AFRL-AFOSR-JP-TR-2016-0079

Security of Quantum Repeater Network Operation

Rodney Van Meter
KEIO UNIVERSITY

10/03/2016
Final Report

DISTRIBUTION A: Distribution approved for public release.

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/ IOA
Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Executive Services, Directorate (0704-0188). Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
04-10-2016	Final	29 May 2014 to 28 May 2016

4. TITLE AND SUBTITLE
Security of Quantum Repeater Network Operation

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA2386-14-1-4051

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Rodney Van Meter

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
KEIO UNIVERSITY
5322, ENDO
FUJISAWA, 252-8520 JP

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AOARD
UNIT 45002
APO AP 96338-5002

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR IOA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-JP-TR-2016-0079

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Much of the work on quantum networks, both entangled and unentangled, has been about the uses of quantum networks to enhance end-host security. The most famous such application, of course, is quantum key distribution (QKD), detecting eavesdroppers and creating shared, secret random numbers for use as encryption keys (Bennett & Brassard, 1984). Typically the study of these applications involves information-theoretic analysis of the amount of information that an attacker can glean from the use of the network.
In this project, we addressed security and quantum networks from an entirely different angle: we investigated the security of the networks themselves. We wanted to know if a single mis-behaving node, or a small number of them, can disrupt operation of the network. Our work produced a first-of-its-kind taxonomy of potential attacks on quantum repeater network operations.

15. SUBJECT TERMS
Quantum Architecture

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			SERNA, MARIO
Unclassified	Unclassified	Unclassified	SAR	5	19b. TELEPHONE NUMBER *(Include area code)* 315-227-7007

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Security of Quantum Repeater Network Operation
Final Report
2016/8/22

Rodney Van Meter
Associate Professor, Faculty of Environment and Information Studies
Keio University, Japan
+81-90-8012-3643
rdv@sfc.keio.ac.jp, rdviii@gmail.com

Abstract/Summary

Much of the work on quantum networks, both entangled and unentangled, has been about the uses of quantum networks to enhance end-host security. The most famous such application, of course, is quantum key distribution (QKD), detecting eavesdroppers and creating shared, secret random numbers for use as encryption keys (Bennett & Brassard, 1984). Typically the study of these applications involves information-theoretic analysis of the amount of information that an attacker can glean from the *use* of the network.

In this project, we addressed security and quantum networks from an entirely different angle: we investigated *the security of the networks themselves*. We wanted to know if a single mis-behaving node, or a small number of them, can disrupt operation of the network.

Our work produced a first-of-its-kind taxonomy of potential attacks on quantum repeater network operations.

Results

First, we examined the set of possible actions that an attacker can deploy against the network, enumerating differences from classical networks. Quantum networks, of course, depend upon successful creation of high-fidelity entanglement at the link level, which requires both good environmental isolation and real-time operation.

It is clear that tapping a fiber makes for an excellent denial of service attack against QKD across that link. What is less clear at the moment is to what extent

DISTRIBUTION A. Approved for public release: distribution unlimited.

larger-scale disruption of the network can be effected through either physical means (e.g., entanglement with in-progress states) or gaming of the control protocols (e.g., via manipulation of the routing protocols to increase latency, affecting real-time operation).

We created a taxonomy of possible attacks on repeater nodes, published in SENT 2015 (Suzuki & Van Meter, 2015). We modeled our taxonomy after security taxonomies for RFID tags, because both RFID tags and quantum links and nodes are sensitive to their local environment, and attacks at the physical level are of importance. We assess points of vulnerability in terms of *confidentiality*, *integrity*, and *availability*.

Our model distinguishes among *interface* qubits, which are directly coupled to an external optical channel, and *buffer* and *terminal* qubits, which reside in repeaters or end respectively and are physically isolated from the optical channel. Evidence from recent experiments has shown that interface qubits, or direct measurement of optical states arriving from the uncontrolled channel, are vulnerable to being manipulated by external parties (Jogenfors, Elhassan, Ahrens, Bourennane, & Larsson, 2015). Tests of entanglement built on *quantum tomography,* which are crucial to the proper operation of the quantum repeater network, are vulnerable to being hacked. Thus, operation of the quantum repeater network is vulnerable to *undetectable* disruption of the network operation. This is equivalent to the classical Internet silently corrupting data somewhere along a network path without the benefit of hop-by-hop error detection and correction. End-to-end checks may reveal that the entanglement has not been properly realized, but determining where along the path corruption occurred may be difficult, resulting in a disruption of network operation. Nodes may be unable to successfully reroute traffic, leaving them completely unable to communicate. This represents a new type of vulnerability in network operation, compared to classical networks.

This leads us to the following security recommendation: **Security of network operation appears to require that tests of entanglement be done *only* once data has been moved to qubits physically isolated from the external channel (e.g., done only terminal or buffer qubits).** Thus, our recommendation is that specifications for nodes intended to form a future Quantum Internet be *required* to support two classes of physically distinct qubits inside the

DISTRIBUTION A. Approved for public release: distribution unlimited.

system, in order to allow secure quantum tomography and maintain high availability for the Quantum Internet.

Future Work and Industry Impact

This work has primarily focused on the attacks possible on individual nodes. We look forward to conducting additional work on understanding the behavior of networks, and whether the proportion of network traffic that can be undermined scales more readily in quantum networks than in classical networks.

Our presentation at the SENT workshop attracted the attention of computer and network researchers from Cisco Systems. Over the last eighteen months, we have had continuing conversations with Cisco about the future of quantum repeater networks and the security. Cisco has expressed interest in funding additional work in this area.

References

Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing* (pp. 175-179). IEEE.

Jogenfors, J., Elhassan, A. M., Ahrens, J., Bourennane, M., & Larsson, J. (2015). Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution. *Science Advances , 1* (11).

Suzuki, S., & Van Meter, R. (2015). Classification of Quantum Repeater Attacks. *Security of Emerging Network Technologies.* San Diego.

DISTRIBUTION A. Approved for public release: distribution unlimited.