Classification of Quantum Repeater Attacks

Shigeya Suzuki[*†], Rodney Van Meter[‡]
[*]Graduate School of Media and Governance, Keio University, Kanagawa, Japan
[†]Auto-ID Lab Japan, Keio Research Institute at SFC, Keio University, Kanagawa, Japan
E-mail: shigeya@wide.ad.jp
[‡]Faculty of Environment and Information Studies, Keio University, Kanagawa, Japan
E-mail: rdv@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, 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.**

I. Introduction

The computers and networks in common use today are built on classical notions of information, generally using small amounts of electrical charge, the orientation of tiny magnets, and optical signals as data. We typically treat the data states as binary numbers or symbols and manipulate them using familiar, comfortable Boolean logic. But over the last three decades, a new theory of information based on quantum mechanics has been discovered, quantum algorithms have been developed, experimental demonstrations of quantum computing have proliferated, and large-scale machines are on the drawing boards [24], [30], [2], [27]. One of the oldest and most successful areas in quantum information has been quantum networks [26].

Work on quantum networks began with the recognition that quantum states serve as exquisite sensors of the real world, and can be used to detect the presence of eavesdroppers on a quantum communication channel while creating shared, secret random numbers useful as keys for encrypting classical data, known as *quantum key distribution* [6]. 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 [19], [15], [3]. 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 [5], [12]. Recently, Broadbent *et al.* developed a fully blind method of conducting any arbitrary quantum calculation [8], [9]. Unlike Gentry's classical homomorphic encryption [14], this technique hides the algorithm itself as well as the input and output data. Thus, if we can find ways of distributing quantum information over long distances, we will enable valuable new functionality.

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

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

Here, we will concern ourselves primarily with the issue of network stability for quantum networks, but in order to do so we will develop a model of attacks on individual components. As engineers working in both classical and quantum networking, we naturally wish to apply the lessons learned in classical networks to minimize security issues with developing quantum networks. We have asked ourselves two questions: *Do quantum networks present different operational vulnerabilities than classical networks?* and *Can we apply known classical countermeasures, or are new techniques required?* In this paper, we discuss the former question and leave the latter for

SENT '15, 8 February 2015, San Diego, CA, USA
Copyright 2015 Internet Society, ISBN 1-891562-39-8
http://dx.doi.org/10.14722/sent.2015.23003

future work.

In the process of classifying these attacks, we have found it useful to refer to proposed taxonomies for classical systems, especially RFID systems, by Weingart [29], Mitrokotsa [22], and Mirowski [21]. Quantum repeater systems and RFID systems has similar properties that make this analogy apt: both systems are tightly coupled hybrid systems of sensing and software elements, and also expect to make use of the effects of interaction with the outside world.

While we can model the basic hardware architecture of a quantum repeater and have some idea of the kind of elements needed, we do not have a concrete design for a specific implementation of such a system. However, we still think it is possible to provide an analysis of a quantum network system, so we begin with a hardware model (Sec. III) that will allow us to identify points of attack (Sec. IV), then classify the attacks (Sec. V).

II. Quantum Repeater Networks

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

Experimental physicists have demonstrated the creation of entanglement over short distances using single photons [23]. Numerous approaches have been proposed and some of them demonstrated, but for our purposes here a single example will suffice. Individual quantum bits, or *qubits*, at each node may be single atoms suspended in a vacuum or another of the dozens of technologies under experimental development. A qubit at each end of a link is coaxed to emit a photon that is entangled with the qubit. The two photons are routed toward each other and ultimately interfere in a fashion that erases knowledge of where each photon came from, leaving the two stationary qubits entangled in what is called a *Bell pair*, named for a proposal made by John Bell almost exactly fifty years ago [4].

Unfortunately, we can't transmit those photons over arbitrary distances. In optical fiber, the probability of success falls exponentially with distance as photons are lost, and classical amplifiers cannot be used in quantum networks because independent copies of quantum data cannot be made [31]. Moreover, in any interesting network, naturally, we want to support multi-hop paths between pairs of nodes, rather than requiring a direct link between each pair. Both problems can be solved by using *entanglement swapping*, which takes two Bell pairs, one between nodes A and B and one between nodes B and C, and splices them together to form a single Bell pair that spans from A to C [32]. Entanglement swapping can be said, very roughly, to perform the role held by packet forwarding in the Internet, with the significant caveat that it operates all along the path rather than at a node at a time.

The quality, or *fidelity*, of these Bell pairs declines as we perform more of these swapping operations, eventually destroying the quantumness of the data and leaving only random classical noise. This problem can be solved using a form of error detection known as *purification* or using quantum error correction. Purification plus entanglement swapping is the canonical setup of a chain of quantum repeaters [7].

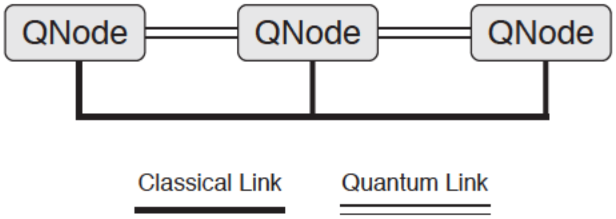

Fig. 1. Quantum Network Node (QNode) and links. QNodes are connected via quantum link and classical link.

More than two qubits can be entangled at one time, either intentionally by the end nodes, by an eavesdropper trying to listen in, or as the quantum information leaks out of imperfectly isolated devices. We can detect the presence of an eavesdropper and assess the fidelity of two-qubit entanglement using a process known as quantum tomography [18], [1], [11]. As we assess the fidelity of our two-party entanglement, we simultaneously rule out that a third party is entangled with us [10], [20], [25]. This serves as the basis of one form of quantum key distribution [13]. This process requires the generation and consumption of many Bell pairs to determine the statistical characteristics of a quantum channel or path, and cannot be used to determine anything about any individual Bell pair. Selection of Bell pairs to be sacrificed for tomography must be random; if the eavesdropper can predict which pairs will be used, she can remain undetected simply by electing not to entangle or interfere with those pairs.

III. Model of Quantum Repeater Networks

In this section, we describe our model of a Quantum Repeater Network and its elements.

A. *Quantum Repeater Node and its communication*

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

Fig. 1 depicts a small quantum repeater network consisting of three quantum repeater nodes (labeled QNode) connected by quantum links and a classical link. QNodes are connected by a quantum communication capable channel, such as a fiber. Physically connected QNodes can create entangled pairs of qubits. Each QNode has network addresses, such as IP addresses, for various inter-repeater classical information communication. While our minimum requirement is having an address unique among the set of reachable quantum repeater

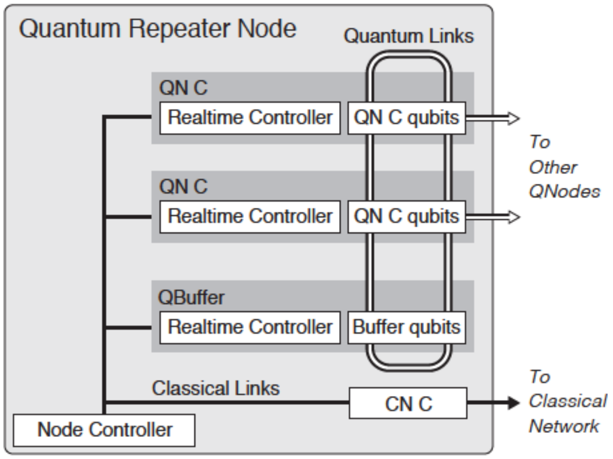

Fig. 2. Model of a Quantum Repeater Node (QRNode). Consists of multiple Quantum Network Interface Card (QNIC) and single Quantum Buffer (QBuffer), single Classical Network Interface Card (CNIC) and a node controller.

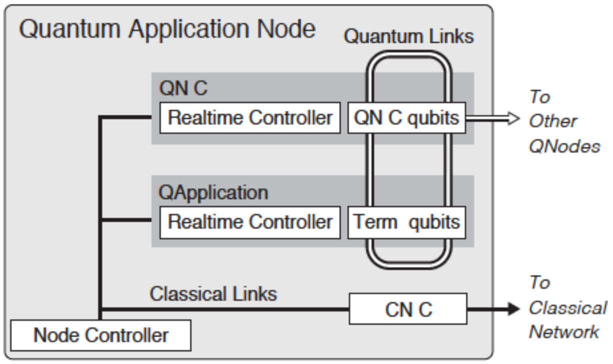

Fig. 3. Model of a Quantum Application Node (QANode). Consists of single Quantum Network Interface Card (QNIC) and single Quantum Application with terminal qubits (QApplication), single Classical Network Interface Card (CNIC) and a node controller.

nodes, to simplify our discussion, we assume all quantum repeater nodes have global Internet access, which means each quantum repeater node must have IP addresses. The discussion which may require consideration on global-scale Internet, such as a topic like distributed denial of service (DDoS) style attack, is outside of the discussion of this paper.

We modeled two types of QNodes:

Quantum Repeater Node (QRNode): A QRNode (Fig. 2) works to create networks. It will have multiple quantum interfaces (QNICs) and may have qubits for buffering (QBuffer), assisted by a classical controller and a classical network interface.

Quantum Application Node (QANode): A QANode (Fig. 3) works as terminal node for running quantum applications. It has at least one QNIC and an application module that has terminal qubits (QApplication), also assisted by a classical controller and a classical network interface.

Each QNode consists of several elements.

B. *Elements of a QNode*

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

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

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

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 like Ethernet. The CNIC provides inter-repeater and application node communications, generally carrying soft real time information necessary for interpreting quantum information and determining future operations.

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

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

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

Node Controller: The Node controller communicates with other QNodes and controls QNIC, QBuffer and QApplication to achieve its goal: for a repeater node, to create entanglement with one of a local QNIC's QNIC-qubits and a remote quantum node's QNIC-qubit; for an application node, to create remote entanglement with its QNIC-qubits, then entangle the terminal qubits to run the application.

QNIC-qubits: Each QNIC has multiple qubits (QNIC-qubits). These qubits create entanglement with remote QNIC-qubits.

Buffer-qubits: Buffer qubits in a QBuffer can hold entangled states, freeing QNIC-qubits for reuse.

Terminal-qubits: Terminal qubits in a QApplication.

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

Classical node internal links: All classical elements in a QNode are connected by classical internal links. A link might be hardware, or just a software based interface.

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

A QNode requires several external resources to operate.

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

Quantum external connectivity: All QNICs will be connected to other QNICs (or QNodes).

Electric power: Chassis should be externally powered, possibly by multiple sources.

IV. Potential Attacks

In this section, we describe the motivation of attacks with a few examples and resources of interest for attackers, then potential points of attack, by element.

A. Motivation and Examples

As we alluded to in the introduction, an attacker's purpose may be:

- *to steal* quantum information or *to hijack* a quantum connection in order to steal either information or computing resources; or
- *to disrupt* either the integrity or availability of quantum nodes or quantum networks.

These goals obviously parallel those in classical networks. The biggest change in quantum networks is the presence of entanglement, so we begin by considering the impact of entanglement. Considering theft of information or resources leads us to wonder, *can use of entanglement result in copying or disclosure of quantum data during a session? Can entanglement lurking in a repeater compromise later sessions by hijacking valuable qubits or undetected disclosure?* Even without entanglement, *can control of the quantum hardware elements allow hijacking or disclosure?*

Considering disruption of operations brings different questions. We know that classical hardware is vulnerable to damage from strong electrical or optical pulses, leading us to wonder, *are quantum nodes more vulnerable than classical systems?* This question is implementation dependent, and is a moving target we will not address here. More generally, *can the function of creating end-to-end entanglement be disrupted on a scale disproportionate to the fraction of the network compromised?* While the attacks aiming at theft may affect operation of a communication session, this category of question can lead to us to question network functionality such as routing [28]. We will not fully answer these questions in this paper, but the framework here will lead us to categorize ways in which attackers might attempt to achieve these goals.

B. Resources of Interest and Target Elements

An attacker wishing to achieve one of the goals of theft or disruption obviously will begin by attempting to compromise some of the qubits in the system.

- For stealing, either qubit or quantum computing resource can be stolen by retrieving one member of the entangled Bell pair.
- For disrupting, either elements of a quantum network node or quantum network channel can be a target.

Two categories of elements exist in QNodes: quantum computing elements and classical computing elements. Each can be attacked independently. Sophisticated attacks on both quantum and classical parts in a coordinated manner are also possible.

We have categorized elements into seven groups by their properties with regard to their security:

1) Terminal qubits: The ultimate goal of the system is to create entanglement between qubits in QApplication, which is the terminus of the entanglement. The quantum operation which the quantum application wants to run is executed terminal qubit to terminal qubit, and is not affected by other qubits. Terminal qubits are connected to other qubits only via the in-node quantum channel (see below).

2) Interface qubits: Qubits in QNICs are used only temporarily. Once terminal qubits are entangled, the qubits in QNICs play no further role in that operation. Interface qubits are connected with other qubits either by the inter-node quantum channel or the in-node quantum channel (see below).

3) Buffer qubits: Qubits in QBuffers are used temporarily. Once terminal qubits are entangled, the qubits in QBuffers play no further role in that operation. Buffer qubits are connected with other qubits via the in-node quantum channels (see below) only.

4) In-node quantum channels: Internal quantum channels between QNIC-qubits, QBuffer-qubits and QApplication-qubits.

5) Inter-node quantum channels: Physical quantum channel between two QNodes (or two QNICs). The inter-node quantum channel is an essential element for creating basic inter-QNode entanglement.

6) Inter-node classical channels: The inter-node classical channel provides a basis for coordination between nodes. Reliable and timely communication is important to create and maintain terminal qubit to terminal qubit entanglement.

7) Classical elements of nodes: Attacks on classical computing elements are well studied and explained by e.g. Weingart [29]. In our networks, the following classical computing elements can be attacked:

- CNIC
- Internal classical channels
- External classical channels
- Controller resources such as clock, memory, processor
- Chassis providing electric power

V. Classification of Attacks

We will visit all seven groups of potential targets one by one to assess three key aspects of information security management: confidentiality, integrity, and availability [16]. We refer to the work of Mitrokotsa [22] as a basis, then simplify the analysis since we cannot estimate costs.

A. Terminal qubits

Terminal qubits can interact only with interface qubits, buffer qubits, or other terminal qubits via the in-node quantum channel. Since terminal qubits do not have direct external connectivity, a successful attack on a inter-node quantum channel cannot be extended directly to an attack on terminal qubits. Terminal qubits will be used by the application itself, so naturally compromise of the application compromises the qubits.

1) Confidentiality: 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 direct manipulation once stored in terminal qubits, but if an eavesdropper has entangled a qubit of hers with our quantum variable before it reaches this buffer, is this characteristic altered? In fact, no; an eavesdropper gains no access to information she did not already have at the time she entangled her qubit with ours.

However, assuming terminal qubits are being used to temporarily hold halves of Bell pairs (completely generic states with no secret information) before teleporting valuable quantum data, we must *randomly* select some of the Bell pairs for tomography to determine that an eavesdropper has not entangled her qubits with ours, as we described in Sec. II.

Of course, since a terminal qubit is connected to a quantum application controller, a compromise on the application side of the hardware affects terminal qubits. This loss of control is beyond scope of this paper since the application controller is not part of the repeater.

2) Integrity: As just noted, of course data can be disclosed or destroyed if the controller has been compromised. Out-of-system attacks such as direct irradiation of a device with RF noise could damage the quantum data and leave us with garbage. If the attack is instead effected through the qubit operation mechanism, data may be manipulated to alter values in chosen ways.

3) Availability: Direct attacks on the hardware, such as the RF attack, affect availability by preventing the designed operation of qubits. For that kind of attack, an attacker may not even need access to the target device itself, as radio waves can blanket an area from a modest distance. Even with good RF shielding, interference effects as weak as subway power and control systems a kilometer away are known to affect some systems. Other attacks, such as on the cooling or other control systems, may be harder to carry out remotely.

B. Interface qubits

Interface qubits can be connected with interface qubits in other QNodes via an inter-node quantum channel. They are connected with either buffer qubits or terminal qubits inside the QNode. Since interface qubits have direct contact with the world outside of the QNode using a physical channel, they may be the most vulnerable elements.

1) Confidentiality: The need for randomized quantum tomography while working with a stream of Bell pairs is the same as for terminal qubits. On the other hand, since interface qubits are connected to an external system, they might be affected either by an external system or the quantum channel. Among the many attacks on QKD implementations developed in Makarov's lab, Jain *et al.* described an eavesdropper that can probe a BB84 quantum key distribution (QKD) system [6] by sending a bright pulse from the quantum channel into the interface and analyzing the back-reflected pulses [17], a classical attack on the hardware used for the quantum states. Entanglement-based QKD protocols do not have this weakness, but a similar attack in which some optical detectors are saturated could be used in a man-in-the-middle attack. (Note: we may categorize this attack under "inter-node quantum channel" also.)

2) Integrity: Attackers may use the same means to destroy data as with terminal qubits, but in addition may be able to directly manipulate quantum states by inserting unauthorized and unexpected optical pulses into the channel.

3) Availability: Because the qubits are directly attached to the channel, it is possible to affect availability. A typical classic attack like destruction or removal of hardware prevents the designed operation of the qubits, but for that kind of attack, the attacker should have access to the target device itself. Out-of-system attacks are the same as terminal qubits.

C. Buffer qubits

Buffer qubits can interact with either interface qubits or terminal qubits. Since buffer qubits do not have any external connectivity, they are difficult to affect from external (inter-node) quantum channels or the application side of other hardware. Their vulnerabilities are similar to terminal qubits, but compromising classical control of a repeater will be different from compromising an application node.

1) Confidentiality: Same as terminal qubits.

2) Integrity: Same as terminal qubits, with the addition that repeater placement may make it easier or harder to physically access the node.

3) Availability: Same as terminal qubits, with the addition that repeater placement may make it easier or harder to physically access the node.

D. In-node quantum channels

In-node quantum channels provide interconnection between terminal qubits, buffer qubits and interface qubits. Since the in-node quantum channel is not exposed to the outside of the node, only indirect attack is possible.

1) Confidentiality: The direct optical attack described above is not possible on the in-node quantum channel without directly modifying the hardware.

2) Integrity: Since this is a channel, discussion on integrity is not applicable.

3) Availability: By attacking the hardware, it is possible to affect availability. A typical classic attack like destruction or removal of hardware prevents the correct operation of a channel, preventing any sharing of entanglement unless another quantum connection between subsystems exists.

E. Inter-node quantum channels

By using an inter-node quantum channel, interface qubits can create node-to-node single hop entanglement. Since the inter-node quantum channels are exposed, they can be potential targets.

1) Confidentiality: The detector attack described above may be used to determine hardware settings, while the detector saturation attack could be used to control what the classical hardware sees. More analysis of this impact on repeater operation is necessary. Since inter-node quantum channel is just a fiber or similar channel between QNodes, it is relatively easy to get access to these channels.

2) Integrity: Since this is a channel, discussion on integrity is not applicable.

3) Availability: By attacking the hardware, it is possible to affect availability. Any attempt to copy the data in this channel or to "listen in" by measuring the data will result in tomography detecting poor fidelity and the presence of an eavesdropper. This denial of service attack is one of the most obvious weaknesses of quantum networks if robustness is an important design goal. Since an inter-node quantum channel is just a fiber or such cable between QNodes, it is relatively easy to get access to these channels.

F. Inter-node classical channels

Inter-node classical channels are required to coordinate with other nodes. All classical attacks aimed at inter-node classical channels may be possible.

Attacks specific to quantum network system's classical channel might be possible in each of following categories (List borrowed and modified to suit from Mitrokotsa's work[22]). We do not discuss each of them in detail.

1) Confidentiality: Classical attacks including but not limited to: eavesdropping, and other privacy threats such as tracking.

2) Integrity: Since this is a channel, discussion of integrity is not applicable.

3) Availability: Any scheme that prevents classical communication between two quantum nodes will equally disrupt the quantum communication.

G. Classical node resources

A node consists of various classical computing and control elements such as microprocessors and high-precision clocks. All classical attacks that can be used against classical node resources may be possible. Also, some classical node resources are especially important to achieve qubit operation. Synchronization of the clock operating on each side of an entangled pair is such an example.

1) Confidentiality: Classical attacks include but are not limited to: eavesdropping on data, other privacy threats such as tracking, crypto attacks.

2) Integrity: Many classical attacks are possible, including but not limited to: relay attacks, replay attacks, message (re)construction, data modifications, data insertion. It is possible to disrupt integrity by tweaking the timing of clock information necessary to coordinate operations on qubits. This can disrupt both integrity and availability at the same time.

3) Availability: It is possible to disrupt availability by tweaking timing of the clock necessary to operate on qubits. This can break both integrity and availability at the same time.

VI. Conclusion

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

From the point of view of confidentiality, quantum repeater systems have great advantages. Since it is possible to detect the presence of an eavesdropper, detection of a breach of confidentiality is possible. Quantum tomography sacrifices a portion of our stream of Bell pairs as part of ongoing network monitoring operations as needed to tune certain physical parameters to optimize the fidelity of our entanglement. This process is extended to include eavesdropper detection by choosing the portion sacrificed for tomography at random. As long as tomography indicates that high fidelity is achieved on the end-to-end connection, our remaining stream of entangled qubits can be safely used without fear of breach of confidentiality if the other end point and application are secure.

From the point of view of integrity and availability, a quantum repeater system seems to be not so different from a classical network system. A repeater includes classical computing hardware and threats to both integrity and availability can target that hardware. Of course, part of the hardware is specially designed for a quantum system, but quantum system hardware is just a special kind of hardware. As we have shown in previous section, the possible attacks are very similar to classical systems.

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

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

Acknowledgments

This research has been supported by Asian Office of Aerospace Research and Development, Air Force Office of Scientific Research under grant 144051.

References

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

[2] D. Bacon and W. van Dam, "Recent progress in quantum algorithms," *Communications of the ACM*, vol. 53, no. 2, pp. 84–93, Feb. 2010.

[3] 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.

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

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

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

[7] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum Repeaters: the Role of Imperfect Local Operations in Quantum Communication," vol. 81, pp. 5932–5935, 1998.

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

[9] C.-H. Chien, R. Van Meter, and S.-Y. Kuo, "Fault-tolerant operations for universal blind quantum computation," Tech. Rep., 2013.

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

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

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

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

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

[15] D. Gottesman, T. Jennewein, and S. Croke, "Longer-Baseline Telescopes Using Quantum Repeaters," *Physical Review Letters*, vol. 109, p. 070503, Aug. 2012.

[16] T. Humphreys, "ISO/IEC 27002: 2013," *ISO Management Systems*, 2013.

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

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

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

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

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

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

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

[24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

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

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

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

[28] R. Van Meter, T. Satoh, T. D. Ladd, W. J. Munro, and K. Nemoto, "Path selection for quantum repeater networks," *Networking Science*, vol. 3, no. 1-4, pp. 82–95, Dec. 2013.

[29] S. H. Weingart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defences," in *CHES '00: Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems*. Springer-Verlag, Aug. 2000.

[30] M. M. Wilde, *Quantum information theory*. Cambridge University Press, 2013.

[31] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[32] M. Zukowski, A. Zeilinger, and M. A. Horne, ""Event-ready-detectors" Bell experiment via entanglement swapping," *Physical Review Letters*, vol. 71, no. 26, pp. 4287–4290, Dec. 1993.