that will be important to understand:

Quantum Key Distribution (QKD) - a quantum cryptographical process that utilises the properties of superposition and qubits to create secret keys, from end to end, that are free from the possibility of eavesdropping.

Superposition – Superposition is a quantum mechanical principle that states a system can exist at multiple states at the same time until it is measured. When measured, superposition will collapse and the system will exist as the state it was measured at.

Qubit – Classical computing utilises the binary bit, which can be 1 or 0; similarly, qubits have two possible values, but unlike bits, qubits can exist in superposition, occupying a probability of both 1 and 0 at the same time.

No-cloning theorem – states that it is impossible to create an independent copy of an arbitrary unknown quantum state i.e. anything in superposition.

Quantum entanglement –the phenomenon observed that shows two quantum states exhibiting strong correlation to each other that cannot be explained by their individual properties, meaning that they are statistically linked to each other.

Teleportation – utilises entangled pairs, over theoretically infinite distance, to teleport a data qubit from the sender to

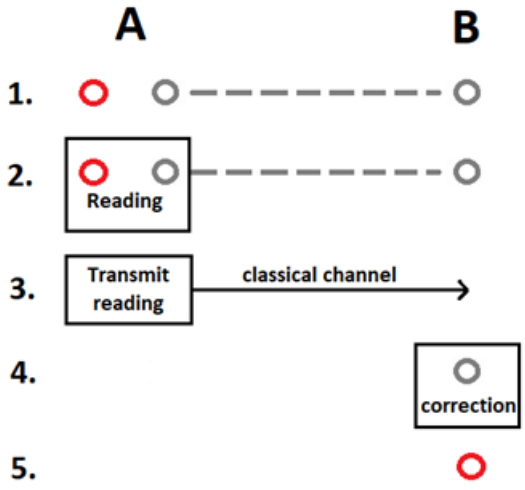

Fig. 1. Teleportation

the receiver. The sender measures their data qubit, along with their entangled qubit, and transmits the measurements to the receiver over an accompanying classical channel. The receiver then performs a correction depending on the measurements provided by the sender, to their own qubit, providing the receiver with a qubit with the same state as that in which the original data qubit was. This is not teleportation of matter , but rather teleportation of data because the data qubit was never physically transmitted across the network, but the receiver now has a qubit in the state of the original data qubit. See Figure 1.

II. Trusted Node Networks

The viability of QKD as a long term cryptographical solution depends on the ability to scale up to larger geographical areas, with multimodal networks that are widely accessible.

QKD devices are commercially available that use photons of light transmitted down fibre cables. In practice, this has a terminal length of about 100km, after which the photons being transmitted aren't discernible from the noise within the cable and the qubit is lost. Experimental demonstrations have shown that this is possible over larger distances, with the current record being up to 600km[7] obtained by The Cambridge Research Laboratory of Toshiba Europe in 2021.

While this is promising, it doesn't promise to account for global coverage on its own and the ability to incorporate QKD into networks is key; looking to classical networks, signal strength is maintained from end to end, via signal amplification. Utilising repeaters along the route, the message is copied (repeated) and resent. Such repeaters are impossible to replicate in quantum networks, due to the no-cloning theorem.

The ideal solution would be and end to end quantum network implementing entanglement and entanglement swapping, but limitations in research and technology are preventing the realisation (more on this later). In the meantime, the adoption of so-called trusted node networks is a stepping stone in the implementation of QKD and the future possibilities.

This network architecture was originally developed in the DARPA network [8] and was later improved upon within the SEOCQC network. If we consider a set up where we have three nodes: Alice, Bob and Charlie, where Alice is the sender, Charlie is the receiver and Bob is the a midway node, end-to-end key transmission between A and C works as follows:

1) Alice and Bob perform QKD creating a key - AB
2) Bob and Charlie perform QKD creating – BC
3) Alice sends a key, AC, along the classical channel to Bob, encrypted with AB
4) Bob decrypts AC, re-encrypts using BC and sends it along the classical channel to Charlie
5) Charlie decrypts it and Alice Charlie now both have AC

For networks of multiple repeaters, stage 4 of encryption and re-encryption would be repeated for as many repeaters as there are in the system, until it reaches Charlie.

A. Security of Trusted Node Networks

There are obvious security concerns that can be raised in this architecture, namely stage 4, where the overall key information is decrypted and re-encrypted at each intermediary node, making them a point of vulnerability as each node would have access to the key data – hence why each node needs to be trusted by the sender and receiver.

The choice of protocol use has an impact on the security considerations. The most utilised protocols being BB84, which can be described as follows:

An amount of qubits (4n) is sent from the sender (Alice) to the receiver (Bob), encoded in one of two basis. Alice randomly selects which basis to encode a qubit in each time it is sent and Bob randomly selects which basis to decode each qubit once it is received. After this, Alice and Bob then share which basis they used each time and discard any results in which they used a different basis, providing roughly 2n readouts of the initial qubits. Next, Alice then randomly selects half (n) of the remaining readouts to randomly test and declares which ones they are to Bob – and Bob compares to his. The protocol then decides if any mismatches (errors) are within the Qubit Error Rate (QBER) of 11%[9], accounting for noise and potential eavesdropping. IF satisfied, Alice will send information to Bob in order to correct errors. Finally, Alice will then generate an extraction seed which, when applied to the remaining n readouts, will produce a key KAlice. The seed is then sent to Bob, who can then produce a key Kbob. Kalice and Kbob are assumed equal, allowing for secure data transfer.

Note – if the QBER is unsatisfactory, the protocol is cancelled and will start again.

BB84 is assumed to be secure because if an eavesdropper were to attempt to intercept the qubits being sent from Alice to Bob, then due to the no-cloning theorem, they couldn't copy them, leaving the only option to decode them, collapsing super position of the qubit in the process. When Alice and Bob then compare readouts using the correct basis, any intrusion can

theoretically be detected by the presence of erroneous results; i.e. where Bob declares one basis and provides the wrong readout back – the eavesdropper has used the wrong basis and collapsed superposition into the incorrect readout. It is worth noting that this isn't always because of eavesdroppers and can be because of environmental noise in the system, but, it is impossible to distinguish between the two.

That assumption does come with some caveats and there are two key areas that have been highlighted as potential points of attack:

Practically, BB84 assumes a single photon is being sent, but in reality this isn't what is applied and attenuated lasers pulses are used because the costs are much lower[11]. These produce multiple photons a time, which are susceptible to proton splitting attacks; where an intruder and split one proton off, being able to observe that without detection. It's possible to mitigate this by adding decoy qubits into the system, where the observer is less likely to identify and attack the correct qubits.

Within QKD information is generally ascribed to the spin of the photon, but photons also possess wavelengths and time-positions, which are referred to in literature as Degrees of Freedom. Rau [12] highlights that these Degrees of Freedom lead to an exploitable side-channel if the qubit's controlled DOF correlates to other DOFs [13]. A third party would be able to read only the wavelength while leaving the spin unmolested.

B. Experimental Networks

The DARPA network was the worlds first QKD network, running from 2000 to 2007. In subsequent years, we have seen more QKD networks arise that look to build upon their achievements. Table 1 [8,18] provides a summary of some of these

The general trend that can be taken from this are as follows:

- An increase in key rate over time
- Increasing the number of nodes increases losses – which correlates to key rate losses
- Increasing the maximum distance reduces key rate

That's not to say that all networks follow these generalisations, with the Beijing-Shanghai network and the Wuhan networks standing out, with phenomenal key rates, despite large amounts of nodes and distances covered.

1) Cambridge Network: A general requirement for scaling up of quantum networks, is, not only to improve the distances and security, but will also be to improve the practicality of the network architectures being used. Previous networks have either adapted the use of dark fibres and/or have key rates insufficient for practical use.[14]

In 2021, Dynes et al.[14] sought to develop broadband capacity of quantum keys, connecting a city-wide QKD network operating on optic fibres already populated with high-bandwidth data traffic, controlled with a three layer network protocol connecting to an AES engine. The network composes a three-node high-speed quantum metropolitan ring topology network based out of Cambridge, in order to develop the kind

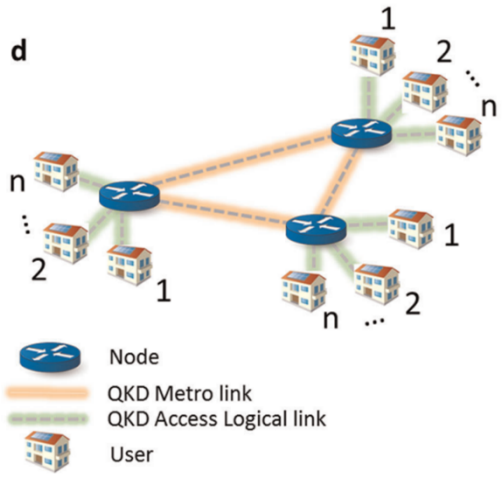

Fig. 2. Figure: Cambridge Network Setup

of QKD network that could sustain a large-scale userbase. This involved coupling onto the existing classical fibre infrastructure and constructing a three-layer network protocol wherein which a key management system could be accessed to send quantum encrypted keys via an API based within C. Further QKD networks, if they are to be used large-scale, must also look to providing large network capacity for multiple users. To satisfy the requirements of a practical level of bandwidth for a large-scale of users, the network comprises state of the art single fibre QKD systems with secure bit rates exceeding 3 Mbps over short distances. The Quantum Key Rates are reported to be capable of supporting thousands of users – the nodes could theoretically connect with smaller Quantum Access Networks serving specific areas, in order to connect users to the overall network who could access the key delivery module via a REST API.

The network also concerned itself with reliability. Attaching to the metropolitan networks which historically are based on fibre ring technologies, QKD can replicate the topology for redundancy if the ring is meshed to connect all the nodes together. All nodes can be interconnected by designing the intermediate nodes to act as relays. If they are all interconnected, the QKD has to provide for high bit rates, which the network has been able to achieve.

The experiment tests for resilience to power outages by disconnecting one of the links. The network layer is able to redirect so that the application layer can consistently make key requests, even if one of the links goes down.

One of the links used achieved an average secure bit rate of 2.58 Mbps with a corresponding 129 Terabit (Tbit) of key material distilled, far in advance of its most comparable network, the SwissQuantum network, which achieved in total secure bits distilled around 0.13Tbits. Important for QKD networking was the high key rate comparable to metropolitan architectures with tens of nodes.

The construction of high-bandwidth networking alongside a proper networking protocol stack serves as an important

TABLE I
LARGE SCALE HISTORICAL QKD NETWORKS

Network	Year	Channel	Nodes	Maximum Distance(km)	Max Key Rate (kbps)	Losses (db/km)	Protocol
DARPA	2007	Fibre + Air	10	29	1	0.2	BB84
SECOQC	2009	Fibre + Air	6	83	11	0.2	BB84, BBM92
UQCC	2011	Fibre	6	90	304	0.4	BB84, BBM92
SwissQuantum	2011	Fibre	3	17.1	1.5	0.05	BB84
HCW	2014	Fibre	9	85	16	0.2	BB84
Beijing-Shanghai	2016	Fibre	32	89	250	-	BB84
Jinan	2019	Fibre	32	65	65	-	BB84
Wuhan	2019	Fibre	71	16	141	2.2	BB84
Madrid QN	2021	Fibre	12	41	70	0.3	BB84

milestone in the scalability of QKD networks. We now see a working setup of key distribution in which end-users may make requests over a robust network.

A distinction made on the lower key exchange frequency is made in regards to the speed of the REST APIs used that hands keys over from the QKD device to the used AES engine. The observation in the research highlights an important development in the progression of QKD Networks, where we are now able to move the discussion forward simply from the base quantum theory and technological elements and towards the software connections. The takeaway from the specific observation is that future implementations should look to speeding up the efficiency of any connecting API, as times to interact with the network would lengthen the amount of time to transact a QKD connection, which places pressure onto the qubit coherence lifetime.

Another downside that the researchers highlight is that the 100g encryptors used as an example application that although allowed for multiplexing onto the same fibre, exacerbates Ramon noise into the channel and then increasing the Quantum Bit Error Rate.

The researchers also admit that the trusted repeaters are not ideal in terms of possible third-party hijacking, resolute in the notion that the node facilities are significantly secure themselves to prevent intrusion. But true quantum entanglement could naturally increase the data encryption significantly. A major step forward would be reached within the network if some of the repeater technologies proposed below would be implemented in future renditions of the network such as MDI-QKD, or with further improvements in Quantum Memory. An explanatory study of network layer protocols using MDI-QKD or Quantum Entangling repeaters should be looked to further.

C. Free Space Transmission

The focus of this paper so far has been looking at fibre networks, and the advances there have been demonstrable – observing a general increase, over time for max distances, implementable node increase, and key rate.

What can be noted though, is that even though there is an observable increase in distance, these maximum distances still sit at less than 100km. This raises the question over scaling the networks past the metropolitan area size and into that of the global size.

Fortunately – research is being performed into the use of satellites and drones to support QKD. Many researchers posit that using satellites is the best way forward given the current technology limitations of Quantum Memory and fibreoptic-based links [15-16].

Three papers below will look into the most recent developments.

D. Space to Ground BBM92 Quantum Links

Up until this point, we have primarily focused on the use of BB84 protocol, and have highlighted some of the security concerns that have been raised with it. Alternative protocols have been developed, such as BBM92, which expands on BB84 to incorporate entanglement - where a photon source is located somewhere between the sender and receiver and provides both with a single photon of an entangled pair.

From Erven[17], we describe BBM92 as follows:

> Alice and Bob each receive one photon from a stream of entangled photon pairs, they randomly pick a basis to measure each photon in, get a measurement result, convert their result to a classical bit, sift their results down to only those where they measured in the same basis, use 10% of their measurements to estimate the quantum bit error rate(QBER), and generate a final secure key from the rest of their measurement results.

QKD can be obtained between entangled pairs by the utilisation of teleportation, as described earlier in the paper. Yin et al[36]. utilised this protocol within the Micius satellite in 2020, to perform QKD at a (then) record of up to 1,200km between two nodes. Although a pioneering demonstrative experiment, the key rate readout of 0.12 bits per second is far lower than what we currently see in fibre link connections[18], and far below the practical requirements for QKD, limiting this experiment to a proof-of-concept that requires improvement.

This is also reiterated in the fact that the results were only able to be obtained during a clear night, indicating that environmental conditions such as sunlight and weather (e.g. haziness, rain, clouds) play a limiting factor in the availability of this approach. Not only that, but the Micius satellite passed over the ground stations on average twice a night, at most four times, and sometimes none, for about 8 minutes each time, hampering any real world application, alongside the low key rate.

E. Space to Ground BB84 Quantum Links

In 2021, Chen at al.[10] demonstrated an Integrated Space-To-Ground Quantum Communication Network over 4,600 kilometres, which purports to break the previous record held by Yin et al as described above.

Chen at al. produced a network that involved connecting a large-scale fibre network of 700 QKD links with two high-speed Space-to-Ground free-space links. The network combines the Beijing-Shanghai network already implemented years prior expanded with more nodes, with the Micius satellite's QKD distance of 2,600 km, in order to study the combined effects of fibre links and satellites.

Approaching the project from as an extension of the work performed by Yin et al., the project attempted to reach the far more ambitious goal of realising a working Quantum network across the largest geographic area yet tested. It set out to achieve advances in six areas:

1) Compatibility with diverse topologies to connect distributed users
2) Address the basic network architecture
3) Use standard QKD devices that are adaptable and extendable
4) Use standard QKD devices that are adaptable and extendable
5) Maintain security against attackers
6) Allow different practical services
7) Preserve the reliability and long-term stability

The adoption of the satellite links were to connect long-distance users to the QKD network, where free-space renders decoherence negligible. Then in order to test different network topologies, the fibre links of 700 nodes were utilised. To achieve this fibre network, four fibre Quantum Metropolitan Area Networks were created. Each QMAN consists of a user node, an all-pass optical switch, and trusted relays.

Chen et al. retrofitted the Micius satellite with a BB84 based transmitter utilising decoy states and in doing so, they were able to achieve a key rate of 47.8kbps. This, multiple orders of magnitude increase to the key rate obtained by Yin et al. indicates that there is still much work to be done with respect to utilising entangled states in space to ground BBM92, but, the a usable system is there with the implementation of BB84. In terms of security, trusted nodes are still relied upon and the security concerns surrounding BB84 are present and in terms of availability, all the issues surrounding the orbit and time availability of the Micius satellite noted by Yin et al. are still present within this system, except that notably, this experiment was able to perform QKD within the daylight hours that the salellite passed overhead, provided the weather was clear, and not just at night.

When evaluating the key rate, it is noted did vary, sometimes dipping under the minimum 20 kbps required for a minimal key rate. The researchers primarily put this down to a difference in setup between the nodes along the overall backbone. Chen et al. note this to be the case because the network serves as a suitable backbone to transmit quantum

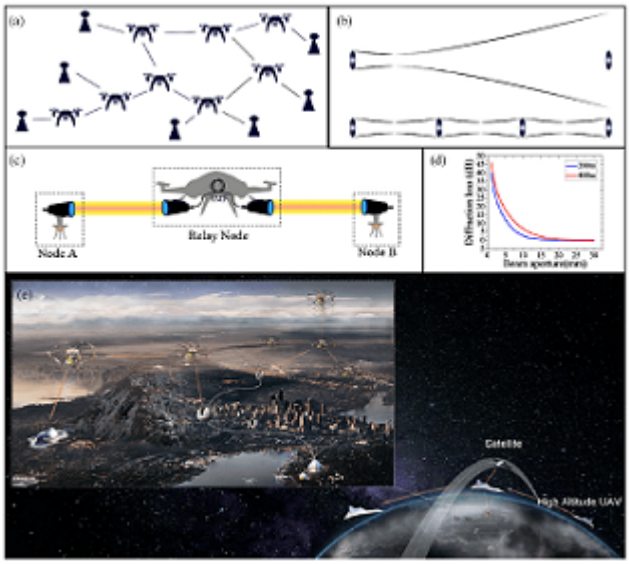

Fig. 3. Figure: Illustrative Scheme for a drone based mobile quantum network with scaling potential

signals which can then be improved upon in future as the more advances in quantum technology, such as measurement-independent devices or quantum repeaters, which will be talked about in part 2.

Finally, the key take-away from the experiment is that quantum technology, utilising trusted node networks, is demonstrating a level of maturity that close to practical, large scale applications. In the shorter term future, marrying the experiments performed by Dynes et al.[14], to improve the key generation rate, and investigate the impact of high traffic within the network would be the next practical step – although, considering the network topology of the fibre backbone, compared to the ring topology specifically chosen and utilised in the Cambridge network, this may not be possible.

F. Ground To Drone Networks

A novel method that addresses the decoherence loss from weather conditions is raised by Liu et al[19]. In this paper, drones take the place of satellites that can be manually operated to move to spaces with optimal conditions for transmission. This would allow for close to full-time all-location coverage, as the drones can be moved into different locations to avoid obstacles and weather that give rise to noise that interferes with the photon signal. The drones are fitted with airborne entangle-photon-sources (AEPS) and acquiring, pointing, and tracking (APT) systems which fit onto a drone, suitable for uplink and downlink directions, and communicate with a ground link.

A main driver behind the work is that the previous ground to satellite networks mentioned above, moved in a fixed-trace and can only establish a quantum data link for certain ground locations within a limited time frame. The satellite examples have also been beholden to light levels and thus have only been successfully implemented at night.

Lui et al. demonstrated the ability to establish entanglement distribution over a distance of 200 meters, providing coverage for around 40 minute intervals before the drone battery was a limiting factor. One could see this time limit as a downside and when thinking about quantum networks as a consistent connection requirement, and that would be correct – the solution being that multiple drones would need to be swapped in and out to provide consistent coverage. However, there are other applications that are worth considering – establishing ad hoc networks for secure communications on the fly, such as disaster zones or even possibly within the security industry.

Therefore true advantage of using such a network rests in it flexibility, however, it's worth noting that this is only proof of concept and is in early stages – no QKD has yet been performed using drones so its impossible to quantify any such networks capabilities. Although there are already further investigations into the use of drones[20], such as utilising BB84 for drone-to-drone QKD, but they are also yet to yield any results.

III. Looking Beyond Trusted Node Networks

As we look to the future, the use of trusted node networks should be relied on less and less, and one of the main directions it should look to is the use of untrusted networks[21]. Security of trusted node networks limit the potential of QKD in being an end-to-end means of security, determined by the laws of physics. The requirement of any network to trust each and every node and for every node to be not only free from cyber-attacks, but also physical attacks, presents a burden on a wide-scale, internet-like, implementation of QKD.

There are two potential avenues for solutions that will be discussed below, with Measurement Device Independent (MDI) QKD and the generation of quantum repeaters that utilise a phenomena known as entanglement swapping. Both show promise, but you will also see that both are currently being hampered by a lack of available technology.

A. Quantum Repeaters

Entanglement has long been considered as a vehicle for quantum communications, as we have seen utilised in BBM92. The outcome an entanglement based network being that each end has a single particle of an entangled pair in which teleportation of a desired data qubit can be performed on. For QKD, that would be key material. What is more desirable, is that entanglement offers a true solution to the no-cloning theorem within large scale networks in the form of quantum repeaters.

Instead of performing hop-by-hop QKD, quantum repeaters seek to perform entanglement swapping in order to bridge larger gaps with entangled particles. If we consider the case we had previously in trusted node networks, with Alice, Bob and Charlie, this time we see a scenario where Alice establishes entanglement with Bob and Bob establishes a separate entanglement with Charlie. Then, Bob teleports the qubit it shares with Alice, to Charlie, consuming the entanglement that was previous generated between Bob and Charlie. The result is a continuous entanglement between Alice and Charlie, see figure 4.

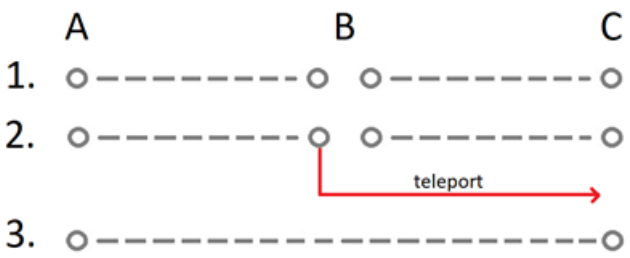

Fig. 4. Diagram of Entanglement Swapping

Finally, once end to end entanglement has been established, data qubits can then be teleported between the sender and the desired receiver. Most importantly, for security, teleportation of data qubits from the sender only occurs once end to end entanglement has been established, meaning that at no point in this system, would any of the intermediary nodes ever have seen any of the transmitted data. This eliminates the point of attack we saw in trusted nodes and opens up the ability to utilise "untrusted" nodes, just as in classical networking. This means that, realistically quantum repeater networks could be embedded within existing classical networks[18], by implementing a quantum data plane, with classical and quantum repeaters stacked together within the network.

This golden goose does comes with some caveats; notably in that form that, in reality, no large scale quantum networks exist yet. Despite understanding the theory of utilising quantum entanglement swapping, there hasn't been sufficient enough technological developments in quantum storage (quantum memories) as of yet to make these realisable.

To understand the impact that memories have, it's important to understand the concept of entanglement fidelity; the correlation between entangled particles isn't binary i.e. on or off; but rather it has is more akin to a gradient, where the strongest entanglements are known to be maximally entangled. Entanglement fidelity describes how well that entanglement is preserved, and is especially important because if the read-out of an entangled state is too low, it is unreliable and inaccurate, rendering it unsuitable for the distribution of keys.

Fidelity of a qubit itself is associated with the probability of the sufficient storage of a qubit i.e. is the storage of a qubit introducing any errors or environmental influence. At each repeater, an entangled qubit will need to be stored for a sufficient enough time for entanglement between a neighbouring node to be established and for the subsequent entanglement swapping to occur. If the fidelity of an entangled qubit is effected by the storage of it at a quantum repeater, and the entanglement of this qubit is subsequently swapped, then overall entanglement fidelity will be impacted. Its important to note that this effect will be also compounded by the number of repeaters that the routing requires from end to end. As noted by Neilsen[22] "...to preserve a quantum state and its

entanglement accurately, it is sufficient to keep the fidelity of storage high. . . ”

Not only do quantum networks have to address fidelity, but they also need to consider the timescales in which it takes to generate entanglement between neighbouring nodes. Peter C. Humphreys et al.[23] defined the term Quantum Link Efficiency(QLE) as the ratio rent/rdec where rent is the entanglement generation rate and rdec is the rate of decoherence of the quantum state. They define a critical threshold in QLE as unity – the threshold which, above this, entanglement is generated faster than it decoheres. Despite promising developments in the fidelity and efficiency of quantum memories[24], there still remains a research puzzle to develop memories, that can significantly reduce decoherence times, thus satisfying unity, before any of this can be realised.

Below, we will discuss some of the theoretical implementations of quantum repeaters, what some of these networks may look like, and review some of the latest studies into the development of relevant technologies.

B. MA QKD and Orbit to Orbit Satellites

MDI QKD[25] applies a novel approach, utilising a 3rd party device, Charlie, that is situated between two nodes, Alice and Bob. Alice and Bob both prepare randomised independent laser pulses using BB84 protocol to generate random polarisations, and direct them towards Charlie. Their signals are met at a beam splitter, which, depending on polarisation generated, will direct them to a specific detector. If precisely two detectors are triggered, Charlie is able to identify the presence of an entangled pair – otherwise known as a Bell Pair – and will announce the detection to Alice and Bob. Alice and Bob will then continue as with the BB84 protocol; comparing results in which were generated in the same basis, discarding those that weren't, randomly selecting half and generating the seed for the key.

MDI QKD is seen as safe because Charlie relays the results to Alice and Bob without ever seeing the results and it is theorised that MDI QKD can eliminate all detector side channels, and moreover, it is practical with current technology [26].

Gundogan et al.[27] employs MDI-QKD, from the work of Abruzzo [28] and applies it to ground to space satellites. The idea being that the security of the network can be improved upon from that of a standard BB84 protocol. Gundogan et al. highlights, much like the Micius experiments, that satellite can be used to bridge much larger distances that that of terrestrial fibre cables, with the requirement for less nodes, increasing theoretical key rate generation in the process.

The paper investigates the use of Memory Assisted MDI QKD (MA QKD) and furthermore – the use of quantum repeater technology within satellites. MA QKD can be utilised to achieve higher key rates but is limited by the lack of available technology.

The were able to demonstrate that utilisation of MA-QKD on satellites in an orbit-orbit configuration, sped up entanglement generation by around 3 orders of magnitude, compared

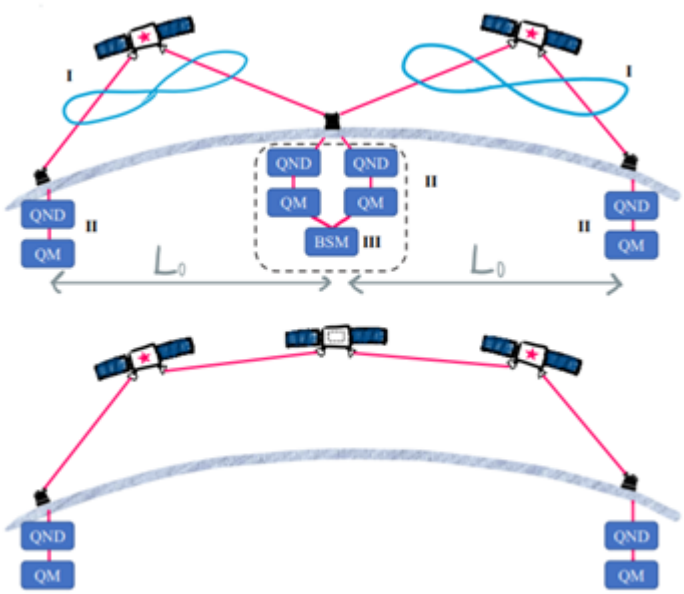

Fig. 5. MA-QKD Diagram

to that of quantum memories based in ground stations – for both schema. See figure 5.

The model uses a source repetition rate of 20MHz, compared to the Micius satellite, which used 5.9MHz. However, according to the simulation, an increase in the source repetition rate provides a large increase in secret key rate even when we lack repeaters. Gundogan admits to as much within the paper.

The uplink signal suffers from higher losses, and the downlink signal is limited by the classical communication needed to use a Bell State Measurement and quantum memories are needed for longer storage times whilst awaiting the classical channel. Further, to create larger secret key rates a large number of memories is required (up to 100) which would increase implementation and maintenance costs.

The orbit to orbit satellites are free of noise, such as atmospheric interference and weather, that would otherwise occur in orbit to ground transmissions, meaning that entanglement protocols had a generally higher success rate. This has a fundamental impact on the overall key rate generation, as the faster entanglement can be generated, the faster entanglement swapping can occur and the faster end to end communications can happen.

Finally, its worth noting that the simulations used do compliment the Micius satellite experiment, which here is baseline to test their calculations. However, without a proper physical experiment in place to test the setup, we lack further solid data to compare the two networks. For instance, in Gundogan's work, both the uplink and downlink distance of 400km is used, which is slightly smaller than the 500km distance between the Ground-Satellite link within the Micius satellite setup. The effect of this difference can only be known with a proper satellite experiment. Similarly, the setup does not go into

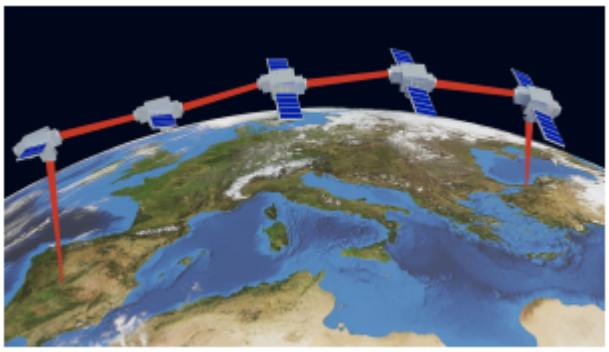

Fig. 6. Pictorial representation of the setup

details around what the orbital configurations for the satellite chain entail. Differences in configuration are unaccounted for, and so results could vary if the proposed configuration in practice was significantly different from those in Micius.

C. A Further Look at Orbit to Orbit Satellite Networks

Liorni et al paper Quantum Repeaters In Space 2021 [29] proposes another satellite to satellite network, combined with quantum repeaters utilising entanglement generating protocols between one another to reach two ground-based end nodes.

Much like the previous paper but Gundogan et al., this proposal addresses the issue of weather-based losses via a hybrid satellite-ground scheme with a concatenated system of repeaters within space. However, what they do is raise the question of satellite configuration in space, raising a "string of pearls" around the earth configuration, to guarantee continuous and global coverage. This configuration avoids both the link loss caused within ground-based examples and also the loss via cloudy weather conditions. It is noted in this paper that the lower loss rates mean that fewer repeaters are needed, leading to eliminating some area for potential unavoidable coherence loss that occurs within a repeater.

This paper shows that repeaters in this orbital configuration would improve the secret key rate amongst the nodes for distances below 6,000 km, which is much greater than what we find with Micius, where the hybrid orbit-ground scheme decays exponentially with distance.

The proposal does have some strengths compared to other methods. The secret key rate attained by the researchers is greater compared to readings present in employing purely ground-based repeaters. Low Earth Orbit Satellites are preferred for their lower costs and shorter distances which reduce the entanglement fidelity link loss. Due to the curvature of the earth the distance is limited to a maximum distance that Liorni posits at round 1500 – 2000 km.

While Gundogan et al. focussed on the memory technology in their assessment of their paper, the focus on this paper was the practical cost of implementation of such a system; comparing to the Shanghai-Beijing setup, Liorni et al. calculated end up with the orbit-to-orbit setup costing round 50% more than Orbit-to-Ground, whilst arguing that OO boasts a performance boost of factor 1000, higher key rate and network availability. Absent from Liorni's calculations are the cost of maintenance for the satellites, and so the total costs could likely run significantly higher.

Finally, when we compare the assessment of Gundogan et al. they showed that to achieve the required key rates for practical usage, we would need to dramatically increase the number of quantum memories within the satellites; that assessment also rings true here as as the same practical technology was suggested.

D. Repeater Technology and Recent Developments

As discussed above, repeater technology and quantum memory technology needs improvement before its practical implementation is possible. Below, we will examine two recent developments in the field of quantum repeaters – one utilising atom to photon entanglement and another, utilising no memory. We will analyse these and draw conclusions on what they can mean for the future of QKD networks utilising quantum repeaters.

1) Cavity Quantum Electro-Dynamic Repeaters:

Quantum Key Distribution is the means to which Langenfeld et al. [30] seeks to test the theoretical protocol proposed by Luong [31] where two atoms in an optical cavity can distribute entangled photons via entanglement swapping. The experiment uses an optical cavity as a light-matter quantum interface to generate atom-photon entanglement, and then two individual atoms stand in place as two distinct high-fidelity quantum memories. The optical cavities heavily rely upon Cavity Quantum Electrodynamics (CQED), the interaction between light confined in a reflective cavity and atoms. Cavity QED allows for the performance of the Bell-State Measurement, the result of which is used by the entangled partner to reconstruct the original state of a teleported particle, thereby performing entanglement swapping. This protocol provides a modular building block that possible concatenation methods to assemble into a suggested networks, are discussed below.

Previous results showcase the ability to produce quantum repeaters from memory atoms but do not sufficiently meet the required error threshold of 11% [32] necessary to perform quantum error correction [33]. The results of this experiment beat this threshold, serving as an important step to prove that unconditional secure communication is possible.

There is one thing to consider within this experiment the general design of the repeater: because photons are send outward from the repeater to each node, it is not possible to chain each of these together in the previously in the previously described repeater architecture as of yet, because we do not have a means to entanglement swap between photons at the receiver nodes.

This limits the practical application of these would therefore be limited to extending the current range of QKD by one hop, but providing unconditionally secure QKD in the form of

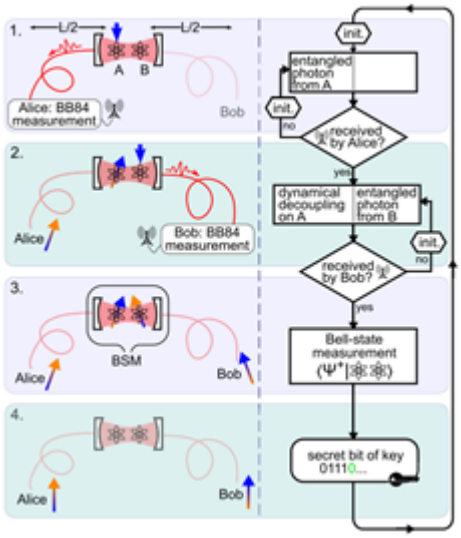

Fig. 7. Quantum Repeater Scheme. Two atoms in a cavity serve as a repeater node

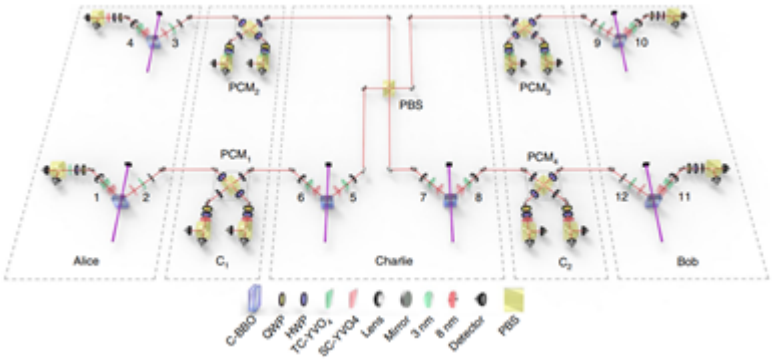

Fig. 8. Experimental Setup showing the six crystal pairs and paths

entanglement swapping; or by implementation within trusted node networks, reducing the overall requirement for trusted nodes by over a half.

However, if and when photonic entanglement is developed, other research with Cavity QED demonstrates that it is possible to perform quantum logic gates[34] which would allow for entanglement purification that in turn boosts the fidelity of the qubit, thereby bolstering the case for repeater's use inside of a quantum network.

When we perform entanglement swapping, we will need to maintain their information for as long as it takes to transmit the entanglement through however many repeaters it takes to sustain a high-fidelity transmission between very distant end users. In a field where we are now seeing an upshot of 70 repeater nodes such as in Wuhan, we quickly begin to lose coherence. If the Entanglement swapping takes too long, decoherence renders the information stored on the qubits illegible. The authors do mention that dynamic decoupling is used to improve coherence time from below 1ms to 20ms, but we would still require a larger coherence time for qubits to accommodate.

Finally, the paper sets the direction of scope of future experiments, saying that they could double coherence time from 20ms to 40ms by applying the previous work on repeater nodes by Luong et al.[31], only that the experiments needed to double the coherence time requires more technologically advanced atom trapping and cooling methods. Once these requirements are accommodated for, the experiment can be repeated and chained to a network of repeater nodes.

2) All photonic, Memory-less Repeaters:

Throughout this paper we have addressed the need for the development of quantum memories within repeater architecture and this idea is based on one fundamental assumption; a repeater will generate forward entanglement once it has received entanglement from the prior node. Another approach that could be taken is to constantly be producing entanglement between nodes in the network, ready for the moment that an end to end link is required. Theoretically, this reduces the memory requirement as entanglement will be instantaneously (or near as) swapped with the next node.

This is highlighted in the QLE ratio mentioned above, which is a rate of entanglement generation : rate of decoherence of the qubit. In this example, the rate of entanglement generation would always be kept high and the rate of decoherence would always be kept low, or lower than that of a repeater utilising memory, as it wouldn't be subject to potential fidelity loss or decoherence on storage.

Li et al. papers Experimental Quantum Repeater without Quantum Memory, based off of Azuma's 2014 proposals[35], explores this avenue, with the generation of an all-photonic, memory free, repeater. The process involves using a pulsed ultra-violet laser to transmit a photons through six separate sandwich-like crystal pairs, generating six entangled pairs. Through this method, twelve photons are used to entangle qubit information to the other side at a faster rate than what is currently achieved by parallel entanglement swapping. The faster rate of transmission means that we protect against photon loss and avoid the coherence time limitations that require quantum memories and for the longer distances that we now see in recent experiments discussed further within this essay.

After the transaction, the density matrix is reconstructed via standard (tomographical) methods with a fidelity readout of 0.606. Hypothetically combined with error correction and quantum purification, this fidelity readout is more than successful to be passed on, a crucial element of implementing a repeater.

The paper is notable because it provides a proof-of-concept that supersedes the coherence time problem that stifles other experiments that rely upon quantum memories, whilst also providing a resilience against photonic loss as required within a scalable quantum network. It is speculated at the end of the paper that their repeater work could compliment a large-scale

network setup where their technology could reduce the need for quantum memory during the transit.

The researchers admit that even with Quantum Memory removed from the intermediate nodes, the end nodes still require it if Alice and Bob require a quantum output state, say in a large-scale concatenated network. Despite this, the memory time at the end nodes here would only scale linearly with communication distance, theorised by Azuma [35], whilst current conventional proposals of quantum repeaters scale exponentially with larger distances.

There are some notable downsides to this experiment. Firstly, admitted by the authors, the demonstration of an all-photonic setup is difficult because of the need to prepare a large repeater graph state of photons. Whilst convenient in this setup to simplify the experiment for a proof of concept, if we are to take advantage of an all-photonic repeater in the future, a more robust implementation must be available to handle all sorts of setups and environments.

While the lack of memory may initially seem enticing, this means that if there is no entanglement ready to swap with when a qubit arrives at the repeater, and the same at every subsequent repeater, the entire link would fail. The delicate construction of the repeater has not thus far been tested within fibre optic networks or in satellites, and so the repeater's resiliency to external noise decoherence is an unknown. So, although the tests have demonstrated a proof-of-concept for an all-photonic quantum repeater, expanding out to large scale networks utilising increasing numbers of these repeaters seems somewhat impractical.

IV. Conclusion

Our vision would be to have a way in which everyone, down to the consumer level, would have access to quantum encrypted communication methods. We believe that in order to do so, the requirements are multifaceted and that scalability of QKD will come down to a number of factors: key rate, transmission distance, and just as importantly, practicality. We structured this survey in such a way, to tell a story of the state of art, and to lead a path forward for future investigation.

We have demonstrated technologies, that show promise: fibre networks in metropolitan areas showing fantastic sustained key generation. Satellite technology that can be used to cover larger distances, and even provide for a bridge between those metropolitan networks. The security concerns over the use of trusted node networks as well as how impractical the current tests with satellite technology are, are clear, but we have also presented papers that show a path forward – moving to untrusted repeaters and papers that look into key rate transmission in satellites and how the configuration of the satellites in orbit can play a part. We have also demonstrated how ad hoc networks could be created in the future, with interesting and novel experiments into the use of drones.

Finally, we posit that the true way forward for QKD mirrors that of the quantum internet – Kozlowski and Wehner in Towards Large-Scale Quantum Networks[21] suggested that early stage quantum networks would need improvements in a number of areas and cited the use of untrusted long-distance communication as the first area. In agreement, we made that the second part of our paper, looking to the future possibility of QKD. Within that section, we analysed papers looking at the most recent repeater technology, the key stumbling point for quantum networks at this moment, analysing two papers in particular. An interesting point about both of these studies, and the reason they were both chosen, is that their potential downsides are both complimentary to one another:

1) In the QED repeaters, we have examples that show good error thresholds indicating the memory may be practical for implementation – however, because of the outward direction of photons from either side of the repeater, it wasn't practical to implement them into large scale networks.
2) In the all photonic memoryless repeaters, we mentioned how their implementation is impractical because of the requirement to always have entanglement readily available and nowhere to store.

What's interesting about these together is that the technology appears to fit like a jigsaw – where we believe some investigation into a network utilising both of these technologies in alternating fashion, could provide a first true path forward.

The problems of photonic entanglement swapping with the QED repeaters would be removed with the memoryless repeaters, and the impact of requiring entanglement to be always ready for forward swapping in the memoryless repeater, would be mitigated by the memory developments within the QED repeater.

What is clear from our research, is that the effort to establish working quantum networks is both broad and impressive, but there are many research obstacles to overcome before our vision will become a reality

References

[1] "What is a Qubit? — Microsoft Azure", Azure.microsoft.com, 2022. [Online]. Available: https://azure.microsoft.com/en-us/overview/what-is-a-qubit/qubit-vs-bit. [Accessed: 22- Jan- 2022].

[2] Y. Cao, J. Romero and A. Aspuru-Guzik, "Potential of quantum computing for drug discovery," in IBM Journal of Research and Development, vol. 62, no. 6, pp. 6:1-6:20, 1 Nov.-Dec. 2018, doi: 10.1147/JRD.2018.2888987.

[3] Alcazar, Javier, Vicente Leyton-Ortega, and Alejandro Perdomo-Ortiz. "Classical versus quantum models in machine learning: insights from a finance application." in Machine Learning: Science and Technology vol.1.3 2020: 035003.

[4] I. Kassal, J. Whitfield, A. Perdomo-Ortiz, M. Yung and A. Aspuru-Guzik, "Simulating Chemistry Using Quantum Computers", Annual Review of Physical Chemistry, vol. 62, no. 1, pp. 185-207, 2011. Available: 10.1146/annurev-physchem-032210-103512

[5] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?," in IEEE Security Privacy, vol. 16, no. 5, pp. 38-41, September/October 2018, doi: 10.1109/MSP.2018.3761723.

[6] S. Lynch, J. Borresen and K. Latham, "Josephson junction binary oscillator computing", 2013 IEEE 14th International Superconductive Electronics Conference (ISEC), 2013. Available: 10.1109/isec.2013.6604275

[7] Quantum Flagship, Quantum Repeaters, VDI Technologiezentrum GmbH, VDI-Platz 1, D-40468, Düsseldorf, Germany, 2020. Accessed on: Jan 18, 2022 [Online]. Available: https://qt.eu/discover-quantum/underlying-principles/quantum-repeaters/

[8] M. Mehic et al., "Quantum Key Distribution: A network perspective", ACM Computing Surveys, vol. 53, no. 5, pp. 1-41, 2020. Available: 10.1145/3402192 [Accessed 22 January 2022].

[9] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters, vol. 85, no. 2, pp. 441-444, 2000. Available: 10.1103/physrevlett.85.441

[10] Y. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres", Nature, vol. 589, no. 7841, pp. 214-219, 2021. Available: 10.1038/s41586-020-03093-8

[11] A. Gaidash, V. Egorov and A. Gleim, "Revealing beam-splitting attack in a quantum cryptography system with a photon-number-resolving detector", Journal of the Optical Society of America B, vol. 33, no. 7, p. 1451, 2016. Available: 10.1364/josab.33.001451

[12] M. Rau et al., "Spatial Mode Side Channels in Free-Space QKD Implementations," in IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 187-191, May-June 2015, Art no. 6600905, doi: 10.1109/JSTQE.2014.2372008.

[13] D. Gottesman, H.-K. Lo, N. L ¨utkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Information Computation, vol. 4, no. 5, pp. 325–360, 2004.

[14] J. Dynes et al., "Cambridge quantum network", npj Quantum Information, vol. 5, no. 1, 2019. Available: 10.1038/s41534-019-0221-4

[15] C. Simon, "Towards a global quantum network", Nature Photonics, vol. 11, no. 11, pp. 678-680, 2017. Available: 10.1038/s41566-017-0032-0

[16] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," in IEEE Journal of Selected Topics in Quantum Electronics, vol. 9, no. 6, pp. 1541-1551, Nov.-Dec. 2003, doi: 10.1109/JSTQE.2003.820918.

[17] C. Erven, "On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source", Hdl.handle.net, 2022. [Online]. Available: http://hdl.handle.net/10012/3021.

[18] Madrid Quantum Network: A First Step To Quantum Internet", in ARES 2021: The 16th International Conference on Availability, Reliability and Security, Vienna Austria, 2021.

[19] H. Liu et al., "Drone-based entanglement distribution towards mobile quantum networks", National Science Review, vol. 7, no. 5, pp. 921-928, 2020. Available: 10.1093/nsr/nwz227

[20] S. Isaac et al., "Drone-Based Quantum Key Distribution", Conference on Lasers and Electro-Optics, 2020. Available: 10.1364/cleo_at.2020.jw2a.16

[21] W. Kozlowski and S. Wehner, "Towards Large-Scale Quantum Networks", Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, 2019. Available: 10.1145/3345312.3345497

[22] M. Nielsen, "The Entanglement Fidelity and Quantum Error Correction", arXiv preprint quant-ph/9606012, 1996.

[23] T. Chen et al., "Implementation of a 46-node quantum metropolitan area network", npj Quantum Information, vol. 7, no. 1, 2021. Available: 10.1038/s41534-021-00474-3 [Accessed 22 January 2022].

[24] H. Lo, M. Curty and B. Qi, "Measurement-Device-Independent Quantum Key Distribution", Physical Review Letters, vol. 108, no. 13, 2012. Available: 10.1103/physrevlett.108.130503

[25] H. Liu et al., "Experimental Demonstration of High-Rate Measurement-Device-Independent Quantum Key Distribution over Asymmetric Channels", Physical Review Letters, vol. 122, no. 16, 2019. Available: 10.1103/physrevlett.122.160501

[26] M. Gundogan, J. Sidhu, V. Henderson and L. Mazzarella, "Space-Borne Quantum Memories for Global Quantum Communication", Quantum Physics, 2020.

[27] S. Abruzzo, H. Kampermann and D. Bruß, "Measurement-device-independent quantum key distribution with quantum memories", Physical Review A, vol. 89, no. 1, 2014. Available: 10.1103/physreva.89.012301

[28] C. Liorni, H. Kampermann and D. Bruß, "Quantum repeaters in space", New Journal of Physics, vol. 23, no. 5, p. 053021, 2021. Available: 10.1088/1367-2630/abfa63

[29] S. Langenfeld, P. Thomas, O. Morin and G. Rempe, "Quantum Repeater Node Demonstrating Unconditionally Secure Key Distribution", Physical Review Letters, vol. 126, no. 23, 2021. Available: 10.1103/physrevlett.126.230506

[30] D. Luong, L. Jiang, J. Kim and N. Lütkenhaus, "Overcoming lossy channel bounds using a single quantum repeater node", Applied Physics B, vol. 122, no. 4, 2016. Available: 10.1007/s00340-016-6373-4

[31] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters, vol. 85, no. 2, pp. 441-444, 2000. Available: 10.1103/physrevlett.85.441

[32] A. Stephens, "Fault-tolerant thresholds for quantum error correction with the surface code", Physical Review A, vol. 89, no. 2, 2014. Available: 10.1103/physreva.89.022321

[33] S. Welte, B. Hacker, S. Daiss, S. Ritter and G. Rempe, "Photon-Mediated Quantum Gate between Two Neutral Atoms in an Optical Cavity", Physical Review X, vol. 8, no. 1, 2018. Available: 10.1103/physrevx.8.011018

[34] K. Azuma, K. Tamaki and H. Lo, "All-photonic quantum repeaters", Nature Communications, vol. 6, no. 1, 2015. Available: 10.1038/ncomms7787

[35] Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres", Nature, vol. 582, no. 7813, pp. 501-505, 2020. Available: 10.1038/s41586-020-2401-y