Attacking the Quantum Internet

TAKAHIKO SATOH[1,2] [ORCID], **SHOTA NAGAYAMA[3] (Member, IEEE),**
SHIGEYA SUZUKI[4] (Member, IEEE), TAKAAKI MATSUO[4], MICHAL HAJDUŠEK[4],
AND RODNEY VAN METER[1,5] (Senior Member, IEEE)

[1] Keio University Quantum Computing Center, Yokohama 223-8522, Japan
[2] Graduate School of Science and Technology, Keio University, Yokohama 223-8522, Japan
[3] Mercari, Inc., Tokyo 106-6118, Japan
[4] Graduate School of Media and Governance, Keio University Shonan Fujisawa Campus, Fujisawa 252-0882, Japan
[5] Faculty of Environment and Information Studies, Keio University Shonan Fujisawa Campus, Fujisawa 252-0882, Japan

Corresponding author: Takahiko Satoh (satoh@sfc.wide.ad.jp)

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 Quantum 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 and quantum algorithms have been developed, experimental demonstrations of quantum computing have proliferated, and large-scale machines are on the drawing boards [3]–[7]. One of the oldest and most successful areas in quantum information has been quantum networks [8]–[12].

Work on quantum networks began with the recognition that transmitted qubits act as exquisite sensors of state modification, 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) [13], [14]. 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 [15]–[17]. Distributed quantum computation will help to build large-scale quantum computers, especially by combining heterogeneous quantum modules [18]–[22]. 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 [23], [24]. Broadbent *et al.* developed a fully blind method of conducting any arbitrary quantum calculation (BQC) [25], [26]. Unlike Gentry's classical homomorphic encryption [27], 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 qubits, stronger than any possible classical correlation [28], [29]. Although entanglement cannot be used to transmit information faster than the speed of light, two qubits may be in an entangled state where their values are decided randomly but seemingly in an instantaneously coordinated fashion *without* any apparent communication.

Many of the applications just discussed require us to create this entanglement over a distance. *Quantum repeaters* (see Section II) are an important path toward building a quantum Internet that will achieve this goal by using quantum entanglement for quantum teleportation.

The early use of the quantum Internet with high noise levels would be to enhance Internet security with QKD [30]–[32]. Various attacks for preventing such security improvement have already been proposed [33]–[37]. Defense methods, operational methods with optimal efficiency, and specific methods for combining with classical protocols have also been proposed [38]–[40]. Urban-scale networks have already been built by trusting INodes to avoid the requirement of quantum repeaters, and their performance has been demonstrated [41]–[44].

The classical Internet, the global-scale network of networks, has emerged over some five decades, and security is a major area in research, engineering, and operations [45], [46]. Both hardware and software evolve quickly, and both attacks and defense applied to network infrastructure and end nodes (ENodes) 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 article, we summarize and develop primitive models of attacks on individual components of quantum networks. We do this within the context of confidentiality, integrity, and availability, often abbreviated as the CIA triad. Confidentiality of a quantum network ensures that no information is leaked to an unauthorized party. Integrity ensures that the quantum information is accurate and trustworthy. Availability guarantees access to the quantum information by authorized parties. These definitions are identical to their usual meaning in classical cybersecurity. However, their interaction may be different in quantum networks due to the presence of entanglement.

As an example, consider the case of quantum teleportation [47] where a sender wishes to communicate a single quantum bit to a receiver with the use of a shared entangled pair and two classical bits. Let us assume an unauthorized third party manages to both steal one half of the entangled pair intended for the receiver without being detected by quantum state certification and gain access to the classical channel. In this case, confidentiality of the quantum state is compromised because the unauthorized party can use the two classical bits to successfully complete the teleportation protocol. On the other hand, if the classical channel remains uncompromised, the unauthorized party cannot complete the

teleportation protocol and, therefore, does not affect confidentiality. In fact, without the two classical bits, the unauthorized party is in possession of a maximally mixed state while the original quantum state is destroyed on the sender's end. In this case, it is the integrity of the quantum information that is affected. Depending on the type of attack on the quantum network, one or multiple aspects of the CIA triad may be compromised. We will see that particularly confidentiality and integrity of quantum information are very closely related due to how quantum information is communicated in quantum networks.

The attackers' purpose may be parallel to those in classical networks:

1) *to steal* quantum information;
2) *to disrupt* either the integrity or availability of quantum nodes or quantum networks;
3) *to hijack* a quantum connection or computing resources such as control of quantum repeaters or external components.

The biggest difference between classical and quantum networks is the presence of entanglement. This difference raises questions, as follows.

1) Can an attacker copy or disclose the transferred quantum data via an illicitly created entanglement?
2) Can an attacker compromise later sessions by hijacking qubits or by undetected malicious acts?

Even without entanglement, new questions are raised, as follows.

1) Can control of the quantum hardware elements allow hijacking of the repeater itself or disclosure of the stored information?
2) 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 assess the scalability and stability of the quantum Internet:

1) 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 on fundamental network functions such as routing [48]. The process of answering these questions will certainly last far into the future. This article gives the first framework to categorize attacks in pursuit of these goals.

Radio-frequency identification (RFID) systems exchange information by letting short-range wireless communication act on radio-frequency (RF) tag with ID information. We noted that RFID systems and quantum repeater systems are similar in that they are hybrid systems with tightly coupled

sensing and software elements. Since RFID systems are sensitive to noise and intentional, malicious input, a classification of attack methods, such as information theft and spoofing, has been developed by Weingart [49], Mitrokotsa [50], and Mirowski [51]. These methods inspired us to classify attacks on quantum networks.

While we can model the basic hardware architecture of a quantum network nodes (QNodes) 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 (see Section II) and a hardware model that will allow us to identify points of attack, then classify the primitive attacks (see Section III). We then investigate the means of attack on the quantum Internet through the elements of the quantum nodes (see Section IV), and also discuss what an attacker who has hijacked control of one or more quantum nodes can do (see Section V). We believe that this article 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. ENodes that can connect to the quantum network will provide various quantum services that enable the uses discussed earlier. As in the classical Internet, individual quantum networks of potentially heterogeneous technology and independent management will ultimately come together to form a quantum Internet [10].

A. 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., [52]). 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 [6], [53]. 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 50 years ago [54].

2) STRETCHING OF ENTANGLEMENT

Naturally, we cannot transmit those photons over arbitrary distances. In optical fibers, the probability of success falls exponentially with distance as photons are lost. Unfortunately, in quantum networks, classical amplifiers cannot be used because independent copies of quantum data cannot be made due to the no-cloning theorem [55].

Moreover, in any interesting network, we want to support multihop paths between pairs of nodes, rather than requiring a direct link between each pair. Both problems can be solved by using *entanglement swapping* (ES), 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 [56]. ES can be viewed as an extension of teleportation to entangled states.

3) MANAGEMENT OF ERRORS

The quality, or fidelity (a measure between two quantum states, generally, ideal state and actual state, hence, it describes the quality of qubits), 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* [57] or using quantum error correction [58], [59]. Purification plus ES is the canonical setup of a chain of quantum repeaters [60].

4) MANAGEMENT OF THE NETWORK

Nodes must also participate actively in the management of the network itself, including routing and multiplexing or resource management. This article is the focus of a number of attacks described in this article.

B. TYPES OF QUANTUM NODES

We can classify quantum nodes (QNodes) under the following five types by the number of connected (quantum) links and their roles.

1) 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.

2) MEASUREMENT NODE (MNODE)

An MNode is a terminal node just for measurement, used by end users for QKD or blind quantum computation [61], [62]. 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.

3) REPEATER NODE (RNODE)

RNodes are installed at fixed distances according to the optical fiber loss level to improve network performance in
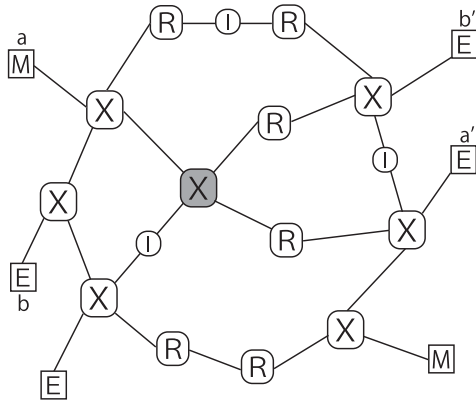
FIG. 1. Schematic diagram of interconnected nodes. Capital letters indicate the first letter of the QNode type. Bell pairs can be shared directly between adjacent nodes. Classical communication is possible between all nodes. Distances will depend on technology, but most likely will be 10 s of km over fiber. If the central (dark) XNode is lost due to hijacking or failure, the number of hops between a–a' (b–b') will increase, and rerouting will strain the bandwidth of the other links [2].

long-distance quantum communications [60]. An RNode has exactly two external links, so that it is useful in a line only. RNodes correspond to repeaters in classical networking.

4) ROUTER NODE (XNODE)

An XNode has two or more external links, e.g., connected internally via an optical backplane [20]. XNodes have more substantial processing capacities than other node types and are responsible for branching the route of the network in complex network topologies. They also serve as network boundaries in an internetwork.

5) INTERMEDIATE NODE (INODE)

INodes may be placed between the abovementioned QNodes and are responsible for generating and connecting Bell pairs. An INode has exactly two external links. Whether a link between QNodes contains an INode or not depends on the Bell pair sharing scheme. There are several configurations of INodes and link, and we describe the elements and functions of INodes in Section II-C. Unless otherwise noted, we do not include INode in our discussion of QNode.

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).

Each QNode has (classical) network addresses, such as IP addresses, for various inter-repeater classical information communication. For this we may use the current Internet, or we may need to build a new dedicated classical network that is strictly isolated and monitored, accessible only by authorized parties. In any case, our minimum requirement is

having an address unique among the set of reachable quantum RNodes. We assume each QNode has a unique address. Since all QNode 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. To simplify our discussion, we assume that all QNode are connected to some kind of classical network that allows them to communicate with each other.

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 article.

C. LINK TYPES AND GENERATIONS OF QUANTUM REPEATER

Muralidharan *et al.* [63] defined three generations of quantum repeaters based on qubit transfer schemes and required technical level. In first and second generation quantum repeater networks each pair of directly connected QNodes needs to share Bell pairs as the first step of quantum communication. A Bell pair is shared between nonadjacent QNodes by ES operation at the relay QNodes. In the third generation quantum repeater networks, logical states encoded directly in a large number of photons are forwarded to nonadjacent nodes.

1) ES QUANTUM REPEATER NETWORK

This type of network executes ES to share Bell pairs between nonadjacent repeaters. Some networks categorized in this type use nonencoded Bell pairs [60], [64]–[66] as first generation repeaters [63] and some employ quantum error correcting codes [67]–[70] as second generation quantum repeaters. Repeaters transfer quantum information by teleportation using shared Bell pairs. As shown in Fig. 2, we modeled ES-type QNode-to-QNode connections into three models, based on their schemes for creating Bell pairs [71]:

2) MEMORY TO MEMORY LINK

This type consists of two QNodes. One QNode receives a photon from a connected RNode (or ENode) and creates Bell pairs using a Bell states analyzer (BSA) entangler built into the node.

3) MEMORIES AND BSA LINK

This type consists of two QNodes and one standalone BSA at the midpoint of the link. The BSA receives a photon entangled with an interface qubit from each QNode, and creates Bell pairs between the interface qubits by measuring the photons together, using the BSA entangler.

4) MEMORIES AND ENTANGLED PHOTON PAIR SOURCE (EPPS) LINK

This type consists of two QNodes and one standalone EPPS at the midpoint of the link. An EPPS creates photonic Bell
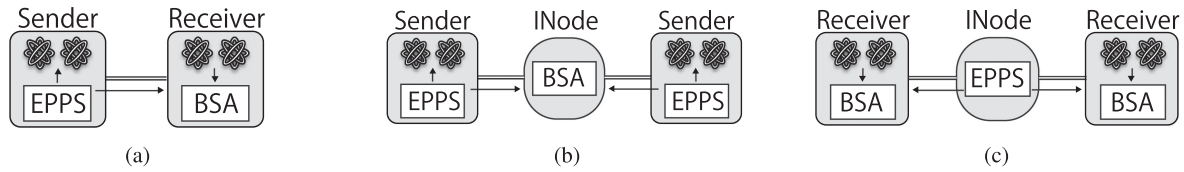
FIG. 2. Model of ES-type QNode-to-QNode connections. Arrows denote the movement of one half of the Bell pair. (a) Memory to Memory link. (b) Memories and BSA link. (c) Memories and EPPS link.

pairs and transmits them to connected RNodes (or ENodes) [71].

5) DIRECT TRANSFER (DT) QUANTUM REPEATER NETWORK

In this type, repeaters directly send encoded quantum states [72] and are categorized as third generation quantum repeaters. The individual links must have very high success probability of transferring physical qubits.

D. MANAGEMENT OF A QUANTUM REPEATER NETWORK

Topology, routing, multiplexing or allocation of network resources, and monitoring of links and the network itself are key work items for network nodes. All of these functions must be designed and implemented assuming the presence of malicious actors. The details of topology and routing are beyond the scope of this article. We focus on handling malicious actors. The essential countermeasure for malicious actors is the same as the technology used for network monitoring, broadly centered around the concept known as *quantum certification* [73].

1) QUANTUM CERTIFICATION

Quantum certification aims to characterize the state created by a particular quantum device or process. Approaches to quantum certification vary based on the amount of resources they consume, the amount of information they provide about the state and crucially the assumptions that are made about the devices being tested [73]. The traditional example of a certification approach is quantum state tomography [74]–[76]. Tomography provides a large information gain about the state and therefore can be used to make accurate estimates of the state fidelity. This comes at the cost of requiring a tremendous amount of resources as well as making strong assumptions about the quantum devices being tested. For these reasons quantum state tomography may play a useful role only in the early stages of the quantum Internet, as shown in Table I. As the technology improves, the demands on the security will increase. In particular, it will not be possible to assume trusted devices as is the case in quantum state tomography. Device-independent protocols [77]–[80] only assume that the tested devices are governed by the laws of quantum mechanics and, therefore, guarantee greater security. An important ingredient of such an approach is self-testing [81] where violation of a Bell inequality is used as a guarantee of high fidelity of the distributed states as well as their confidentiality [28], [82]–[85].

TABLE I Stages in the Development of the Quantum Internet [11]

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

As the stage progresses, more advanced hardware is required to deliver richer functions.

Quantum certification 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. An important requirement is that the selection of Bell pairs to be sacrificed for certification 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 [2]. 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 [73], [86]. Violation of a Bell inequality supporting quantum certification serves as the basis of one form of QKD [14]. Hence, it is secure, given an authenticated classical channel and classical plane. Considering the physical implementation, the qubits used for certification must be isolated from the external network in this type of verification scheme, as cracking of the Bell test through the photon detector has been demonstrated [87].

2) CLASSICAL AUTHENTICATION

Classical channel between QNodes performing quantum teleportation or quantum certification requires authentication. If we perform quantum certification without authentication, the classical communication partner that shares measurement results and basis information may not be the original QNode, but the attacker who is stealing qubits. In this case, we obviously cannot detect the attack by quantum certification. And then we would teleport the quantum data to the attacker. The confidentiality of quantum data requires authenticated classical communication, and we assume this for the discussion in Sections IV and V.
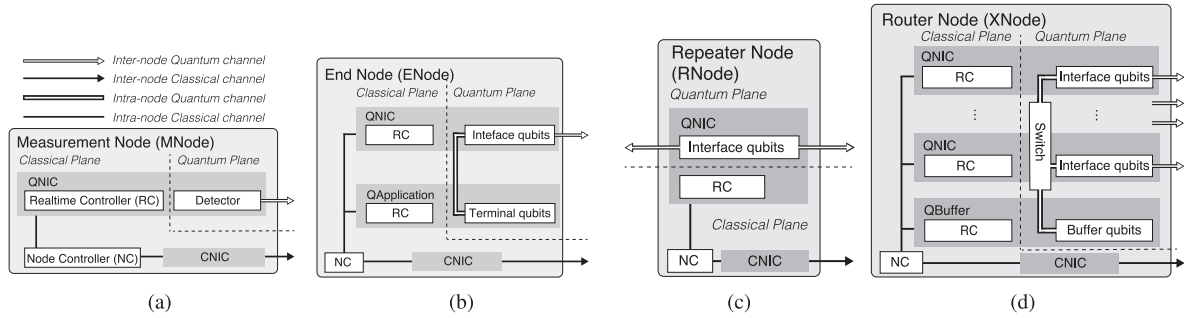
FIG. 3. Model of QNodes. (a) MNode must be able to measure incoming qubits in any basis. Like other QNodes, we can separate components into quantum plane and classical plane. (b) ENode can perform universal computations on terminal qubits. (c) RNode connects two nonadjacent QNodes. (d) XNode connects to several QNodes and is responsible for communicating on various routes.

E. APPLICATIONS OF A QUANTUM INTERNET

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 or more distant QNodes chosen at the discretion of the application user. Based on the level of required functions, Wehner *et al.* [11] classified the development of a quantum Internet by stage and showed the applications provided at each stage (see Table I). This article focuses on networks at stage 2 and mentioned above.

Application layer protocols may have end-to-end verification mechanisms, such as QKD and more general device-independent protocols (e.g., above classical authentication via another provider service). On the other hand, an attack on the routing layer is a sufficient threat even if the application layer adopts secure protocols in classical networks [88]. From this point of view, we believe that not all security to confidentiality should depend on the application layer, and we mainly discuss attacks outside the application layer.

III. HARDWARE MODEL OF THE QUANTUM INTERNET

In this section, we describe our models of QNodes and those elements. A QNode will have different modules depending on its role shown in Section II-B. We draw the internal structure of each QNode type in Fig. 3 (see also Section III-C for INode). We classify these components into two planes, classical and quantum, and describe details as follows.

A. QUANTUM PLANE COMPONENTS OF A QNODE

The networks corresponding to stages 1 to 4 in Table I are functionally constrained, and we call them NISQI, or noisy intermediate scale quantum Internet. In this era, qubit memories will be noisy and limited in number. In fulfilling the network's responsibilities, they will have several roles. Ideally, these roles are performed by qubits with different physical placement in the system, but with limited resources qubits may be assigned more than one role. With the primary focus of this article being on physical vulnerability to attacks, for security analysis purposes, qubits should be treated as the most vulnerable role to which they belong. For example,

buffer qubits (described below) are defined to be isolated from the internode optical channel; if software assigns the role of buffer to an interface qubit, it still must be treated as an interface qubit.

1) QUANTUM NETWORK INTERFACE CARD (QNIC)

A QNIC is a quantum network's equivalent of a classical network interface card. Depending on the physical implementation, it may consist of transmitters, receivers or detectors, and qubits (Interface 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 a fiber.

A hard real-time controller (RC) in a QNIC also handles all real-time operation, such as automatic creation of on-physical-link entanglement [89]. In Fig. 3, we control each classified Qubits with a different RC, but a single integrated RC could be adopted.

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

2) QUANTUM APPLICATION PLATFORM (QAPPLICATION)

A QApplication controls terminal qubits, intended for quantum applications (see Section II-E). These qubits can be entangled or swapped with interface qubits, and hence, can be entangled with remote terminal qubits.

3) QUANTUM BUFFER (QBUFFER)

A QBuffer is a pool of qubits (Buffer qubits) used to prevent QNIC congestion. A QBuffer may be optional depending on workload and hardware design, but our analysis assumes it is present.

4) INTERFACE QUBITS

Each QNIC other than MNode has multiple interface qubits, which are exposed to internode channels and can create

entanglement with remote interface qubits. Interface qubits in QNICs are used only temporarily. Once the entanglement which the interface qubits hold is transferred to buffer qubits or terminal qubits, interface qubits play no further role in that operation.

5) BUFFER QUBITS
Buffer qubits in a QBuffer (usually in a RNode or XNode) can hold entangled states but are not optically connected to the outside, freeing interface qubits for reuse and are more secure than interface qubits. Buffer qubits are used for temporal buffering. They may have different physical characteristics than interface qubits and can interact with either interface qubits or terminal qubits.

6) TERMINAL QUBITS
Terminal qubits are similar to buffer qubits, but are located at ENodes. Terminal qubits are under the direct control of a QApplication. They are assumed to be optically isolated from any internode quantum channel.

7) DETECTOR
A detector is a device for measuring received photonic qubits. Here, detectors are assumed to be nonphoton number counting detectors; they detect the presence or absence of light. Measuring a photonic qubit in a specific basis is different depending on the photonic qubit representation (e.g., time bin or polarization), and may require the addition of linear optical elements such as polarizing beamsplitters. Detectors are often built into larger subsystems such as Bell state analyzers. Detectors are connected through quantum channels to buffer qubits, terminal qubits, or interface qubits, either via an optical switch or directly. Detection is a conversion from quantum information to classical information.

8) INTRANODE QUANTUM CHANNEL
Intranode quantum channels provide interconnection between quantum elements in a QNode such as terminal qubits, buffer qubits, and interface qubits. Intranode quantum channels are not exposed to the outside of the node.

9) INTERNODE QUANTUM CHANNEL
By using an internode quantum channel, node-to-node single hop entanglement is created between interface qubits.

10) LINEAR OPTICAL COMPONENTS
Passive linear optical components, such as ordinary or polarizing beamsplitters or wave plates, alter photonic qubit states in simple ways or are combined with other components to create subsystems such as BSAs.

11) OPTICAL SWITCH
An optical switch (e.g., a nanomechanical crossbar [90]) changes the optical connections between quantum plane elements. Although such switches can be used in the long-distance optical paths [31], here we focus on use inside a node with multiple QNICs to achieve nonblocking photon routing. A node with one or two QNICs would not need a node-internal switch (see Fig. 3).

B. CLASSICAL PLANE COMPONENTS OF A QNODE
1) 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-QNodes communications, generally carrying soft real-time information necessary for interpreting quantum information and determining future operations.

2) RC
An RC 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 RC are shown: the QNIC RC, the buffer RC, and the application RC.

3) NODE CONTROLLER
The node controller communicates with other QNodes and controls QNIC, QBuffer and QApplication to achieve its goal: for an RNode, to create entanglement between a local interface qubit and a remote interface qubit; for an ENode, to create entanglement between a local terminal qubit and a remote qubit via its interface qubit, to run an application.

4) INTRANODE CLASSICAL CHANNELS
Here, we stick to intranode classical channels as a subsystem of intranode qubit transmission functionality, such as transferring meta-information, Pauli frames (which define the polarity of a qubit relative to a reference signal) or acknowledgments of quantum channels. Intranode classical channels are not exposed to the outside of the node.

5) INTERNODE CLASSICAL CHANNELS
Internode classical channels are used to coordinate with other nodes.

6) 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.

C. ELEMENTS OF QNODE TO QNODE CONNECTION AND EXTERNAL RESOURCE

1) EPPS

An EPPS may be connected to internode quantum channels in INodes, or may be used along an intranode quantum channel in other nodes. An EPPS is a simple component, which continuously creates and sends entangled photons to two connected components. The canonical example of an EPPS is *symmetric parametric down conversion* [91].

2) BSA

A BSA is a subsystem built from detectors and linear optical components that measures two photons in the Bell basis. If the incoming photons are entangled with stationary memories or other photons, the measurement effects ES. A BSA may be deployed as a standalone INode or incorporated into a QNode.

As mentioned in Section II-B, when we use BSA and EPPS as a standalone nodes (INodes), they also have internode classical channels. BSA implementations using linear optics suffer from the shortcoming that only two of the four Bell states can be distinguished with certainty. This limits the success probability of such BSA to 50%. Also, the canonical BSA cannot choose the outcome of the measurement; the two photons are projected onto one of the Bell states at random.

3) QUANTUM EXTERNAL CONNECTIVITY

All QNICs are connected to other adjacent QNICs (or QNodes) via optical link. Such a link is point-to-point system for creating entanglement (see Section II-C).

4) CLASSICAL EXTERNAL CONNECTIVITY

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

IV. ATTACKS WITHOUT CONTROL OF QUANTUM NODES

In this section, we describe the primitive attacks on each element of the quantum Internet. Quantum network devices can be divided into 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. 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 notions of confidentiality, integrity, availability (CIA). The CIA of the nodes and links introduced in Section III can be considered by combining elemental discussion of primitive attacks in this Section. Due to the no-cloning theorem, confidentiality, integrity, and availability are closely linked. For example, by stealing quantum data from an interface qubit, another value can be injected in the qubit. In this case, an attack on confidentiality attacks integrity, too.

The focus of this article is categorizing attacks, hence, such relationships are beyond the scope.

We note that the attacks covered in this section are based on physical manipulation of or physical proximity to each element.

A. ATTACKS ON THE QUANTUM PLANE

First, we will discuss the target devices on the quantum plane and the details of each attacking scheme shown in Table II.

1) EAVESDROPPING (QUANTUM CHANNEL)

Eavesdropping on photons flying in internode quantum channel affects confidentiality if valuable quantum data are encoded onto photons. Transferring half-Bell pairs and executing quantum teleportation afterward would protect valuable quantum data from eavesdropping as long as the operation is authenticated properly.

Eavesdropping also works as an attack on availability, because it breaks the quantum states. This denial-of-service (DoS) attack is one of the most obvious weaknesses of quantum networks if robustness is an important design goal. Since an internode quantum channel is just a fiber or such cable between QNodes, it is relatively easy to get access to these channels.

2) OPTICAL PROBES

Optical probing of detector settings has been demonstrated. Among the many attacks on QKD implementations developed in Makarov's lab, Jain *et al.* described an eavesdropper that can probe the chosen measurement basis used in a BB84 QKD system [13] by sending a bright pulse of light from the quantum channel into the interface and analyzing the back-reflected pulses [92], a classical attack on the hardware used for the quantum states. The attack could be executed directly by cutting fibers and inserting hardware, or by tapping the fiber, e.g., via evanescent coupling.

Though entanglement-based QKD protocols do not have this weakness because state certification is performed end-to-end, a similar attack in which some optical detectors are saturated could be used in a man-in-the-middle attack. *Optical probes* damage the confidentiality of quantum states and the following devices will also be attacked:

3) CASE: DETECTOR WITH BSAS

For XNodes, those (backplane) detectors are located behind the node-internal optical switch and are not exposed. Hence, *optical probes* do not affect confidentiality.

For INodes, these detectors are optically connected to the internode channel directly and are exposed. Then, *optical probes* may be used to determine hardware settings, or may be used to control what the classical hardware sees. Nevertheless, confidentiality will not be affected, as quantum state leakage is not expected to occur.

TABLE II Attacks on the Quantum Plane, Ordered Roughly According to the Severity or Intrusiveness of the Attack

Attacker's action	Attacker's resources	Components under attack	Compromised elements
Eavesdropping	Access to inter-node channel	In-flight optical states	Confidentiality, Availability
Optical probe	Insertion & detection of optical pulses	Interface qubit, Intra-node Quantum channel, Detector	Confidentiality
Fault injection	Insertion of optical pulses	Interface qubit, Quantum channel (Intra-node, Inter-node), Detector	Integrity, Availability
Out-of-system, standoff attacks	Physical access near nodes	All Qubits, Quantum channel (Intra-node, Inter-node), Switch, Detector	Integrity, Availability
Malicious entanglement	Ersatz node	Interface qubits	Confidentiality, Integrity, Availability
Destruction or vandalism	Physical access to node equipment	Interface qubit, Intra-node quantum channel, Switch, Detector	Availability
Theft of hardware	Physical access to node equipment, node operational expertise	All	Confidentiality, Integrity, Availability

4) CASE: INTERNODE QUANTUM CHANNEL

Blinding of detectors as a kind of optical probe would cause the leakage of quantum state, while the detector saturation attack described above could be used to control what the classical hardware sees. More analysis of this impact on QNode operation is necessary. Since an internode quantum channel is physically just an optical fiber or similar media between QNodes, it is relatively easy to get access to these channels.

Optical probes are not executable on the intranode quantum channel without directly modifying the hardware.

5) FAULT INJECTION

Fault injections involve inserting unauthorized and unexpected optical pulses into the internode quantum channel, hoping to reach the detector [93], [94]. For some qubit representations, it is also known that altering the temperature of fibers affects the quantum states of photons passing through by slightly altering the effective path length.

Depending on the design of the QNodes, *fault injections* may disturb the state of *interface qubits*, *internode quantum channel*, and *detector* (if exposed), affecting availability and integrity. This attack is also not executable on the intranode quantum channel without directly modifying the hardware.

6) OUT-OF-SYSTEM ATTACKS

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 act as any quantum operation, including noncomputational operations such as leakage from the computational basis. For this 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. Other attacks, such as on the cooling or other control systems, may be harder to carry out remotely.

These attacks also prevent designed qubit operations, which affects integrity and availability of interface qubits, buffer qubits, and terminal qubits. *Out-of-system attacks* would alter the state of photons during transfer and correct signals become unrecognizable due to injected noise. Therefore, intranode quantum channel, switches, internode quantum channel, and detector would also be targets of such attack.

7) MALICIOUS ENTANGLEMENT

Malicious entanglement attempts to steal information via teleportation by replacing a legitimate qubit with a qubit created by and entangled with other qubits controlled by the attacker, or by entangling additional qubits with otherwise legitimate qubits under the nominal control of legitimate nodes. In the worst case, this malicious entanglement can result in the attacker being the receiving party in a teleportation operation; this theft of a qubit causes the loss of confidentiality. Malicious entanglement also disturbs integrity because it affects any other qubits with which it is entangled, and affects availability as a result of the no-cloning theorem [55].

As creating malicious entanglement requires that the attacker have control of some quantum memory, this involves either compromise of an otherwise licit network node, or connection of an illicit, ersatz network node. Compromised control of licit nodes will be addressed further in Section V.

The targeted qubit operations and the affected situations are described as follows.

8) CASE: INTERFACE QUBIT

Since optical fibers for internode quantum channel are attached to *interface qubits* directly (see below), interface qubits are most exposed to external risks. *Malicious entanglement* may affect interface qubits via the internode 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 in the theft of valuable quantum data if quantum teleportation is executed without awareness of the attack.

The essential countermeasure for this vulnerability is quantum state certification. Assuming interface qubits are used to temporarily hold half-Bell pairs (completely generic states with no secret information) before teleporting valuable quantum data, quantum certification *randomly* selects some of the Bell pairs to measure to determine if an eavesdropper has entangled her qubits with ours, as described in Section II.

We may consider the scenario where the eavesdropper avoids detection by sheer luck and interacts with qubits, which were not picked for the certification procedure. In this case, the confidentiality of quantum data is not necessarily compromised. If the classical channel retains its confidentiality, so does the quantum data. Classical data must be sent to

TABLE III Attacks on the Classical Plane Ordered Roughly According to Their Invasiveness or Severity

Attacker's action	Attacker's resources	Components under attack	Compromised elements
Eavesdropping	Access to inter-node channel	Data-relevant messages	Confidentiality
Message disruption	Access to inter-node channel	RC, Detector with BSA, EPPS	Availability
Man-in-the-middle attack	Intercept & resend on inter-node channel	All connection setup, action messages, network management tomography, etc.	Integrity
Message rerouting	Control of a classical router	Switch, Detector with BSA	Confidentiality, Integrity, Availability
DoS attack	Ability to overtax network resources	Intra-node classical channel	Availability
Destruction or vandalism	Physical access to classical controller	CNIC, Controller resources, Electric power	Availability
Theft of hardware	Physical access to node equipment, node operational expertise	All	Confidentiality, Integrity, Availability

the recipient in order to successfully complete teleportation of quantum data. Without this classical data the eavesdropper ends up in possession of useless maximally mixed states.

9) CASE: BUFFER QUBIT AND TERMINAL QUBIT

Since buffer qubits and terminal qubits themselves do not have any external connectivity, they are not exposed to risks from internode 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.

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 qubit 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. Quantum certification while working with a stream of Bell pairs is needed here as well as on interface qubits.

10) CASE: NISQI QUBIT

NISQI qubits will have all of the weaknesses of other qubits due to their many roles. This assumption is likely to be true for the other attack methods discussed as follows, and attackers will have many avenues to exploit.

Malicious entanglement may be inserted via interface qubits, then transferred to terminal qubits, or other buffer qubits. If the insertion is successful, malicious entanglement is threats against confidentiality, integrity, and availability of buffer qubits, terminal qubits as well as interface qubits.

11) DESTRUCTION OR VANDALISM OF HARDWARE

Destruction of or damage to hardware and other typical classic attacks prevent the designed operation of the qubits, if the attacker has access to the target device. These attacks pose a threat to the availability of each QNode device: qubits (interface, buffer, terminal), intranode quantum channel, optical switch, and detectors with BSA.

12) THEFT OF HARDWARE

Theft of quantum equipment naturally affects availability of the system and integrity of any data active at the time of theft, but confidentiality is not affected, because quantum systems do not yet support nonvolatile memory. The state of any memory would be destroyed by removal of power to the system as part of a theft.

B. ATTACKS ON THE CLASSICAL PLANE

Next, we will discuss the target devices on classical plane and details of each attacking scheme shown in Table III. The attacks here concentrate on reading, modifying, or destroying classical messages and signals in the channel, but extend to more physical attacks as well. Some of these attacks aim to take control of a QNode via classical vulnerabilities; cases in which such hijacking has succeeded are discussed in the following section.

1) EAVESDROPPING (CLASSICAL CHANNEL)

All classical attacks aimed at *internode classical channels* may be possible. We will show examples of specific attacks on classical channels in quantum network systems, for each compromised element.

Classical privacy threats, such as *eavesdropping* and tracking user behavior, would progressively reduce the inherent confidentiality of quantum information.

2) MESSAGE DISRUPTION

The disruption of classical communications will destroy availability. There are concrete cases such as *Attacks to clock synchronization* against *RC*, *EPPS*, and *detectors with BSAs* and *Attacks to measurement information* against *RC*.

3) MAN-IN-THE-MIDDLE ATTACK

Man-in-the-middle attack against *internode classical channels* can disrupt the generation of Bell pairs, in a variety of ways, including overwriting Pauli frames. It would be difficult to determine from the quantum state disturbance whether this attack, which violates integrity, is an attack on classical or quantum communication.

4) MESSAGE REROUTING

Message rerouting, disobeying routing information, would forward qubits to eavesdroppers. This attack is achieved by

falsified routing information as well as hijacked controller of *optical switches.*

Message rerouting would work as *malicious entanglement* and may result in inserting incorrect quantum states, thus affecting integrity and availability. In a particular configuration of the network, using bounded entanglement state (or low distillation state) we can resist such an attack [95].

5) DOS ATTACK

When using public classical channels such as the Internet, DoS attacks would disrupt coordination messages such as ACK messages for photons, affecting availability.

6) DESTRUCTION OR VANDALISM OF HARDWARE

These attacks are well studied and explained by, for example, Weingart [49]. In our networks, the following classical computing elements responsible for availability can be attacked:

1) CNIC;
2) controller resources (e.g., clock, memory, processor);
3) chassis providing electric power.

7) THEFT OF HARDWARE

Theft of the classical equipment controlling quantum systems naturally affects availability of the system and integrity of any data active at the time of theft. Here, we distinguish theft from simple destruction (above) by defining theft to assume the attacker has the ability to operate the node. Unlike the quantum plane devices, classical components often contain nonvolatile storage holding data important to security. Encryption keys used for authentication or for keying communication sessions are of particular concern. Thus, while an immediate attack on the confidentiality of in-progress communications is not possible here, looking forward, the attacker gains all of the capabilities ascribed to malicious nodes in the following section.

V. ATTACKS USING MALICIOUS QNODE(S)

The game changes substantially if a malicious party gains control of one or more QNodes. In this section, we investigate what can be done by an attacker(s) who have successfully hijacked full control of one or more QNodes. The attack vectors and protocol stack considered in this section are based mainly on architectural principles outlined in [2] and [96]. It is worth noting that the types of QNodes, along with their vulnerabilities, discussed in this section are expected to form the basic building blocks of the quantum Internet. Early realizations of quantum networks will not be implemented exactly as outlined here. For example, some node designs will have no physical distinction among types of qubits, but instead will only assign differences in roles via software. Nevertheless, even as different hardware designs evolve, the fundamental roles described here will form the architectural foundation. Those differences in implementation may result in some devices being inherently immune to certain attacks. This is a desirable feature, but one that should be recognized

explicitly rather than going unstated, in order to ensure that all subsequent generations maintain such guarantees.

The quantum Internet will continuously use a certain fraction of performance for cross-validation to detect anomalies such as equipment failures or hijacking [2].

1) Each QNode regularly and continuously verifies neighboring nodes and their assigned communications.
2) 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 an attacker successfully hijacks one or more QNodes and summarize attacks using these nodes in Table IV.

1) HIJACKED CONTROLLER

Since *interface*, *buffer*, and *terminal qubits* are controlled by classical controllers, they can be hijacked by carelessness on the part of the controller (software or hardware). An attacker will be able to arbitrarily control these qubits depending on the operations implemented, and will cause the following damage: Loss of confidentiality due to disclosure of quantum data via arbitrary sessions. Disruption of integrity by changing values using manipulation of qubits (flipping qubits, measuring values, initialization, etc.). Loss of availability of any session due to improper execution or interruption of instructions.

An attacker would use the hijacked *intranode classical channel* to cause the following threats: Leakage of most meta-information, such as session information and classical channel usage (confidentiality). Anomalies in the quantum state by tampering with Pauli frames and other management information (integrity). Interference with specific sessions due to forged channel failures (availability).

An attacker also could change the quantum state in the *internode classical channel* by changing management information using a hijacked controller.

Falsified measurement outcome by hijacked *detector with BSA* alters residual quantum states, affecting integrity. *Changing the input light power* of *EPPS* would affect its availability. In addition to these active attacks, the *hijacked controller* might also selectively interfere with the session by sabotage.

A. ATTACKS BY A MALICIOUS END USER

What can a malicious terminal node, an 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 (falsely) complains that an application such as BQC will not work, the network will have to initiate careful

Attacker's action	Attacker controls	Components under attack	Compromised elements
False failure report	MNode	Network reliability	Availability
QDoS attack	ENode and MNode	Network resources	Integrity, Availability
Malicious application	ENode	Terminal qubit	Confidentiality, Integrity, Availability
Dishonest quantum computation	ENode	Performed quantum computation	Integrity
Link down attack	RNode	Network resources	Availability
Link connection attack	RNode	Network resources	Integrity, Availability
Man-in-the-middle attack	RNode	QKD operation	Confidentiality
Switching disruption	XNode	Network reliability	Integrity, Availability
Framing innocent repeaters	XNode	Local area network	Integrity, Availability
Path black hole	Classical path management	Path setup information	Availability
QDDoS attack	Multiple ENodes	Service providing QNode	Integrity, Availability
Framing using multiple hijacked QNodes	Multiple QNodes	Wide area network	Integrity, Availability

self-verification. The network system can then conclude that either the claim is falsified or the MNode has failed.

2) QUANTUM DENIAL-OF-SERVICE (QDOS) ATTACK

A DoS 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 [55], the damage will be more serious than the classical DoS. In particular, we should be wary of direct qubit transmissions on DT repeaters (see Section II-C), if the data qubits themselves are sent via the quantum Internet. (If a half-Bell pair is sent followed by quantum teleportation, it does not matter.) Examples of QDoS attacks include the following.

1) A malicious user requests that an oversized key be generated via QKD, overtaxing the quantum link bandwidth.
2) A malicious user requests a massive number of calculations to a cloud quantum computer. Primarily an application server problem, this also affects network resource consumption and operations.

In order to counter these attacks, defenses in the classical plane, such as application behavior monitoring and request filtering, are important. ENode and MNode are capable of these attacks.

Given physical access to an ENode, an attacker can easily entangle additional qubits into a state. This additional entanglement generally destroys the usefulness of a quantum state, acting as a QDoS attack. This attack is similar to attempts to eavesdrop on QKD. More formally, the intended qubits are subsystem of the larger entangled state and, hence, are left in a mixed state.

3) MALICIOUS APPLICATION

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 article. However, such threats from applications need careful discussion. *Malicious application* may disclose the quantum data of any

session, disrupting the confidentiality. Since fundamentally other components are not made to detect abnormalities of quantum applications, malicious applications are hard to detect.

4) 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 other ENodes. 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 should adopt a method that allows reliable quantum calculations even with a small number of fraudsters [97].

B. ATTACKS BY A MALICIOUS RNODE

An RNode can perform all three types of attacks that ENode (MNode) can. Fundamentally, an RNode participates in control of the two links to which it is connected and of the connections that pass through it. Attacks performed using a hijacked RNode, then, affect one of these two subjects.

1) LINK ATTACKS

Obviously, a malicious RNode can simply mis-operate a link or mis-report the link status, bringing the link down altogether. This results in connections routing around the node and link, resulting in network inefficiency.

More clever, insidious attacks may, for example, have the hijacked RNode perform the Bell test to check the link status in good faith, but not correctly perform the quantum operations required for internode communication. This bad faith attack will cause the network to suspect that another node has failed. This is a limited form of framing, discussed as follows. To prevent more severe performance degradation, the network needs to perform a Bell test undetected by the attacker [2].

2) MAN-IN-THE-MIDDLE ATTACK

This attack technique, in which an attacker creates a fake private connection while eavesdropping and tampering, is popular in the classical Internet. The ENodes believe they
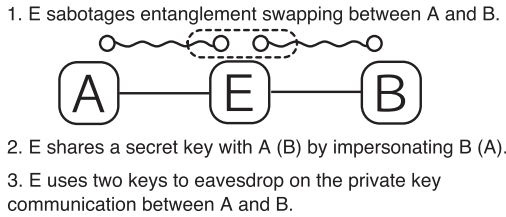
1. E sabotages entanglement swapping between A and B.

2. E shares a secret key with A (B) by impersonating B (A).

3. E uses two keys to eavesdrop on the private key communication between A and B.

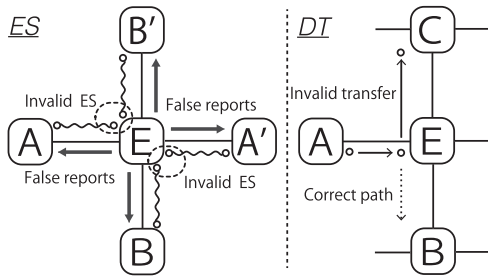**FIG. 4. Man-in-the-middle attack on the quantum Internet.**

FIG. 5. In an ES network, an attacker controlling hijacked Xnode E can share Bell pairs between incorrect node pairs $A - B'$ and $A' - B$ instead of correct pairs $A - A'$ and $B - B'$ using malicious ES. On a DT repeater network, the attacker may intentionally transfer qubits to an inappropriate QNodes C instead of destination B. These disruptions decrease network integrity and availability of transferred information.

FIG. 6. 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.

have a single, private connection, but in reality each is communicating with the node in the middle. If authentication is faulty, the attacker can also execute this attack in the quantum Internet by using a hijacked RNode. For example, we assume a ES type network for QKD operation using BBM92 (see Fig. 4) [98].

A and *B* share a Bell pair for quantum communication, so they ask *E* for ES. The hijacked RNode *E* sabotages the instructions and continues to share two separate streams of Bell pair with *A* and *B*. *A* and *B* try to generate the secret key by measuring qubits they hold, 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*.

C. ATTACKS BY A MALICIOUS XNODE
An XNode is the most powerful QNode; the set of attacks it can perform are a superset of the attacks that an RNode can. 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-mentioned attacks [2].

1) SWITCHING DISRUPTION
An attacker can execute ES without following the distributed ruleset created to govern a connection [96], and forward the Qubit to a node far away from the destination (see Fig. 5). We can detect the intentionally wrong ES operation by Bell test, but we cannot avoid the negative effects on integrity and availability before the detection [2].

2) FRAMING INNOCENT QNODES
The quantum Internet will perform certification to monitor network quality and intrusion. Malicious XNodes can "frame" other RNodes or XNodes as having failed or been hijacked by misreporting certification results or selectively interfering with the communication process through a particular node [2]. This framing can cause a QNode to be excluded from acting on the network. By framing a chosen set of XNodes (a *separator*, in graph theory terms [99]), the malicious node can partition the network (see Fig. 6). To minimize such threats, we need to detect and respond as soon as possible.

The loss of availability due to the isolation of a XNode from the network is more significant than other nodes due to the large amount of connectivity involved. To avoid a significant network performance loss due to the isolation of a XNode, we should keep the certification cycle secret, secure resources that do not identify the communication path and design the network with as rich a topology as possible.

3) PATH BLACK HOLE
Early on, and perhaps even into the indefinite future, the quantum Internet will execute path setup first in the classical (management) plane, then quantum plane will start to generate end-to-end entanglement. Therefore, the classical *packet black hole attack* by advertising an incorrect address block results in collecting path setup packets, preventing the classical packets from arriving at the destination. While this disrupts communication involving affected nodes or networks, because it does not result in new traffic on the quantum plane, any communications not involving the black holed nodes should continue unaffected. This is different from dishonest quantum communication and attacks such as ES sabotage by a single node, which result in wasting quantum plane resources.

D. ATTACKS BY MULTIPLE HIJACKED QNODES

Next, we discuss the case where the attacker has 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) QUANTUM DISTRIBUTED DENIAL-OF-SERVICE (QDDOS) ATTACK

First, we consider the possible attack methods for cooperating malicious ENodes and MNodes. A 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.

The effect of the attack on the classical plane spills over to the quantum plane. 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 attack.

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 (availability) and information loss (integrity).

QDDoS attack will be especially effective to serious in quantum Internet because ENodes will have bandwidth.

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, the 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 false reports from multiple nodes could more easily fool the network.

VI. CONCLUSION

This article is the first attempt to summarize the threats on the quantum Internet. Modeling threats is an essential step toward providing countermeasures against attacks, and is essential to achieve secure and sustainable quantum networks.

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. 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 shares many of the vulnerabilities with a classical network system. A repeater includes classical computing hardware and threats to both integrity and availability can target that hardware.

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 to defend against loss in the network like classical networking. In this sense, directly transmitting data qubits in the DT repeater network has more serious risk against DoS attacks. This problem can be avoided by sending half-Bell pairs even in the third 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 article, 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.

to realize the quantum Internet, and participants in the quantum Internet Research Group (QIRG) of the Internet Research Task Force, for comprehensive and interdisciplinary discussions of the quantum Internet.

REFERENCES

[1] S. Suzuki and R. Van Meter, "Classification of quantum repeater attacks," in *Proc. Network Distributed Syst. Secur. Symp. Workshop Secur. Emerg. Technol.*, 2015, doi: 10.14722/sent.2015.23003.

[2] T. Satoh, S. Nagayama, T. Oka, and R. Van Meter, "The network impact of hijacking a quantum repeater," *Quantum Sci. Technol.*, vol. 3, no. 3, 2018, Art. no. 0 34008, doi: 10.1088/2058-9565/aac11f.

[3] D. Bacon and W. van Dam, "Recent progress in quantum algorithms," *Commun. ACM*, vol. 53, no. 2, pp. 84–93, 2010, doi: 10.1145/1646353.1646375.

[4] A. Montanaro, "Quantum algorithms: An overview," *NPJ Quantum Inf.*, vol. 2, 2016, Art. no. 15023, doi: 10.1038/npjqi.2015.23.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, Jan. 2000, doi: 10.1017/CBO9780511976667.

[6] R. Van Meter and C. Horsman, "A blueprint for building a quantum computer," *Commun. ACM*, vol. 56, no. 10, pp. 84–93, Oct. 2013, doi: 10.1145/2494568.

[7] M. M. Wilde, *Quantum Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2013.

[8] A. Dahlberg *et al.*, "A link layer protocol for quantum networks," 2019, *arXiv:1903.09778*. doi: 10.1145/3341302.3342070.

[9] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, Jun. 2008, doi: 10.1038/nature07127.

[10] R. Van Meter, *Quantum Networking*. Chichester, U.K.: Wiley, May 2014, doi: 10.1002/9781118648919.

[11] S. Wehner, D. Elkouss, and R. Hanson, "Quantum Internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018, doi: 10.1126/science.aam9288.

[12] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür, "Long-range big quantum-data transmission," *Phys. Rev. Lett.*, vol. 120, Jan. 2018, Art. no. 0 30503, doi: 10.1103/PhysRevLett.120.030503.

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Dec. 1984, vol. 11, pp. 175–179, doi: 10.1016/j.tcs.2014.05.025.

[14] A. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991, doi: 10.1103/PhysRevLett.67.661.

[15] 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, doi: 10.1103/RevModPhys.79.555.

[16] D. Gottesman, T. Jennewein, and S. Croke, "Longer-baseline telescopes using quantum repeaters," *Phys. Rev. Lett.*, vol. 109, Aug. 2012, Art. no. 070503, doi: 10.1103/PhysRevLett.109.070503.

[17] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, "Quantum clock synchronization based on shared prior entanglement," *Phys. Rev. Lett.*, vol. 85, no. 9, pp. 2010–2013, 2000, doi: 10.1103/PhysRevLett.85.2010.

[18] 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, doi: 10.1103/PhysRevA.59.4249.

[19] L. K. Grover, "Quantum telecomputation," 1997, *arXiv*: quant-ph/9704012.

[20] S. Nagayama, "Distributed quantum computing utilizing multiple codes on imperfect hardware," Ph.D. dissertation, Keio Univ., Graduate school of Media and Governance, Tokyo, Japan, 2017. [Online]. Available: https://arxiv.org/abs/1704.02620

[21] A. Steane and D. Lucas, "Quantum computing with trapped ions, atoms and light," *Fortschritte Phys.*, vol. 48, no. 9–11, pp. 839–858, 2000, doi: 10.1002/1521-3978.

[22] 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, pp. 354–365, May 2006, doi: 10.1145/1150019.1136517.

[23] M. Ben-Or and A. Hassidim, "Fast quantum Byzantine agreement," in *Proc. 37th Annu. ACM Symp. Theory Comput.*, 2005, pp. 481–485, doi: 10.1145/1060590.1060662.

[24] C. Crepeau, D. Gottesman, and A. Smith, "Secure multi-party quantum computation," in *Proc. 34th Annu. ACM Symp. Theory Comput.*, 2002, pp. 643–652, doi: 10.1103/PhysRevA.102.022405.

[25] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Measurement-based and universal blind quantum computation," in *Formal Methods for Quantitative Aspects of Programming Languages*. Berlin, Germany: Springer, 2010, pp. 43–86, doi: 10.1007/978-3-642-13678-8_2.

[26] 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, doi: 10.1145/2700248.

[27] C. Gentry, "Computing arbitrary functions of encrypted data," *Commun. ACM*, vol. 53, no. 3, pp. 97–105, Mar. 2010, doi: 10.1145/1666420.1666444.

[28] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Rev. Modern Phys.*, vol. 81, no. 2, pp. 865–942, 2009, doi: 10.1103/RevModPhys.81.865.

[29] R. F. Werner and M. M. Wolf, "Bell inequalities and entanglement," 2001, *arXiv:quant-ph/0107093*.

[30] 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, doi: 10.1103/PhysRevLett.77.2818.

[31] C. Elliott, "Building the quantum network," *New J. Phys.*, vol. 4, p. 46, 2002, doi: 10.1088/1367-2630/4/1/346.

[32] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," in *Proc. SIGCOMM ACM*, Aug. 2003, doi: 10.1145/863955.863982.

[33] 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 Commun.*, vol. 2, 2011, Art. no. 349, doi: 10.1038/ncomms1348.

[34] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Â. Larsson, "Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution," *Sci. Adv.*, vol. 1, no. 11, 2015, Art. no. e1500793, doi: 10.1126/sciadv.1500793.

[35] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. Photon.*, vol. 4, no. 10, pp. 686–689, 2010, doi: 10.1038/NPHOTON.2010.214.

[36] V. Makarov and D. Hjelme, "Faked states attack on quantum cryptosystems," *J. Modern Opt.*, vol. 52, no. 5, pp. 691–705, 2005, doi: 10.1080/09500340410001730986.

[37] A. Pirker, V. Dunjko, W. Dür, and H. J. Briegel, "Entanglement generation secure against general attacks," *New J. Phys.*, vol. 19, no. 11, 2017, Art. no. 113012, doi: 10.1088/1367-2630/aa8086.

[38] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, no. 23, 2007, Art. no. 230501, doi: 10.1103/PhysRevLett.98.230501.

[39] 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," Mar. 2013, *arXiv:1303.3456v1*.

[40] A. Mink, S. Frankel, and R. Perlner, "Quantum key distribution (QKD) and commodity security protocols: Introduction and integration," *Int. J. Netw. Secur. Appl.*, vol. 1, no. 2, Jul. 2009.

[41] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075001, doi: 10.1088/1367-2630/11/7/075001.

[42] M. Sasaki *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011, doi: 10.1364/OE.19.010387.

[43] D. Stucki *et al.*, "Long-term performance of the swissquantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, 2011, Art. no. 123001, doi: 10.1088/1367-2630/13/12/123001.

[44] S. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Exp.*, vol. 22, no. 18, pp. 21739–21756, 2014, doi: 10.1364/OE.22.021739.

[45] S. M. Bellovin, "Security problems in the TCP/IP protocol suite," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 19, no. 2, pp. 32–48, 1989, doi: 10.1145/378444.378449.

[46] M. A. Bishop, *Computer Security: Art and Science*, 2nd ed. Reading, MA, USA: Addison-Wesley, 2018.

[47] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar. 1993, doi: 10.1103/PhysRevLett.70.1895.

[48] R. Van Meter, T. Satoh, T. D. Ladd, W. J. Munro, and K. Nemoto, "Path selection for quantum repeater networks," *Netw. Sci.*, vol. 3, no. 1–4, pp. 82–95, 2013, doi: 10.1007/s13119-013-0026-2.

[49] S. H. Weingart, "Physical security devices for computer subsystems: A survey of attacks and defences," in *Proc. 2nd Int. Workshop Cryptographic Hardware Embedded Syst.*, 2000, doi: 10.1007/3-540-44499-8_24.

[50] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, "Threats to Networked RFID Systems," in *Unique Radio Innovation for the 21st Century*. Berlin, Germany: Springer, 2010, pp. 39–63, doi: 10.1007/978-3-642-03462-6_3.

[51] L. Mirowski, J. Hartnett, and R. Williams, "An RFID attacker behavior taxonomy," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 79–84, Oct.–Dec. 2009, doi: 10.1109/MPRV.2009.68.

[52] D. L. Moehring *et al.*, "Entanglement of single-atom quantum bits at a distance," *Nature*, vol. 449, no. 7158, pp. 68–71, 2007, doi: 10.1038/nature06118.

[53] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien, "Quantum computers," *Nature*, vol. 464, no. 7285, pp. 45–53, 2010, doi: 10.1038/nature08812.

[54] J. S. Bell, "On the Einstein-Podolsky-Rosen paradox," *Physics*, vol. 1, no. 3, pp. 195–200, 1964, doi: 10.1103/PhysicsPhysiqueFizika.1.195.

[55] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982, doi: 10.1038/299802a0.

[56] 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, doi: 10.1103/PhysRevLett.71.4287.

[57] 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," *Phys. Rev. Lett.*, vol. 76, no. 5, pp. 722–725, 1996, doi: 10.1103/PhysRevLett.76.722.

[58] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Rep. Prog. Phys.*, vol. 76, no. 7, 2013, Art. no. 076001, doi: 10.1088/0034-4885/76/7/076001.

[59] W. Dür and H. J. Briegel, "Entanglement purification and quantum error correction," *Rep. Prog. Phys.*, vol. 70, no. 8, 2007, Art. no. 1381, doi: 10.1088/0034-4885/70/8/R03.

[60] H.-J. Briegel, W. Dür, J. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, 1998, doi: 10.1103/PhysRevLett.81.5932.

[61] T. Morimae, "Verification for measurement-only blind quantum computing," *Phys. Rev. A*, vol. 89, Jun. 2014, Art. no. 060302, doi: 10.1103/PhysRevA.89.060302.

[62] T. Morimae and K. Fujii, "Blind quantum computation protocol in which alice only makes measurements," *Phys. Rev. A*, vol. 87, May 2013, Art. no. 050301, doi: 10.1103/PhysRevA.87.050301.

[63] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," *Sci. Rep.*, vol. 6, 2016, Art. no. 20463, doi: 10.1038/srep20463.

[64] 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, doi: 10.1103/PhysRevA.59.169.

[65] L. Jiang, J. M. Taylor, N. Khaneja, and M. D. Lukin, "Optimal approach to quantum communication using dynamic programming," *Proc. Nat. Acad. Sci. USA*, vol. 104, no. 44, pp. 17291–17296, 2007, doi: 10.1073/pnas.0703284104.

[66] 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, doi: 10.1103/RevModPhys.83.33.

[67] 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, May 2010, Art. no. 180503, doi: 10.1103/PhysRevLett.104.180503.

[68] 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, 2009, Art. no. 032325, doi: 10.1103/PhysRevA.79.032325.

[69] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, "Long range failure-tolerant entanglement distribution," *New J. Phys.*, vol. 15, no. 2, 2013, Art. no. 023012, doi: 10.1088/1367-2630/15/2/023012.

[70] E. Knill and R. Laflamme, "Concatenated quantum codes," Aug. 1996, *ArXiv: quant-ph/9608012*.

[71] 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 J. Phys.*, vol. 18, no. 8, 2016, Art. no. 083015, doi: 0.1088/1367-2630/18/8/083015.

[72] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Ultrafast and fault-tolerant quantum communication across long distances," *Phys. Rev. Lett.*, vol. 112, Jun. 2014, Art. no. 250501, doi: 10.1103/PhysRevLett.112.250501.

[73] J. Eisert *et al.*, "Quantum certification and benchmarking," *Nature Rev. Phys.*, vol. 2, pp. 382–390, 2020, doi: 10.1038/s42254-020-0186-4.

[74] J. B. Altepeter, E. R. Jeffrey, and P. G. Kwiat, "Photonic state tomography," *Adv. Atomic, Mol., Opt. Phys.*, vol. 52, pp. 105–159, 2005, doi: 10.1016/S1049-250X(05)52003-2.

[75] M. Cramer, M. B. Plenio, S. T. Flammia, and R. Somma, "Efficient quantum state tomography," *Nature*, vol. 1, no. 9, 2010, Art. no. 149, doi: 10.1038/ncomms1147.

[76] D. James, P. G. Kwiat, W. J. Munro, and A. G. White, "Measurement of qubits," *Phys. Rev. A*, vol. 64, 2001, Art. no. 052312, doi: 10.1103/PhysRevA.64.052312.

[77] Y. Liu *et al.*, "Device-independent quantum random-number generation," *Nature*, vol. 562, no. 7728, pp. 548–551, 2018, doi: 10.1038/s41586-018-0559-3.

[78] B. W. Reichardt, F. Unger, and U. Vazirani, "Classical command of quantum systems," *Nature*, vol. 496, no. 7446, pp. 456–460, 2013, doi: 10.1038/nature12035.

[79] M. Hajdušek, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Device-independent verifiable blind quantum computation," 2015, *arXiv:1502.02563*.

[80] M. Hayashi and M. Hajdušek, "Self-guaranteed measurement-based quantum computation," *Phys. Rev. A*, vol. 97, May 2018, Art. no. 052308, doi: 10.1103/PhysRevA.97.052308.

[81] I. Šupić and J. Bowles, "Self-testing of quantum systems: A review," *Quantum*, vol. 4, p. 337, Sep. 2020, doi: 10.22331/q-2020-09-30-337.

[82] 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, doi: 10.1103/PhysRevLett.23.880.

[83] M. Koashi and A. Winter, "Monogamy of quantum entanglement and other correlations," *Phys. Rev. A*, vol. 69, no. 2, 2004, Art. no. 022309, doi: 10.1103/PhysRevA.69.022309.

[84] B. M. Terhal, "Is entanglement monogamous?," *IBM J. Res. Dev.*, vol. 48, no. 1, pp. 71–78, 2004, doi: 10.1147/rd.481.0071.

[85] P. Pathumsoot, T. Matsuo, T. Satoh, M. Hajdušek, S. Suwanna, and R. Van Meter, "Modeling of measurement-based quantum network coding on IBMQ devices," *Phys. Rev. A*, vol. 101, no. 5, May 2020, Art. no. 052301, doi: 10.1103/PhysRevA.101.052301.

[86] T. Oka, T. Satoh, and R. Van Meter, "A classical network protocol to support distributed quantum state tomography," in *Proc. Quantum Commun. Inf. Technol.*, 2016, doi: 10.1109/GLOCOMW.2016.7848802.

[87] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, "Hacking the Bell test using classical light in energy-time entanglementbased quantum key distribution," *Sci. Adv.*, vol. 1, no. 11, 2015, Art. no. e1500793, doi: 10.1126/sciadv.1500793. [Online]. Available: http://advances.sciencemag.org/content/1/11/e1500793

[88] Y. Sun *et al.*, "Securing internet applications from routing attacks," *Commun. ACM*, vol. 64, no. 6, pp. 86–96, May 2021, doi: 10.1145/3429775.

[89] D. J. Reilly, "Engineering the quantum-classical interface of solid-state qubits," *NPJ Quantum Inform.*, vol. 1, 2015, Art. no. 15011, doi: 10.1038/npjqi.2015.11.

[90] J. Kim *et al.*, "1100x1100 port MEMS-based optical crossconnect with 4-dB maximum loss," *IEEE Photon. Technol. Lett.*, vol. 15, no. 11, pp. 1537–1539, Nov. 2003, doi: 10.1109/LPT.2003.818653.

[91] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Phys. Rev. Lett.*, vol. 75, pp. 4337–4341, Dec. 1995, doi: 10.1103/PhysRevLett.75.4337.

[92] 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," *IEEE J. Sel. Topics Quantum Electron.*, vol. 21, no. 3, pp. 168–177, May/Jun. 2015, doi: 10.1109/JSTQE.2014.2365585.

[93] O. Benoît, *Fault Attack*. Boston, MA, USA: Springer, 2005, doi: 10.1007/0-387-23483-7_157.

[94] K. Lemke and C. Paar, *Physical Attacks*. Boston, MA, USA: Springer, 2005, doi: 10.1007/0-387-23483-7_300.

[95] O. Sakarya, M. Winczewski, A. Rutkowski, and K. Horodecki, "Hybrid quantum network design against unauthorized secret-key generation, and its memory cost," *Phys. Rev. Res.*, vol. 2, Oct. 2020, Art. no. 043022, doi: 10.1103/PhysRevResearch.2.043022.

[96] T. Matsuo, C. Durand, and R. Van Meter, "Quantum link bootstrapping using a RuleSet-based communication protocol," *Phys. Rev. A*, vol. 100, no. 5, 2019, Art. no. 052320, doi: 10.1103/PhysRevA.100.052320.

[97] J. F. Fitzsimons and E. Kashefi, "Unconditionally verifiable blind quantum computation," *Phys. Rev. A*, vol. 96, Jul. 2017, Art. no. 012303, doi: 10.1103/PhysRevA.96.012303.

[98] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, 1992, doi: 10.1103/PhysRevLett.68.557.

[99] J. C. Doyle *et al.*, "The "robust yet fragile" nature of the Internet," *Proc. Nat. Acad. Sci. USA*, vol. 102, no. 41, pp. 14497–14502, 2005, doi: 10.1073/pnas.0501426102.

Takahiko Satoh studied at Keio University, Yokohama, Japan, and the University of Tokyo (UT), Tokyo, Japan, in 2015. He received the Ph.D. degree in computer science from UT.

He is currently a Project Assistant Professor of the Keio University Quantum Computing Center, Yokohama, Japan. His research field is quantum computing and quantum networking, particularly quantum network coding, NISQ algorithm design, and quantum Internet security.

Dr. Satoh is a member of the Physical Society of Japan (JPS).

Shota Nagayama (Member, IEEE) received the Ph.D degree in media and governance from Keio University, Yokohama, Japan, in 2017.

He is currently a Senior Researcher with Mercari, Inc., Tokyo, Japan, and the Founder and co-ordinator of the Quantum Internet Task Force, an interdisciplinary industry-academia collaboration research consortium established in Japan. His research interests include quantum Internet, quantum network architectures, quantum computer architecture, quantum error correction, and crypto communication systems utilizing quantum key distribution.

Dr. Nagayama is a member of ACM, APS, and IPSJ.

Shigeya Suzuki received the Ph.D. degree from the Graduate School of Media and Governance, Keio University, Yokohama, Japan, in 2012.

He is currently a Researcher specializing in computer networks and distributed systems. He is an expert in systems architecture and software development. He is currently research interests are on Blockchain Technology. He is a Project Professor with the Graduate School of Media and Governance, Keio University, an Associate Director of the Keio Blockchain Laboratory, and also a Board Member of the WIDE Project.

Dr. Suzuki is a member of ACM, IACR, IEICE, and IPSJ.

Takaaki Matsuo received the master's degree from the Graduate School of Media and Governance, Keio University, Yokohama, Japan, in 2019.

He is currently a System Engineer with Softbank Corp., Tokyo, Japan. His research interests include quantum network architecture and layered protocol designing for quantum networks.

Mr. Matsuo member of the AQUA group in the WIDE project

Michal Hajdušek received the Ph.D. degree in theoretical quantum information from Leeds University, Leeds, U.K., in 2010.

He is currently a Project Assistant Professor with the Graduate School of Media and Governance, Keio University Shonan Fujisawa Campus, Fujisawa, Japan. His research interests include quantum networking, quantum computation, and dynamics of open quantum systems.
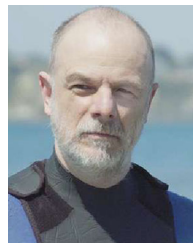
Rodney Van Meter (Senior Member, IEEE) received the Ph.D. degree in computer science from Keio University, Yokohama, Japan, in 2006.

He is currently a Professor of Environment and Information Studies with Keio University Shonan Fujisawa Campus, Fujisawa, Japan. Besides quantum networking and quantum computing, his research interests include storage systems, networking, and post-Moore's law computer architecture.

Dr. Meter is a member of ACM, the American Physical Society, and the American Association for the Advancement of Science.