# Attacking the Quantum Internet

Takahiko Satoh, Shota Nagayama, Shigeya Suzuki, *Member, IEEE*, Takaaki Matsuo, and Rodney Van Meter, *Member, IEEE*



***Abstract*—The main service provided by the coming Quantum Internet will be creating entanglement between any two quantum nodes. We discuss and classify attacks on quantum repeaters, which will serve roles similar to those of classical Internet routers. We have modeled the components for and structure of quantum repeater network nodes. With this model, we point out attack vectors, then analyze attacks in terms of confidentiality, integrity and availability. While we are reassured about the promises of quantum networks from the confidentiality point of view, integrity and availability present new vulnerabilities not present in classical networks and require care to handle properly. We observe that the requirements on the classical computing/networking elements affect the systems' overall security risks. This component-based analysis establishes a framework for further investigation of network-wide vulnerabilities.**

***Index Terms*—Quantun Internet, Quantum network security.**

## I. Introduction

THE computers and networks in common use today are built on classical notions of information, generally using small amounts of electrical charge, the orientation of tiny magnets, and optical signals as data. We typically treat the data states as binary numbers or symbols and manipulate them using familiar, comfortable Boolean logic. But over the last three decades, a new theory of information based on quantum mechanics has been discovered, quantum algorithms have been developed, experimental demonstrations of quantum computing have proliferated, and large-scale machines are on the drawing boards [3], [61], [75], [82]. One of the oldest and most successful areas in quantum information has been quantum networks [20], [45], [74], [79], [84].

Work on quantum networks began with the recognition that quantum states serve as exquisite sensors of the real world, and can be used to detect the presence of eavesdroppers on a quantum communication channel while creating shared, secret random numbers useful as keys for encrypting classical data, known as quantum key distribution (QKD [8], [26]). The array of proposed applications for distributed quantum information has grown to include other cybernetic uses such as clock synchronization, reference frame alignment, and interferometry for astronomy [4], [32], [43]. Distributed quantum computation will help to build large scale quantum computers, especially by combining heterogeneous quantum modules. [16], [33], [60], [70], [76]. The development of large-scale quantum computers would affect classical security systems that depend on the difficulty of certain computational problems, but conversely distributed security-related functions such as Byzantine agreement and secret sharing recoup some of those losses [7], [19]. Broadbent *et al*. developed a fully blind method of conducting any arbitrary quantum calculation (BQC [14], [15]). Unlike Gentry's classical homomorphic encryption [30], this technique hides the algorithm itself as well as the input and output data. Thus, if we can find ways of distributing quantum information over long distances, we will enable valuable new functionality.

Quantum entanglement is a correlation between the states of two or more quantum variables, stronger than any possible classical correlation [34], [81]. Although entanglement cannot be used to transmit information faster than the speed of light, two quantum variables may be in an entangled state where their values are decided randomly but seemingly in an instantaneously coordinated fashion without any apparent communication. This phenomenon worried Einstein enough that he dubbed it "spooky action at a distance." Many of the applications just discussed require us to create this entanglement over a distance. Quantum repeaters (Sec. II) are an important path toward building a Quantum Internet that will achieve this goal.

The early use of the quantum Internet with high noise levels would be to enhance Internet security with QKD [21], [27], [28]. Various attack methods for preventing such security improvement have already been proposed [31], [40], [50], [51], [65]. Defense methods, operational methods with optimal efficiency, and specific methods for combining with classical protocols have also been proposed [1], [12], [53] Urban-scale networks have already been built by trusting intermediate nodes to avoid the requirement of quantum repeaters, and their performance has been demonstrated [64], [68], [71], [78].

The classical Internet, the global-scale network, has emerged over some five decades, and security is a major area in research, engineering and operations [6]. Both hardware and software evolve quickly, and both attacks and defense applied to network infrastructure and end nodes emerge at an astounding rate. Some attacks compromise individual computers or data, either during the initiation or data transfer phases of a communication session, by spoofing data packets, hijacking connections, or cracking encryption. Attacks on sessions can also be attempted more speculatively by compromising systems, then laying in wait for opportunities to present themselves. Other vulnerabilities affect the stability of the network itself by disrupting routing or naming systems, or by flooding portions of the network with excess traffic. Such vulnerabilities and attacks have to be discussed to design secure quantum Internet architectures.

In this paper, we summarize and develop primitive models

T. Satoh, S. Suzuki, and R. Van Meter are with Keio University.

S. Nagayama is with Mercari, Inc.

T. Matsuo was with Graduate School of Media and Governance, Keio University, 5322 Endo, Fujisawa-shi, Kanagawa 252-0882 Japan E-mail: kaaki@sfc.wide.ad.jp.

Portions of this paper appeared in an NDSS workshop paper by S. Suzuki and R. Van Meter [72]. This paper also extends work from Satoh *et al.* [69]

of attacks on individual components of quantum networks. Attackers' purpose may be parallel to those in classical networks:

- *to steal* quantum information; or
- *to hijack* a quantum connection; or
- *to disrupt* either the integrity or availability of quantum nodes or quantum networks; or
- *to hijack* computing resources such as controls of quantum repeaters or external components.

The biggest difference between classical/quantum networks is the presence of entanglement. This difference raises questions:

- Can the use of entanglement results in copying or disclosure of quantum data during a session?
- Can entanglement lurking in a repeater compromise later sessions by hijacking valuable qubits or undetected disclosure?

Even without entanglement, new questions are raised, such as

- Can control of the quantum hardware elements allow hijacking or disclosure? (classical hardware is vulnerable to damage from strong electrical or optical pulses)
- Are quantum nodes more vulnerable than classical systems? (This question is dependent on implementation, and is a moving target we will not address here.)

More generally, to have the quantum Internet scalable,

- can the function of creating end-to-end entanglement be disrupted on a scale disproportionate to the fraction of the network compromise?

While attacks attempting theft target operations of a communication session, this question conjures effects to fundamental network functionalities such as routing [77]. The discussion to answer these questions must last long in the future. This paper gives the first framework to categorize attacks in pursuit of these goals.

To classify attacks on quantum networks, it would be valuable to refer to proposed taxonomies for classical systems, especially RFID systems, by Weingart [80], Mitrokotsa [55], and Mirowski [54]. Quantum repeater systems and RFID systems have similar properties that make this analogy apt: both systems are tightly coupled hybrid systems of sensing and software elements, and also expect to make use of the effects of interaction with the outside world, and hence are sensitive to noise or deliberate inputs.

While we can model the basic hardware architecture of a quantum network nodes and have some idea of required elements, a concrete design for a specific implementation of such a system has not been achieved yet. We begin with an overview of the Quantum Internet (Sec. II) and a hardware model that will allow us to identify points of attack, then classify the primitive attacks (Sec. III). We then investigate the means of attack on the Quantum Internet through the elements of the Quantum Nodes (Sec. IV), and also discuss what an attacker who has hijacked control of one or more Quantum Nodes can do (Sec. V). We believe that this paper will contribute toward designing secure quantum Internet architectures. In such work, knowledge gained during the engineering of classical networks will be beneficial to minimize security issues of developing quantum networks.

## II. Quantum Internet

We have already introduced the concept of quantum entanglement and what it is good for, but not how widely distributed entanglement can be created. A network of optical links connected by quantum repeaters will fill the role of classical network links and switches or routers. End nodes that can connect to the quantum network will provide various quantum services that enable the uses discussed above. As in the classical Internet, individual quantum networks of potentially heterogeneous technology and independent management will ultimately come together to form a Quantum Internet [74].

### A. The role of a Quantum Repeater

To perform long distance communication, a Quantum repeater must supply the following four functions.

*1) Node-to-Node Entanglement generation:* Experimental physicists have demonstrated the creation of entanglement over short distances using single photons (e.g. [56]). Numerous approaches have been proposed and some of them demonstrated, but for our purposes here a single example will suffice. Individual quantum bits, or qubits, at each node may be single atoms suspended in a vacuum or another of the dozens of technologies under experimental development. A qubit at each end of a link is coaxed to emit a photon that is entangled with the qubit. The two photons are routed toward each other and ultimately interfere in a fashion that erases knowledge of where each photon came from, leaving the two stationary qubits entangled in what is called a Bell pair, named for a proposal made by John Bell over fifty years ago [5].

*2) Stretching of Entanglement:* Unfortunately, we can't transmit those photons over arbitrary distances. In optical fibers, the probability of success falls exponentially with distance as photons are lost, and classical amplifiers cannot be used in quantum networks because independent copies of quantum data cannot be made [83]. Moreover, in any interesting network, naturally, we want to support multi-hop paths between pairs of nodes, rather than requiring a direct link between each pair. Both problems can be solved by using entanglement swapping, which takes two Bell pairs, one between nodes $A$ and $B$ and one between nodes $B$ and $C$, and splices them together to form a single Bell pair that spans from $A$ to $C$ [35]. Entanglement swapping can be said, very roughly, to perform the role held by packet forwarding in the Internet, with the significant caveat that it operates all along the path rather than at a node at a time.

*3) Management of errors:* The quality, or fidelity, of these Bell pairs declines as we perform more of these swapping operations, eventually destroying the quantumness of the data and leaving only random classical noise. This problem can be solved by using a form of error detection known as purification [10] or using quantum error correction [23], [22]. Purification plus entanglement swapping is the canonical setup of a chain of quantum repeaters [13].

*4) Participate in managing network:* Management of topology, routing, tomography, also presence of malicious actors, key point of this paper.

More than two qubits can be entangled at one time, either intentionally by the end nodes, by an eavesdropper trying to listen in, or as the quantum information leaks out of imperfectly isolated devices [63]. We can detect the presence of an eavesdropper and assess the fidelity of two-qubit entanglement using a process known as quantum tomography [2], [18], [37]. As we assess the fidelity of our two-party entanglement, we simultaneously attempt to rule out that a third party is entangled with us [17], [34], [47], [73]. This serves as the basis of one form of quantum key distribution [26]. This process requires the generation and consumption of many Bell pairs to determine the statistical characteristics of a quantum channel or path, and cannot be used to determine anything about any individual Bell pair. Selection of Bell pairs to be sacrificed for tomography must be random and secure; if the eavesdropper can predict which pairs will be used, she can remain undetected simply by choosing not to entangle or interfere with those pairs [69]. However, confidence in our assessment grows slowly as a full tomographic procedure converges incrementally by consuming substantial numbers of Bell pairs, so other approaches to state monitoring are under development; this remains an important research topic for robust, secure, efficient Quantum Internet operation [25], [62].

### *B. Types of nodes*

We can classify quantum network nodes (QNodes) under four types by the number of connected (quantum) links and their roles:

End node (ENode)

An ENode works as a terminal node for running quantum applications. In order to support various applications, qubit operations and memory functions are required. An ENode has exactly one external link and corresponds to clients and servers.

Measurement node (MNode)

An MNode is a terminal node just for measurement, used by end users for QKD or blind quantum computation [57], [58]. The only necessary function is to measure qubits, therefore an MNode has no static memory. An MNode has exactly one external link. We can regard an MNode as a simpler ENode.

Repeater (RNode)

RNodes are installed at fixed distances according to the optical fiber loss level to improve network performance in long-distance quantum communications [13]. An RNode has exactly two external links, so that it is useful in a line only. RNodes correspond to repeaters in classical networking.

Router (XNode)

An XNode has two or more external links, e.g. connected internally via an optical backplane [60]. XNodes have more substantial processing capacities than other node types and are responsible for branching the route of the network.

Fig. 1 depicts an example of a small quantum repeater network consisting of QNodes connected by quantum channels. QNodes are physically connected by a quantum communication-capable channel, such as optical fiber. Adjacent QNodes can create entanglement between their qubits. We assume that QNodes can classically communicate with any other QNodes via classical channels such as the Internet (not shown in Fig. 1). Therefore, security issues in classical communications share the situation with Internet security.

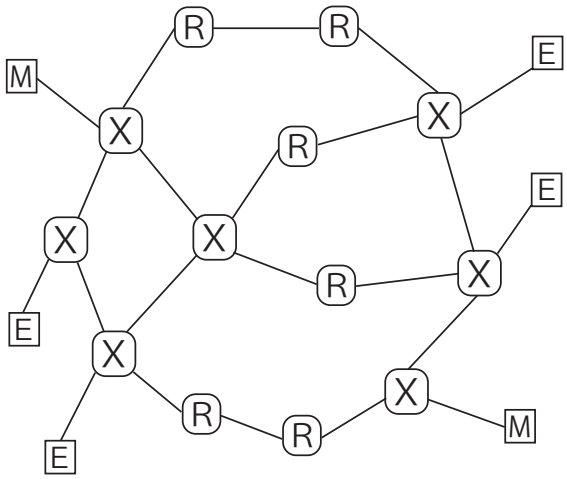



Fig. 1. Schematic diagram of interconnected nodes. Bell pairs can be shared directly between adjacent nodes. Classical communication is possible between all nodes. Distances will depend on technology, but most likely will be 10s of km over fiber.

Each QNode has network addresses, such as IP addresses, for various inter-repeater classical information communication. While our minimum requirement is having an address unique among the set of reachable quantum repeater nodes, to simplify our discussion, we assume all quantum repeater nodes have global Internet access, which means each quantum repeater node must have IP addresses. Topics that may require consideration in the context of a global-scale classical Internet, such as distributed denial of service (DDoS)-style attacks, are outside the scope of this paper.

### *C. Types of networks*

Types of quantum repeater networks are characterized by mechanisms for managing the two most important forms of errors: photon losses and state errors caused by gate errors and memory decoherence [59]. They are labeled in several generations depending on signaling directions transmitted by the used technologies:

1G repeater

Entanglement purification and acknowledged entanglement swapping are employed in this type [13], [24], [39], [67]. High fidelity Bell pairs are generated by entanglement purification with bidirectional classical communication (a two-way entanglement purification protocol, or 2-EPP) and those Bell pairs

are shared between non-neighboring repeaters using entanglement swapping [35]. This type is useful with low success rate, low fidelity, and a small number of qubit memories.

2G repeater

In this type, the network generates encoded Bell pairs between each nearest neighbor repeater pair and performs entanglement swapping to create encoded Bell pairs between arbitrary repeater pair [29], [38], [49], [46]. To create encoded Bell pairs over each link, we consume physical Bell pairs and perform unidirectional classical communication (a one-way entanglement purification protocol, or 1-EPP).

3G repeater

In this type of network, repeaters directly send quantum states that are encoded by QEC via unidirectional classical communication (1-EPP). This network type requires unacknowledged but heralded loss control to enable direct transmission of states. The individual links must have very high success probability for creating entanglement.

### D. Applications of a Quantum Internet

Based on the level of required functions, Wehner *et al.* classified the development of a Quantum Internet by stage and showed the applications provided at each stage (Tab. I [79]). Stage 1 applications are provided using trusted nodes with optical fiber or satellite links. Today, many researchers are promoting research aimed at higher stages, and this research also focuses on all stages.

| Stage of Quantum Internet | Examples of known applications |
|---|---|
| 1. Trusted repeater | QKD (no end-to-end security) |
| 2. Prepare and measure | QKD, secure identification |
| 3. Entanglement generation | Device independent protocols |
| 4. Quantum memory | Blind quantum computation, simple leader election and agreement protocols |
| 5. Few qubit fault tolerant | Clock synchronization, Distributed quantum computation |
| 6. Quantum computing | Leader election, fast byzantine agreement |

TABLE I
STAGES IN THE DEVELOPMENT OF THE QUANTUM INTERNET [79]. AS THE STAGE PROGRESSES, MORE ADVANCED HARDWARE IS REQUIRED TO DELIVER RICHER FUNCTIONS.

## III. HARDWARE MODEL OF THE QUANTUM INTERNET

In this section, we describe our models of QNodes and those elements. The ultimate purpose of the Quantum Internet, which consists of distributed QNode connected with both quantum channels and classical channels, is to create entanglement between two or more terminal application qubits in two distant QNodes chosen at the discretion of the application user. We assume each quantum node has a unique address. Since all quantum nodes require both quantum and classical communication, a natural approach is to use global IP addresses as an addressing scheme. This is also the most general, from the point of view of security analysis.

### A. Elements of a QNode

An MNode (Fig. 2a) has exactly one Quantum Network Interface Card (QNIC) assisted by a Node Controller (C4) and a Classical Network Interface Card (CNIC).

An ENode (Fig. 2b) has exactly one QNIC and an application module that has terminal qubits (QApplication), also assisted by a C4 and a CNIC.

An RNode (Fig. 2c) is built from exactly one CNIC and a C4, with exactly two QNICs, internally homogeneous device, internal operations all done via local gates; may incorporate BSA (Bell states analyzer) device, or may not.

An XNode (Fig. 2d) is built from multiple QNICs and Quantum Buffer (QBuffer), single CNIC and a C4.

We classify these components into two planes, classical and quantum, and elaborate below.

### B. Quantum plane elements of a QNode

Quantum Network Interface Card (QNIC)

A QNIC is a quantum network's equivalent of a classical NIC (Network Interface Card). Depending on the physical implementation, it may consist of transmitters, receivers or detectors, and qubits (QNIC qubits) used to create entanglement with a remote QNIC's qubits. A QNIC has both internal and external interfaces. An internal interface consists of both control and quantum connections to other elements in the QNode. An external interface is a quantum channel, combined with basic, hard real time classical signaling for framing and sequencing. A QNIC will be connected to a counterpart QNIC with a physical link such as fiber.

A hard real-time controller in a QNIC also handles all real-time operation, such as automatic creation of on-physical-link entanglement [66].

The node controller can direct the QNIC to operate on QNIC-qubits.

QBuffer

A QBuffer is a pool of qubits (Buffer-qubits) between a QNIC and a Switch or between QApplication and a Switch, that can be entangled then swapped with QNIC-qubits (or counterpart Buffer-qubits). QBuffer-qubits may have different physical characteristics than QNIC-qubits. A QBuffer may be optional depending on workload and hardware design, but our analysis assumes it is present.

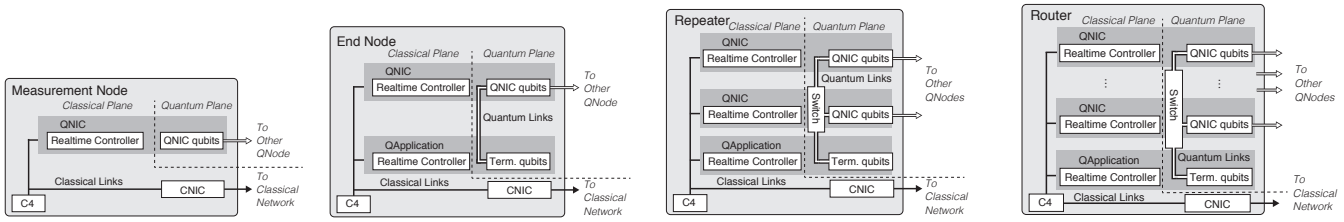
QApplication

A QApplication has terminal qubits, intended for quantum applications. These qubits can be entangled or swapped with QNIC-qubits, and hence can be entangled with remote QApplication-qubits.

QNIC-qubits

Each QNIC has multiple qubits (QNIC-qubits). QNIC-qubits are exposed to external channels and can create entanglements with remote QNIC-qubits.

Buffer-qubits




(a) MNode (b) ENode (c) RNode (d) XNode

Fig. 2. Model of QNodes. (a) MNode must be able to measure QNIC-qubits in any basis. MNodes may measure incoming qubits photon detectors. (b) ENode can perform universal computations on Terminal qubits. Like other QNodes, we can separate components into Quantum plane and Classical plane. (c) An RNode connects two non-adjacent QNodes. (d) XNode connects to several QNodes and is responsible for communicating on various routes.

Buffer-qubits in a QBuffer can hold entangled states but not optically connected to outside, freeing QNIC-qubits for reuse.

Terminal-qubits

Terminal-qubits in a QApplication.

Quantum node internal links

All quantum elements in a QNode are connected by quantum internal links.

Optical switch (Switch)

An optical switch (e.g., a nanomechanical crossbar [44]) changes the optical connections between quantum plane elements. Although such switches can be used in the long-distance optical paths [27], here we focus on use inside a node with multiple QNICs to achieve non-blocking photon routing. A node with a single or two QNICs would not need a Switch (Fig. 2).

### C. Classical plane elements of a QNode

Classical Network Interface Card (CNIC)

A CNIC is a standard classical network interface that can be connected to the classical Internet. We assume this to be an interface such as Ethernet. The CNIC provides inter-repeater and application node communications, generally carrying soft real time information necessary for interpreting quantum information and determining future operations.

Realtime Controller

A real-time controller controls the qubits in each unit, meeting the hard real time constraints for maintaining quantum states and performing operations on qubits either individually or collectively. In our current model, three types of real-time controller are shown: the QNIC real-time controller, the Buffer real-time controller and the Application real-time controller.

C4 (Node Controller)

The Classical Chassis Controller Card communicates with other QNodes and controls QNIC, QBuffer and QApplication to achieve its goal: for a repeater node, to create entanglement between a local QNIC-qubit and a remote QNIC-qubit; for an application node, to create entanglement between a local terminal qubit and a remote qubit via its QNIC-qubit, to run an application.

Classical node internal links

All classical elements in a QNode are connected by classical internal links.

Other classical computing elements

Since a QNode consists of hybrid classical computing elements and quantum elements, it also may have various classical computing elements such as clock, memory, processor, and chassis including expansion buses or backplanes.

### D. Elements of QNode to QNode connection and external resource

A QNode requires several external resources to operate.

Classical external connectivity

Through a CNIC, QNodes are connected to the Internet. All QNodes may communicate with each other via this external classical connectivity.

Quantum external connectivity

All QNICs are connected to other adjacent QNICs (or QNodes) via optical links so that each pair of directly connected QNodes needs to share Bell pairs as the first step of quantum communication. Such a link is point-to-point system for creating entanglement. A Bell pair are shared between non-adjacent QNodes by entanglement swapping operation at the relay QNodes, in first and second generation quantum networks. In third generation, an encoder forwarded to non-adjacent nodes.

We modeled three types of QNode-to-QNode connections, based on their schemes for generating Bell pairs [42]:

*1) Memory to Memory link ($M \rightarrow M$):* An $M \rightarrow M$ consists of two QNodes. One QNode receives a photon from a connected RNode (or ENode) and creates Bell pairs using a BSA (Bell states analyzer) entangler.

*2) Memories and BSA node link ($M \rightarrow I \leftarrow M$):* An $M \rightarrow I \leftarrow M$ consists of two QNodes and one standalone BSA node at the midpoint of the link. The BSA node receives a photon entangled with the QNIC-qubit in the connected QNode from each QNode, and create Bell pairs between the QNIC-qubits by measuring the photons together, using the BSA entangler.

*3) EPPS node and Memories link ($M \leftarrow S \rightarrow M$):* An $M \leftarrow S \rightarrow M$ consists of two QNodes and one standalone entangled photon pair source (EPPS) at the midpoint of the link. An EPPS creates photonic Bell pairs and transmits them to connected RNodes (or ENodes).

Standalone devices may have external classical links too.

## IV. Primitive Attacks on Quantum Nodes

In this section, we describe the primitive attacks on the quantum Internet, by element. Quantum network devices hold the quantum plane and the classical plane. The quantum plane holds qubits and quantum channels. The classical plane holds quantum application software, qubit controllers, classical channels, and operating systems. Both shares links. Primitive attacks come externally. (More complex attacks may be caused internally by the hijacked components; including physical security violation.)

This section summarizes how primitive attacks affect the security CIA (Confidentiality, Integrity, Availability). The CIA of Nodes and links introduced in Sec. III can be considered by combining elemental discussion of primitive components in this Section. Since quantum information has no-cloning theorem, confidentiality, integrity and availability have close linkage. For example, by stealing quantum data from a quantum variable, another value can be set in the quantum variable. In this case, an attack on confidentiality attacks integrity, too. The focus of this paper is categorizing attacks, hence such relationships are beyond the scope.

Functionality of quantum networks is to manipulate quantum data. In this sense, attacks on the quantum plane are fundamentally attacks on data. Attacks on classical plane are attacks on programs, as well.

### A. QNIC-qubits

QNIC-qubits in QNICs are used only temporarily. Once the entanglement which the QNIC-qubits hold is transferred to buffer-qubits or terminal-qubits, QNIC-qubits play no further role in that operation. QNIC-qubits are connected with other qubits either by the inter-node quantum channel or the in-node quantum channel (see below). Since optical fibers for inter-node quantum channel are attached to QNIC-qubits directly, interface qubits are most exposed to external risks.

*1) Quantum Plane:* Since interface qubits have direct contact with the world outside of the QNode via a physical quantum channel, they may be the most vulnerable elements.

- *Confidentiality*
  **Malicious entanglement** may QNIC-qubits have via the external quantum channel, by receiving maliciously entangled qubits or by having half Bell pairs sent from this interface entangled with malicious qubits by eavesdroppers' operations. Malicious entanglement would result the theft of valuable quantum data if quantum teleportation is following and executed without awareness of the attack. The essential countermeasure for this vulnerability is quantum state tomography. Assuming interface qubits are used to temporarily hold half Bell pairs (completely generic states with no secret information) before teleporting valuable quantum data, quantum state tomography randomly selects some of the Bell pairs to measure to determine if an eavesdropper has not entangled her qubits with ours, as we described in Sec. II. Target qubits must be isolated from external networks in this kind of verification scheme, because cracking of Bell tests via photon detector has been demonstrated [41]. If some half Bell pairs are entangled to qubits of eavesdroppers somehow such that only a few qubits are stolen so as to not be get detected by quantum state tomography, the confidentiality of valuable quantum data depends on that of the classical channel. This is because the quantum teleportation to transfer the valuable quantum data, which follows sharing Bell pairs, uses the classical channel. If the classical channel retains confidentiality, interface qubits also retains confidentiality. This is because the eavesdropper merely gets a completely mixed state in the absence of the observed value sent via the classical channel.
  **Optical probes** have been demonstrated. Among the many attacks on QKD implementations developed in Makarov's lab, Jain et al. described an eavesdropper that can probe a BB84 quantum key distribution (QKD) system [8] by sending a bright pulse from the quantum channel into the interface and analyzing the back-reflected pulses [36], a classical attack on the hardware used for the quantum states. Though entanglement-based QKD protocols do not have this weakness, a similar attack in which some optical detectors are saturated could be used in a man-in-the-middle attack.
- *Integrity*
  **Malicious entanglement** affects QNIC-qubits, therefore disrupts the integrity.
  **Fault injections** on interface qubits may involve inserting unauthorized and unexpected optical pulses into the quantum channel [11], [48].
  **Out-of-system attacks** such as direct irradiation of a device with RF noise could damage the quantum data and leave garbage. Such attacks may work as any quantum operation, including non-computational operation, such as leakage from computational basis. For that kind of attack, an attacker may not even need access to the target device itself, as radio waves can blanket an area from a modest distance. Even with good RF shielding, interference effects as weak as subway power and control systems a kilometer away are known to affect some systems.
- *Availability*
  **Malicious entanglement** to steal quantum data may result in disruption of the availability due to no-cloning theorem [83].
  **Fault injections** may disturb the state of interface qubits, affecting availability.
  **Blinding of detectors** by inserting optical pulses results in failure of detecting photons.
  **Out-of-system attacks** such as RF noise affect availability too, by preventing the designed operation of qubits. Other attacks, such as on the cooling or other control systems, may be harder to carry out remotely.
  **Destruction or removal of hardware** and other typical classic attacks prevent the designed operation of the qubits, if the attacker has access to the target device.

*2) Classical Plane (interface qubit controller):* Since interface qubits are controlled by a classical controller, a compromise on the controller side (software or hardware) allow crackers to control interface qubits arbitrarily, depending on implemented operations.

- *Confidentiality*
  **Hijacked controller** may disclose the quantum data via any session, disrupting the confidentiality.
- *Integrity*
  **Hijacked controller** may manipulate qubits to alter values coherently in chosen ways such as flipping bits, to measure values, or to initialize values, disrupting the integrity.
- *Availability*
  **Hijacked controller** may disrupt availability for arbitrary sessions.

### B. Buffer-qubits

Buffer-qubits are used for temporal buffering for in-node qubit transmissions. Buffer-qubits can interact with either interface qubits or terminal qubits. Since buffer-qubits themselves do not have any external connectivity, they are not exposed to risks from external (inter-node) quantum channels or that from the application side of other hardware directly.

*1) Quantum Plane:* Data in a classical memory buffer can be assumed to be "safe", untouchable from the outside world provided the buffer cannot be reached by DMA hardware that can be activated from outside and the host OS has not been compromised. Our quantum data are similarly safe from fault injection once stored in terminal qubits. Even if an eavesdropper has entangled a qubit of hers with our quantum variable before it reaches this buffer, she gains no access to information she did not already have at the time she entangled her qubit with ours. Randomized quantum tomography while working with a stream of Bell pairs is needed here as well as on interface qubits.

- *Confidentiality*
  **Malicious entanglement** may be inserted via QNIC-qubits, terminal-qubits, or other buffer-qubits.
- *Integrity*
  **Malicious entanglement** and **Out-of-system attacks** are threats against confidentiality of buffer-qubits as well as QNIC-qubits.
- *Availability*
  **Malicious entanglement**, **Out-of-system attacks**, and classical attacks such as **Destruction or removal of hardware** are threats against availability of buffer-qubits as well as QNIC-qubits.

*2) Classical Plane (interface qubit controller):* As well as QNIC-qubits, compromises on classical controllers are serious threats.

- *Confidentiality*
  **Hijacked controller** may disclose the quantum data via any session, disrupting the confidentiality.
- *Integrity*
  **Hijacked controller** may manipulate qubits to alter values coherently in chosen ways such as flipping bits, to measure values, or to initialize values, disrupting the integrity.
- *Availability*
  **Hijacked controller** may disrupt availability for arbitrary sessions.

### C. Terminal-qubits

The ultimate goal of the Quantum Internet system is to create entanglement among qubits in QApplication. The quantum application executes quantum operations only on terminal-qubits. Quantum end node must have terminal-qubits; quantum repeater and quantum router optionally may have them. Since terminal-qubits themselves do not have any external connectivity, they are not exposed to risks from external (inter-node) quantum channels directly. However, since it is assumed that the quantum application can execute any quantum operation on the terminal-qubits, a compromise of the application software is a compromise of the terminal-qubits.

*1) Quantum Plane:* Discussions for buffer-qubits can be applied to terminal-qubits, but for compromise of the application software.

- *Confidentiality*
  **Malicious entanglement** may be inserted via QNIC-qubits, or other buffer-qubits.
- *Integrity*
  **Malicious entanglement** and **Out-of-system attacks** are threats against confidentiality of terminal qubits, as well as QNIC-qubits and buffer-qubits.
- *Availability*
  **Malicious entanglement**, **Out-of-sytem attacks**, and classical attacks such as **Destruction or removal of hardware** are threats against availability of terminal-qubits, as well as QNIC-qubits and buffer-qubits.

*2) Classical Plane:* Terminal-qubits are controlled by a quantum application controller. Therefore, a compromise on the application side of the hardware affects terminal-qubits. Since the application controller is not a networking functionality, the detail of this loss of control is beyond scope of this paper. However, such threats from applications need careful discussion.

- *Confidentiality*
  **Hijacked controller** may disclose the quantum data via any session, disrupting the confidentiality.
  **Malicious application** may disclose the quantum data via any session, disrupting the confidentiality. Since fundamentally other components are not made to detect abnormalities of quantum applications, malicious applications are hard to detect.
- *Integrity*
  **Hijacked controller** and **Malicious application** may manipulate qubits to alter values coherently in chosen ways such as flipping bits, to measure values, or to initialize values, disrupting the integrity.
- *Availability*
  **Hijacked controller** and **Malicious application** may disrupt availability for arbitrary sessions.

### D. In-node quantum channels

In-node quantum channels provide interconnection between terminal-qubits, buffer-qubits and interface qubits. Since in-node quantum channels are not exposed to the outside of the node, attacks require indirect access or physical access to the hardware.

- *Confidentiality*
  **Optical probes** are not executable on the in-node quantum channel without directly modifying the hardware.
- *Integrity*
  **Out-of-system attacks** would alter the state of qubits.
  **Fault injections** are not executable on the in-node quantum channel without directly modifying the hardware.
- *Availability*
  **Destruction or removal of hardware** and **Out-of-system attacks** may compromise availability.

### E. In-node classical channels

Here we stick to in-node classical channels as a subsystem of in-node qubit transmission functionality, such as transferring meta-information, Pauli frames[1] or acknowledgments on of quantum channels. Since in-node classical channels are not exposed to the outside of the node, attacks require indirect access or physical access to the hardware.

- *Confidentiality*
  **Hijacked controller** may leak at most meta-information, such as session information and the usage.
- *Integrity*
  **Hijacked controller** may change management information such as Pauli frames, resulting in altering quantum states.
- *Availability*
  **Hijacked controller** can behave as if the channel is out of order. It also can sabotage particular sessions, by abusing probabilistic nature of quantum channels.

### F. Inter-node quantum channels

By using an inter-node quantum channel, node-to-node single hop entanglement is created between interface qubits. Since inter-node quantum channels are exposed, they are potential targets of attacks.

- *Confidentiality*
  **Eavesdropping** on photons flying in fibers affects confidentiality if valuable quantum data is encoded onto photons. Transferring half Bell pairs and executing quantum teleportation afterwards would protect valuable quantum data from eavesdropping as long as the operation is authenticated properly.
  A kind of **Optical probe** may be used to determine hardware settings, while the detector saturation attack described above could be used to control what the classical hardware sees. More analysis of this impact on repeater operation is necessary. Since an inter-node quantum channel is physically just a optical fiber or similar media between QNodes, it is relatively easy to get access to these channels.
- *Integrity*
  **Fault injections** exist and affect integrity by accessing fibers. The attack could be like a man-in-the-middle by cutting fibers and inserting hardware, or tapping the fiber. It is known that altering the temperature of fibers changes quantum states going through.
  **Photon injection** would be performed by an attacker via fiber, reaching detectors. Depending on the design of the repeaters, attacker also can inject photon that reaches QNIC-qubit in repeaters.
- *Availability*
  **Eavesdropping** works as an attack on availability, because it breaks the quantum states. This denial of service attack is one of the most obvious weaknesses of quantum networks if robustness is an important design goal. Since an inter-node quantum channel is just a fiber or such cable between QNodes, it is relatively easy to get access to these channels.

[1]The Pauli frame of a qubit defines its polarity relative to a reference signal.

### G. Inter-node classical channels

Inter-node classical channels are used to coordinate with other nodes, and used as a subsystem of in-node qubit transmission functionality. Since inter-node classical channels are exposed, they are potential targets of attacks. All classical attacks aimed at inter-node classical channels may be possible. Attacks specific to a quantum network system's classical channel might be possible in each of following categories.

- *Confidentiality*
  Vulnerable to classical attacks including but not limited to: **eavesdropping**, and other privacy threats such as **tracking**.
- *Integrity*
  **Hijacked controller** may change management information, resulting in altering quantum states.
  **Man-in-the-middle attack** can disrupt the generation of Bell pairs, in many ways, overwriting Pauli frames, disnegotiation, and so on. If Pauli frames are overwritten, it is difficult to determine whether the disturbance of the quantum state is caused by the attack on classical communication or quantum communication.
- *Availability*
  **Denial of Service attacks** disrupt the coordination messages, and obstruct such as ack messages for photons, hence affecting availability.

### H. Optical switch (crossbar)

Optical switches are settled in QNodes for switching quantum connections. Optical switches obey a routing table. Therefore a hijacked routing table data can makes the optical switch dysfunctional.

*1) Quantum Plane:*

- *Confidentiality*
  Attacks on the quantum plane of optical switches do not affect confidentiality, because an optical switch is

just a "pipe" of photons with switching paths classically obeying the controller.
- *Integrity*
  **Out-of-system attacks** would alter the state of photons during transfer, as well as in-node quantum channels.
- *Availability*
  **Destruction or removal of hardware** and **Out-of-system attacks** may compromise availability.

*2) Classical Plane:*

- *Confidentiality*
  **Switching disruption**, disobeying routing information, would forward quantum variables to eavesdroppers. This attack is achieved by **hijacked controller** of optical switches or by **falsified routing information**.
- *Integrity*
  **Switching disruption** would work as **malicious entanglement** and may result in inserting incorrect quantum variables.
- *Availability*
  **Switching disorder** affects availability.

### *I. Detectors with BSAs*

Detectors with BSAs are used to "connect" entanglement by entanglement swapping. Those detectors are connected to buffer-qubits, terminal-qubits or interface-qubits via an optical switch or directly. Detection is actually a conversion from quantum information to classical information. For XNodes, those (backplane) detectors are located behind the optical switch and are not exposed. For intermediate nodes, these detectors are optically connected to the inter-node channel directly and are exposed.

*1) Quantum Plane:*

- *Confidentiality*
  For XNodes, an detector is the dead end for photons and is not exposed. Hence the quantum plane does not affect confidentiality.
  If exposed, **Optical probes** may be used to determine hardware settings, or may be used to control what the classical hardware sees. Therefore confidentiality is affected.
- *Integrity*
  **Out-of-system attacks** would alter the quantum states.
  If exposed, **fault injections** to fake signals would be executable.
- *Availability*
  **Out-of-system attacks** would inject noise and correct signals become unrecognizable due to such noise.
  **Destruction or removal of hardware** may compromise availability.
  If exposed, **fault injections** may compromise availability.

*2) Classical Plane:*

- *Confidentiality*
  Attacks on the classical plane of detectors with BSAs may not affect confidentiality.
- *Integrity*
  **Falsified measurement outcome** by **hijacked controller** or by **out-of-system attacks** alters residual quantum states, affecting integrity.
- *Availability*
  **Hijacked controller** may sabotage sessions selectively.

### *J. EPPS*

An Entangled Photon Pair Source may be connected to inter-node quantum channels in intermediate nodes, or may be used along an in-node quantum channel in other nodes. EPPS is a simple component which continuously creates and sends entangled photons to connected two components. Hence, a complex attack is not achievable.

*1) Quantum Plane:*

- *Confidentiality*
  EPPS does not affect confidentiality.
- *Integrity*
  EPPS does not affect integrity.
- *Availability*
  By altering the power of input light would affect availability.

*2) Classical Plane:*

- *Confidentiality*
  EPPS does not affect confidentiality.
- *Integrity*
  **Hijacking** EPPS leads to generate a false bell pair.
- *Availability*
  **Attacks to clock synchronization** results in breaking availability.

### *K. Other components*

As component, optical switch (crossbar), detectors with BSAs, and EPPS would exist in quantum network devices. Those modules are actually discussed above as in-node quantum/classical channels.

Attacks on classical computing elements are well studied and explained by e.g. Weingart [80]. In our networks, the following classical computing elements have the potential to be attacked:

- CNIC
- Controller resources (such as clock, memory, processor)
- Chassis providing electric power.

## V. Attacks Using Hijacked QNode(s)

In this section, we investigate what attacker(s) can do if they successfully hijack full control of QNode(s).

The Quantum Internet will continuously use a certain amount of performance for cross-validation to detect anomalies such as equipment failures or hijacking [69].

- Each QNode regularly and continuously verifies neighboring nodes and their assigned communications.
- The network performs these verifications at irregular intervals during normal communication and eventually detects the presence of an attacker.

Under these circumstances, what can an attacker do with the hijacked node before her presence is detected? First, we discuss the case where the attacker successfully hijacked one QNode.

### A. Attacks by a malicious end user

What can a malicous terminal node, a MNode or an ENode, do to attack the network?

*1) False failure report:* An attack by a MNnode would be nothing more than a false report claiming a network failure for reduction of **availability**. If an attacker complains that an application such as BQC will not work, the network will need some work for careful self-verification. The network system can then conclude with a false claim or MNode failure.

*2) QDOS (Quantum Denial of Service attack):* A DOS (Denial of Service attack) attack is a typical **availability** attack on the classical Internet. Attacks on network resources, such as network bandwidth and server computing power, will also work against the Quantum Internet. Since the quantum state cannot be replicated [83], the damage will be more serious than the classical DOS. In particular, we should be wary of direct Qubit transmissions on 3G repeaters, if the data qubits themselves are sent via the Quantum Internet (If half-Bell pair is sent followed by quantum teleportation, it does not matter). As examples of QDOS, we assume the following attacks:

- A malicious user requests an oversized quantum key distribution for the quantum link bandwidth.
- A malicious user requests a massive number of calculations to a cloud quantum computer.

ENode and MNode are capable of these attacks.

As part of QDOS, an ENode can also perform some form of "eavesdropping" using fraudulently entangled qubits. Eavesdropping is very simple to implement given physical access to an ENode anywhere in the chain.

*3) Dishonest quantum computation:* An ENode can carry out more sophisticated attacks to reduce **integrity**. When we perform distributed quantum computation, it is risky to commit part of the calculation to an external ENode. An attacker could send incorrect quantum information via teleportation or perform wrong calculations. It is challenging to ensure the redundancy of quantum information by the no-cloning theorem. We need to perform calculations using trusted nodes, or adopt a method that allows reliable quantum calculations even with a small number of fraudsters.

### B. Attacks by a malicious repeater node

An RNode can perform all three types of attacks that ENode (MNode) can do because an Rnode has a higher-level function than ENode (see Fig. 2c).

*1) Composite attack:* The details of the attack by an RNode may differ depending on the role of the target node. For example, an RNode can perform the following attacks:

- Hijacked RNode does the Bell test to check the link status in good faith, and the work for the inter-node communication responds in bad faith. This attack will cause the network to suspect another node has failed.
- The attacker disables the inter-XNode link to which the RNode belongs due to an intentional RNode malfunction. Other communications must use other circuitous links, and attackers can achieve network inefficiencies.

We can classify these attacks into QDOS with dishonest quantum computation. To prevent more severe performance degradation, the network needs to perform a Bell test undetected by the attacker [69].

*2) Man in the middle attack:* This attack technique, which is popular in the classical Internet, can also be used in the Quantum Internet by using a hijacked RNode. For example, we assume a 1G network for QKD operation using BBM92 (Fig. 3) [9]. A and B share a Bell pair for quantum communication, so they ask E for entanglement swapping. The hijacked RNode E sabotages the instructions and continues to share the Bell pair with A and B. A and B try to generate a secret key via teleportation, but actually share the key with E, who is impersonating the other. E uses these keys to decrypt and re-encrypt the encrypted information transferred between A and B.

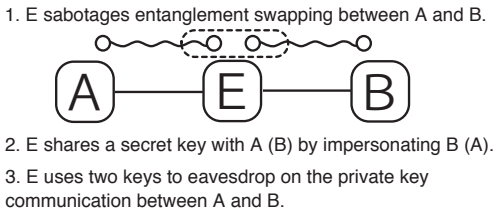



Fig. 3. Man in the middle attack on the Quantum Internet.

### C. Attacks by a malicious router node

An XNode is the most powerful QNode and can perform all the attacks that an RNode can do. When an attacker aims to maximize the hijacking time and the range of influence while remaining undetected, the following attack means are available in addition to the above attacks [69].

*1) Switching disruption:* An attacker can execute entanglement swapping without following the distributed ruleset [52], and forward the Qubit to a node far away from the destination (Fig. 4). We can detect the intentionally wrong entanglement swapping operation by Bell test, but we cannot avoid the negative effects on availability and integrity before the detection [69].

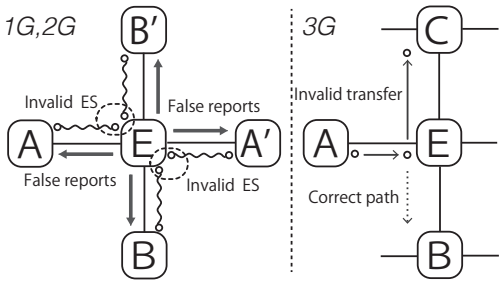



Fig. 4. With the 1G or 2G hijacked Xnode E, attacker can share Bell pairs between incorrect pairs $A-B'$ and $A'-B$ instead of correct pairs $A-A'$ and $B-B'$ using malicious entanglement swapping. In the case of 3G repeater network, intentionally qubits transfer to a inappropriate QNodes C instead of destination B. These disruptions decrease network availability and integrity of transferred information.

*2) Framing innocent repeaters:* The hijacker can frame another innocent QNode using the combination of false failure report and dishonest quantum computation. For every successful framing by hijacked Xnode, the processing power of the network is reduced. A lot of framing would eventually partition the network (Fig. 5), a very serious disruption. Even a single highjacked node can partition the network. To prevent such threats, we need to detect and respond as soon as possible.

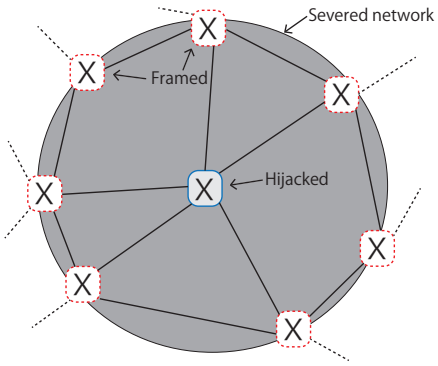



Fig. 5. A network partitioned by the isolation of innocent QNodes. Red nodes denote isolated innocent nodes. The blue node denotes hijacked XNode. Solid lines denote working links. Dashed lines denote links cut by surrounding innocent nodes due to framing. The repeated success of framing leads to this situation. Due to differences in the frequency of communications, the closer a QNode is to a hijacked XNode, the more vulnerable it is.

The loss of availability due to the isolation of the router from the network is more significant than other nodes due to a large amount of communication involved. To avoid a significant network performance loss due to the isolation of a router, we should design the network with as many links connected to each router as possible. Besides, we must operate routers connected to a large number of links in an environment that is as reliable as possible.

*3) Path Black Hole:* The early quantum Internet will have path-setup at first in the classical (management) plane and then quantum plane starts to generate End-to-End entanglements. Therefore, the **packet black hole attack** by advertising incorrect address block results in collecting path-setup classical packets. The classical packets will not arrive at the destination. Therefore the quantum path will not be set up, hence such black hole attacks won't waste quantum plane resources. This is different from the sabotage attack by a single node which results in wasting quantum plane resources.

### *D. Attacks by multiple hijacked QNodes*

Next, we discuss the case where the attacker successfully hijacked multiple QNodes. The attack methods available to each node remain the same, but combining them will change the situation. We investigate what kinds of attacks are possible or enhanced, depending on the combination of malicious nodes.

*1) QDDoS:* First, we consider the possible attack methods for the cooperated malicious ENodes and MNodes. A distributed denial of service (DDoS) attack is a method that compromises availability by attacking a single Internet service from many machines at once. As in the classic DDoS, the DDoS in the Quantum Internet (QDDoS) attacks available to end-users will be cost-effective and malicious. We can divide QDDoS into attacks on the **classical plane** as system controller and assaults on the **quantum plane** as quantum resources provider.

As with server crashes caused by DDoS, failure of the system controller can cause not only service outages but also loss of information on the terminal Qubit and QNIC Qubit. The reconstruction of quantum information is more complicated than classical information. The classic system responsible for managing these Qubits should be independent of the systems affected by QDDoS.

As a way to attack the quantum plane, we can expect an excessive number of service requests. If the applications we provide are quantum key generation or cloud quantum computation, increasing the number of QNODEs can address the attack. If an application requires manipulation of certain quantum information, the attack can cause significant service delays and information loss.

*2) Framing using multiple hijacked QNodes:* In order for a hijacker to perform framing, the target QNode needs to be on the communication path. Assuming no bias in network structure or frequency of use, hijacker is less likely to frame QNodes that are farther away from the hijacked QNode. If you succeed in multiple hijackings, the situation will change. It is difficult to quantitatively discuss threats without defining the network structure, but a (false) call from multiple nodes could more easily fool the network.

## VI. Conclusion

This work is the first attempt to summarize the threats on the Quantum Internet. Modeling threats is an essential work to provide countermeasures against attacks, therefore, essential to achieve secure and sustainable quantum networks. The current Internet is showing that situations of security issues are always changing. Threat models needs to be kept updated.

We have provided an analysis of security for a quantum repeater architecture based on our current knowledge, by referring to proposed taxonomies for classical systems, especially RFID systems. By providing a model of a quantum repeater network and grouping the elements of the modeled repeater, we provide a first look at the kinds of attacks that may be possible.

From the point of view of confidentiality, quantum repeater systems have great advantages. Since it is possible to detect the presence of **an eavesdropper**, detection of a breach of confidentiality is possible. Quantum tomography sacrifices a portion of our stream of Bell pairs as part of ongoing network monitoring operations as needed to tune certain physical parameters to optimize the fidelity of our entanglement. This process is extended to include eavesdropper detection by choosing the portion sacrificed for tomography at random. As long as tomography indicates that high fidelity is achieved on the end-to-end connection, our remaining stream of entangled qubits

can be safely used without fear of breach of confidentiality if the other end point and application are secure.

From the point of view of integrity and availability, a quantum repeater system seems to be not so different from a classical network system.

A repeater includes classical computing hardware and threats to both integrity and availability can target that hardware. Of course, part of the hardware is specially designed for a quantum system, but quantum system hardware is just a special kind of hardware. As we have shown in previous section, the possible attacks are very similar to classical systems.

One of the keys to security of the quantum repeater system is not a quantum system specific issue, but rather the classical parts of the system, including the classical part of the quantum node and classical network services in the node, which are no different from classical network equipment. Mixed attacks making use of a combination of quantum and classical parts may also prove to be an important topic.

One big difference is that quantum mechanics has the no-cloning theorem; quantum information cannot be copied in case loss in the network like classical networking. In this sense, direct transmitting data qubits in the 3rd generation has more serious risk against DoS attacks. This problem can be avoided by sending half Bell pairs even in the 3rd generation. In that case, distributed connection management is required. There will be choices of protocols, rapid and memory-efficient but risky protocol which sends data qubits directly, and safe but slow and memory-inefficient protocol which sends half Bell pairs then executes quantum teleportation.

This paper, comprising a framework of attack points and goals, represents only the first step in assessing the security of quantum networks. We plan to extend our study further as engineers working in both classical and quantum networking, to apply the lessons learned in classical networks to develop a full taxonomy of attacks, assess mitigation strategies, and ultimately minimize security issues with developing quantum networks.

## ACKNOWLEDGMENT

This material is based upon work supported by the Air Force Office of Scientific Research under award number FA2386-19-1-4038. Authors acknowledge members of Quantum Internet Task Force, which is a research consortium to realize the Quantum Internet, for comprehensive and interdisciplinary discussions of the Quantum Internet.

## REFERENCES

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," Physical Review Letters, vol. 98, no. 23, p. 230501, 2007.

[2] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, "Photonic state tomography," Advances in Atomic, Molecular, and Optical Physics, vol. 52, pp. 105–159, 2005.

[3] D. Bacon and W. van Dam, "Recent progress in quantum algorithms," Communications of the ACM, vol. 53, no. 2, pp. 84–93, 2010. [Online]. Available: http://doi.acm.org/10.1145/1646353.1646375

[4] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, "Reference frames, superselection rules, and quantum information," Rev. Mod. Phys., vol. 79, pp. 555–609, Apr 2007. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.79.555

[5] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," Physics, vol. 1, no. 3, pp. 195–200, 1964.

[6] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," ACM SIGCOMM Computer Communication Review, vol. 19, no. 2, pp. 32–48, 1989.

[7] M. Ben-Or and A. Hassidim, "Fast quantum Byzantine agreement," in Proceedings of the thirty-seventh annual ACM symposium on Theory of computing. ACM, 2005, pp. 481–485.

[8] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, vol. 11, Dec. 1984, pp. 175–179.

[9] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Physical Review Letters, vol. 68, no. 5, pp. 557–559, 1992.

[10] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," Physical review letters, vol. 76, no. 5, p. 722, 1996.

[11] O. Benoît, Fault Attack. Boston, MA: Springer US, 2005, pp. 218–219. [Online]. Available: https://doi.org/10.1007/0-387-23483-7_157

[12] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, "Quantum repeaters and quantum key distribution: the impact of entanglement distillation on the secret key rate," arXiv:1303.3456v1 [quant-ph], Mar. 2013.

[13] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," Physical Review Letters, vol. 81, pp. 5932–5935, 1998.

[14] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Measurement-based and universal blind quantum computation," in Formal Methods for Quantitative Aspects of Programming Languages. Springer, 2010, pp. 43–86.

[15] C.-H. Chien, R. Van Meter, and S.-Y. Kuo, "Fault-tolerant operations for universal blind quantum computation," J. Emerg. Technol. Comput. Syst., vol. 12, no. 1, pp. 9:1–9:26, Aug. 2015. [Online]. Available: http://doi.acm.org/10.1145/2700248

[16] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello, "Distributed quantum computation over noisy channels," Phys. Rev. A, vol. 59, pp. 4249–4254, Jun 1999. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.59.4249

[17] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," Phys. Rev. Lett., vol. 23, pp. 880–884, Oct 1969. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.23.880

[18] M. Cramer, M. B. Plenio, S. T. Flammia, and R. Somma, "Efficient quantum state tomography," Nature, vol. 1, no. 9, p. 149, 2010.

[19] C. Crepeau, D. Gottesman, and A. Smith, "Secure multi-party quantum computation," in Proceedings of the thiry-fourth annual ACM symposium on Theory of computing. New York, NY, USA: ACM, 2002, pp. 643–652.

[20] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpędek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveria, R. Hanson, and S. Wehner, "A link layer protocol for quantum networks," arXiv preprint arXiv:1903.09778, 2019.

[21] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," Phys. Rev. Lett., vol. 77, no. 13, pp. 2818–2821, Sep 1996.

[22] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," Reports on Progress in Physics, vol. 76, no. 7, p. 076001, 2013.

[23] W. Dür and H. J. Briegel, "Entanglement purification and quantum error correction," Reports on Progress in Physics, vol. 70, no. 8, p. 1381, 2007.

[24] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," Phys. Rev. A, vol. 59, no. 1, pp. 169–181, Jan 1999.

[25] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, "Quantum certification and benchmarking," arXiv preprint arXiv:1910.06343, 2019.

[26] A. Ekert, "Quantum cryptography based on Bell's theorem," Physical Review Letters, vol. 67, no. 6, pp. 661–663, 1991.

[27] C. Elliott, "Building the quantum network," New Journal of Physics, vol. 4, p. 46, 2002.

[28] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," in Proc. SIGCOMM 2003, ACM. ACM, Aug. 2003.

[29] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. Van Meter, and L. C. L. Hollenberg, "Surface code quantum communication," Phys. Rev. Lett., vol. 104, no. 18, p. 180503, May 2010.

[30] C. Gentry, "Computing arbitrary functions of encrypted data," Communications of the ACM, vol. 53, no. 3, pp. 97–105, Mar. 2010.

[31] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nature communications, vol. 2, p. 349, 2011.

[32] D. Gottesman, T. Jennewein, and S. Croke, "Longer-baseline telescopes using quantum repeaters," Phys. Rev. Lett., vol. 109, p. 070503, Aug 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.109.070503

[33] L. K. Grover, "Quantum telecomputation," 1997.

[34] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," Reviews of modern physics, vol. 81, no. 2, p. 865, 2009.

[35] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""Event-ready-detectors" Bell experiment via entanglement swapping," Phys. Rev. Lett., vol. 71, pp. 4287–4290, Dec 1993. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.71.4287

[36] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk analysis of Trojan-horse attacks on practical quantum key distribution systems," Selected Topics in Quantum Electronics, IEEE Journal of, no. 99, pp. 1–1, 2014.

[37] D. James, P. G. Kwiat, W. J. Munro, and A. G. White, "Measurement of qubits," Physical Review A, 2001.

[38] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," Phys. Rev. A, vol. 79, p. 032325, 2009. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.79.032325

[39] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, "Optimal approach to quantum communication using dynamic programming," Proceedings of the National Academy of Sciences, vol. 104, no. 44, pp. 17 291–17 296, 2007.

[40] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, "Hacking the bell test using classical light in energy-time entanglement–based quantum key distribution," Science Advances, vol. 1, no. 11, p. e1500793, 2015.

[41] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, "Hacking the bell test using classical light in energy-time entanglement–based quantum key distribution," Science Advances, vol. 1, no. 11, 2015. [Online]. Available: http://advances.sciencemag.org/content/1/11/e1500793

[42] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, "Design and analysis of communication protocols for quantum repeater networks," New Journal of Physics, vol. 18, no. 8, p. 083015, 2016.

[43] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, "Quantum Clock Synchronization Based on Shared Prior Entanglement," Physical Review Letters, vol. 85, no. 9, pp. 2010–2013, 2000.

[44] J. Kim et al., "1100x1100 port MEMS-based optical crossconnect with 4-dB maximum loss," IEEE Photonics Technology Letters, vol. 15, no. 11, pp. 1537–1539, 2003.

[45] H. J. Kimble, "The quantum Internet," Nature, vol. 453, pp. 1023–1030, Jun. 2008.

[46] E. Knill and R. Laflamme, "Concatenated quantum codes," http://arXiv.org/quant-ph/9608012, Aug. 1996.

[47] M. Koashi and A. Winter, "Monogamy of quantum entanglement and other correlations," Physical Review A, vol. 69, no. 2, p. 022309, 2004.

[48] K. Lemke and C. Paar, Physical Attacks. Boston, MA: Springer US, 2005, pp. 458–459. [Online]. Available: https://doi.org/10.1007/0-387-23483-7_300

[49] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, "Long range failure-tolerant entanglement distribution," New Journal of Physics, vol. 15, no. 2, p. 023012, 2013. [Online]. Available: http://stacks.iop.org/1367-2630/15/i=2/a=023012

[50] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photonics, vol. 4, no. 10, pp. 686–689, 2010.

[51] V. Makarov and D. Hjelme, "Faked states attack on quantum cryptosystems," Journal of Modern Optics, vol. 52, no. 5, pp. 691–705, 2005.

[52] T. Matsuo, C. Durand, and R. Van Meter, "Quantum link bootstrapping using a RuleSet-based communication protocol," Physical Review A, vol. 100, no. 5, 2019. [Online]. Available: https://arxiv.org/abs/1904.08605

[53] A. Mink, S. Frankel, and R. Perlner, "Quantum key distribution (QKD) and commodity security protocols: Introduction and integration," International Journal of Network Security & Its Applications (IJNSA), vol. 1, no. 2, Jul. 2009.

[54] L. Mirowski, J. Hartnett, and R. Williams, "An RFID Attacker Behavior Taxonomy," IEEE Pervasive Computing, vol. 8, no. 4, pp. 79–84, 2009.

[55] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, "Threats to Networked RFID Systems," in Unique Radio Innovation for the 21st Century. Berlin, Heidelberg: Springer Berlin Heidelberg, Jul. 2010, pp. 39–63.

[56] D. L. Moehring, P. Maunz, S. Olmschenk, K. C. Younge, D. N. Matsukevich, L.-M. Duan, and C. Monroe, "Entanglement of single-atom quantum bits at a distance," Nature, vol. 449, no. 7158, pp. 68–71, 2007.

[57] T. Morimae, "Verification for measurement-only blind quantum computing," Phys. Rev. A, vol. 89, p. 060302, Jun 2014. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.89.060302

[58] T. Morimae and K. Fujii, "Blind quantum computation protocol in which alice only makes measurements," Phys. Rev. A, vol. 87, p. 050301, May 2013. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.87.050301

[59] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," Scientific Reports, vol. 6, p. 20463, 2016.

[60] S. Nagayama, "Distributed quantum computing utilizing multiple codes on imperfect hardware," Ph.D. dissertation, Keio University, 2017. [Online]. Available: https://arxiv.org/abs/1704.02620

[61] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge University Press, Jan. 2000. [Online]. Available: http://www.worldcat.org/isbn/521635039

[62] T. Oka, T. Satoh, and R. Van Meter, "A classical network protocol to support distributed quantum state tomography," in Proc. Quantum Communications and Information Technology, 2016.

[63] P. Pathumsoot, T. Matsuo, T. Satoh, M. Hajdušek, S. Suwanna, and R. Van Meter, "Modeling of measurement-based quantum network coding on ibmq devices," arXiv preprint arXiv:1910.00815, 2019.

[64] M. Peev et al., "The SECOQC quantum key distribution network in Vienna," New Journal of Physics, vol. 11, no. 7, p. 075001 (37pp), 2009. [Online]. Available: http://stacks.iop.org/1367-2630/11/075001

[65] A. Pirker, V. Dunjko, W. Dür, and H. J. Briegel, "Entanglement generation secure against general attacks," New Journal of Physics, vol. 19, no. 11, p. 113012, 2017. [Online]. Available: http://stacks.iop.org/1367-2630/19/i=11/a=113012

[66] D. J. Reilly, "Engineering the quantum-classical interface of solid-state qubits," npj Quantum Information, vol. 1, p. 15011, 2015.

[67] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," Rev. Mod. Phys., vol. 83, pp. 33–80, Mar 2011. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.83.33

[68] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka et al., "Field test of quantum key distribution in the tokyo qkd network," Optics express, vol. 19, no. 11, pp. 10 387–10 409, 2011.

[69] T. Satoh, S. Nagayama, T. Oka, and R. Van Meter, "The network impact of hijacking a quantum repeater," Quantum Science and Technology, vol. 3, no. 3, p. 034008, 2018.

[70] A. Steane and D. Lucas, "Quantum computing with trapped ions, atoms and light," Fortschritte der Physik, vol. 48, no. 9âĂŘ11, pp. 839–858, 2000.

[71] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the swissquantum quantum key distribution network in a field environment," New Journal of Physics, vol. 13, no. 12, p. 123001, 2011. [Online]. Available: http://stacks.iop.org/1367-2630/13/i=12/a=123001

[72] S. Suzuki and R. Van Meter, "Classification of quantum repeater attacks," in Proc. NDSS Workshop on Security of Emerging Technologies, 2015.

[73] B. M. Terhal, "Is entanglement monogamous?" IBM Journal of Research and Development, vol. 48, no. 1, pp. 71–78, 2004.

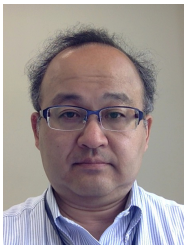
[74] R. Van Meter, Quantum Networking. Chichester, UK: John Wiley & Sons, May 2014.

[75] R. Van Meter and C. Horsman, "A blueprint for building a quantum computer," Communications of the ACM, vol. 56, no. 10, pp. 84–93, Oct. 2013.

[76] R. Van Meter, K. Nemoto, W. J. Munro, and K. M. Itoh, "Distributed arithmetic on a quantum multicomputer," SIGARCH Comput. Archit. News, vol. 34, no. 2, p. 354âĂŞ365, May 2006. [Online]. Available: https://doi.org/10.1145/1150019.1136517
[77] R. Van Meter, T. Satoh, T. D. Ladd, W. J. Munro, and K. Nemoto, "Path selection for quantum repeater networks," Networking Science, vol. 3, no. 1-4, pp. 82–95, 2013.
[78] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang et al., "Field and long-term demonstration of a wide area quantum key distribution network," Optics express, vol. 22, no. 18, pp. 21 739–21 756, 2014.
[79] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," Science, vol. 362, no. 6412, 2018. [Online]. Available: http://science.sciencemag.org/content/362/6412/eaam9288
[80] S. H. Weingart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defences," in CHES '00: Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems. Springer-Verlag, Aug. 2000.
[81] R. F. Werner and M. M. Wolf, "Bell inequalities and entanglement," arXiv preprint quant-ph/0107093, 2001.
[82] M. M. Wilde, Quantum information theory. Cambridge University Press, 2013.
[83] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature, vol. 299, no. 5886, pp. 802–803, 1982.
[84] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür, "Long-range big quantum-data transmission," Phys. Rev. Lett., vol. 120, p. 030503, Jan 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.120.030503

**Takahiko Satoh** is the project lecturer of Keio University Quantum Computing Center. He studied at Keio University and the University of Tokyo. He received a PhD in computer science from UT. His research field is quantum computing and quantum networking, particularly quantum network coding, NISQ algorithm design, and Quantum Internet security. He is a member of the Physical Society of Japan (JPS).

**Shota Nagayama** is a senior researcher at Mercari, Inc. and the coordinator of Quantum Internet Task Force. He received his Ph.D in Media and Governance from Keio University. His research interests include quantum error correction, quantum computer architecture, quantum network architectures with heterogeneity, and crypto communication systems utilizing quantum key distribution.



**Shigeya Suzuki** is a researcher specializing in computer networks and distributed systems, also an expert in systems architecture and software development. He is currently enthusiastic on Blockchain technology since it consists of many of the areas which he understands and experienced well. He received his Ph.D. from Keio University, Graduate School of Media and Governance. Currently a Project Professor at Graduate School of Media and Governance at Keio University, Associate Director, Technology Officer of Keio Blockchain Laboratory, and also a Board Member of WIDE Project, which established the Japanese Internet. He is a member of ACM, IEEE, IACR, IEICE, and IPSJ.

**Takaaki Matsuo** is a system engineer at Softbank Corp. and a member of the AQUA group in WIDE project. He received his Master's degree from Keio University Graduate school of Media and Governance. His research interest includes quantum network architecture and layered protocol designing for quantum networks. Contact him at kaaki@sfc.wide.ad.jp.

**Rodney Van Meter** is a professor of Environment and Information Studies at Keio University Shonan Fujisawa Campus. Besides quantum networking and quantum computing, his research interests include storage systems, networking, and post-Moore's law computer architecture. Van Meter received a PhD in computer science from Keio University. He is a member of ACM, IEEE, the American Physical Society, and the American Association for the Advancement of Science (AAAS). Contact him at rdv@sfc.wide.ad.jp.