The Network Impact of Hijacking a Quantum Repeater

Takahiko Satoh†, Shota Nagayama‡, Takafumi Oka† and Rodney Van Meter†
Keio University†, Mercari, Inc.‡, {satoh, kurosagi, takafumi, rdv}@sfc.wide.ad.jp
http://aqua.sfc.wide.ad.jp/

arXiv:1701.04587

A single hijacked quantum repeater can frame innocent repeaters and bring down an entire network, unless protocols are designed to be secure

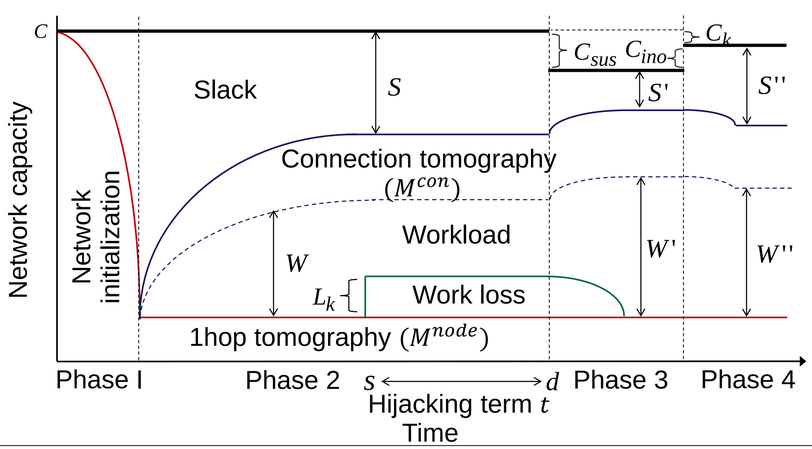
1. Overall purpose and Goal

Project Goal

Simulating a reliable large-scale complex Quantum Internet, in order to assess its robustness and its practicality, and to establish key design decisions to build a long-lived network.

Subproject Goal

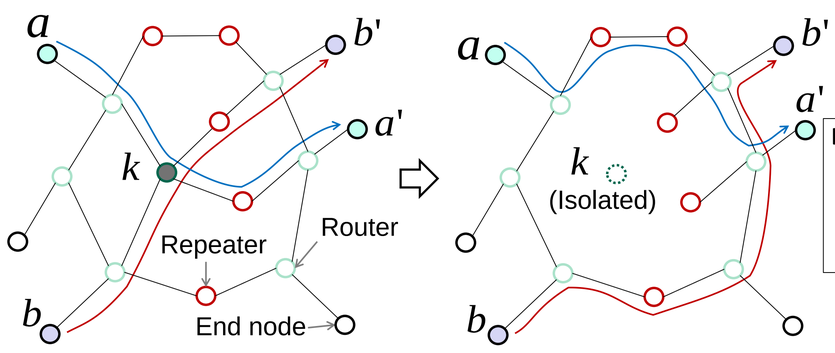
To investigate the network impact of hijacking a quantum repeater, we evaluate the unavoidable operating costs and network slack "*S*" in each phase.
Phase 1: Network launching. **Phase 2: Normal operation.**
Phase 3: After repeater hijacking detection. **Phase 4: Return of innocent repeaters.**



2. The impact of repeater hijacking

Increase communication cost due to isolation of hijacked repeater

We assume a quantum repeater network with several active connections.
When the network detects repeater hijacking, the corresponding repeater (k) is isolated from the network and connections adopt newly recalculated shortest paths [1].



Links denote optical fiber and nodes denote quantum repeaters serving as Routers (Hub node), Repeaters (connected to two nodes), and End Nodes.

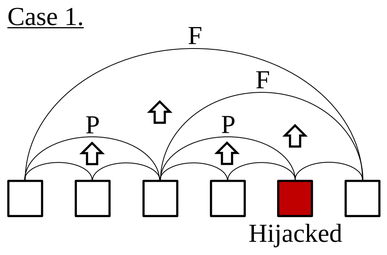
Connections via k
$a \longrightarrow a'$: 5hop communication
$b \longrightarrow b'$: 5hop communication

Rerouted connections
$a \longrightarrow a'$: 6hop communication
$b \longrightarrow b'$: 6hop communication

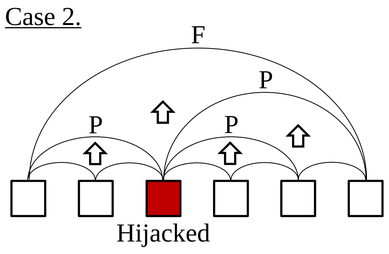
Identification of hijacking repeater

When the hijacked repeater always acts maliciously on every connection, the administrator can identify that repeater by using the combination of reported tomography results [2].
(Related poster: "A Classical Network Protocol to Support Distributed Quantum State Tomography")
In contrast, when the hijacked repeater targets only the connection between two specific repeaters, whether administrator can identify or not depends on the repeater models.

Case 1.

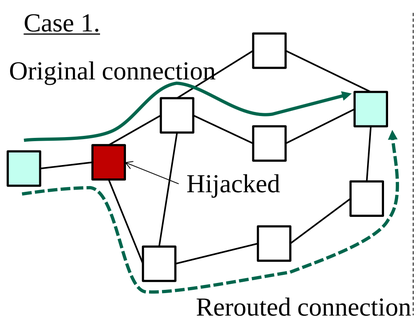


Case 2.

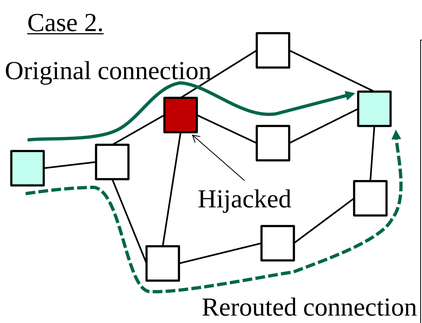


In the ES model, repeaters perform entanglement swapping in a nested tree to share final Bell pairs for communication. If we perform cryptographically secure tomography along with every ES operation, we can finger the culprit repeater

Case 1.



Case 2.



In the QEC model, we can detect the repeater hijacking using end to end tomography but our ability to correctly identify the hijacked repeater is weak.
The information of hijacking detection narrow down the candidates. The rapid sharing of these information entire network is important.

3. Network operation

We classify the phases of network operation as follows.

Phase 1. Network bootstrapping

At the start of network operations, we need to initialize network components.
To check the condition of quantum repeaters and links, some types of tomography are utilized.
Almost the entire capacity of the network is spent to execute these operations, so that quantum communications for users are not yet provided.

Phase 2. Normal operation

In normal operations, the network performs quantum communications for end node applications and various tomography operations for the maintenance of the network. The network slack prevents instability of connections and requires us to minimize possible maintenance costs. This phase is the main portion of network operations and continues until the detection of repeater hijacking.

Phase 3. After repeater hijacking detection

The amount of useful workload lost depends on our lag in detecting the start of hijacking, which in turn depends on the frequency of tomography. The network performs rerouting operations and isolates all suspected repeaters. Reduced network performance and increased communication costs shrink the slack.

Phase 4. Return of innocent repeaters

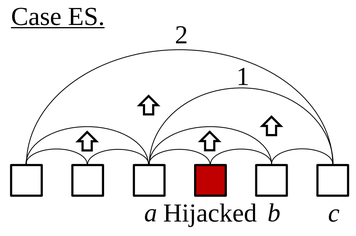
By careful verification, if the administrator identifies the actual hijacked repeater, he returns all isolated innocent repeaters to the network.
After these operations, the network is reset to a new steady-state equilibrium, giving us a new Phase 2.

4. Framing innocent repeaters

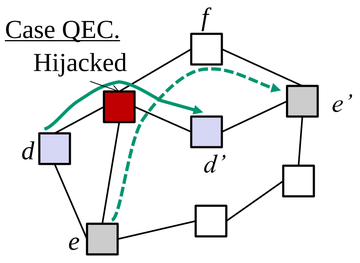
Framing an innocent repeater

If the hijacker can identify Bell pairs that will be used for hijack detection, the hijacker can frame another, innocent repeater in one of two ways:
First, when it is the endpoint of a Bell pair, it can directly falsify measurement results, causing the failure of the entanglement checks that test for the presence of a hijacker, in which case the last node to perform entanglement swapping will be blamed.
Second, if it knows the sequence of tests performed by the other nodes after entanglement swapping, it can selectively choose which Bell pairs to corrupt.

Case ES.



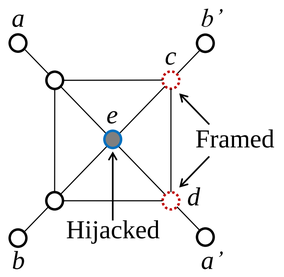
Case QEC.

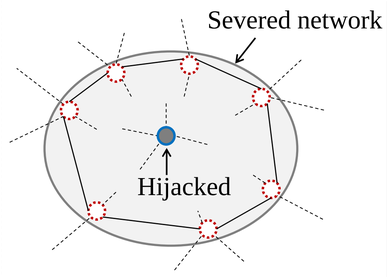


In a path of repeaters in an ES network, the hijacker can frame repeaters a and b in several ways.
In QEC a network, the hijacker can frame by attacking a specific connection.

Possibility of bringing down the network

When the attack is detected, the network administrator will isolate suspect repeaters from the network.
Depending on the network structure, framing several chosen repeaters can bring down the network.





In the left case, framing of repeaters c and d by hijacked repeater e prevents the communications between $a - a'$ and $b - b'$. Then, the exact framing can bring down a network of a particular topology.
In the right case, the hijacked repeater severs the network surrounded by a circle using framing. After framing the seven repeaters, nodes inside the circle will be unable to communicate with those outside the circle.

5. Workload shedding

Definition of variables to calculate the network slack

W	Total number of attempts of the entire network to share Bell pairs for teleportation per sec.
W''	Workload including rerouting penalty.
S, S''	The slack of network at each time point.
C	Total network capacity, in Bell pairs per sec.
R	Maintenance rate, in Bell pairs per sec.
L	Amount of work loss from isolation.
P	Rerouting penalty from the change of network topology.

Always during network operation, workload needs to be smaller than network slack to prevent workload shedding [3] occurrence. For example, we show workload and slack at Phase 4.

$$S'' = (C - C_k) - W'' - (R - R_k)$$
$$W'' = W - L + P$$

We showed the detail of those quantitative discussion in arXiv:1701.04587

References

[1] Rodney Van Meter, Takahiko Satoh, Thaddeus D. Ladd, William J. Munro, and Kae Nemoto. Path selection for quantum repeater networks. Networking Science, 3(1):82–95, 2013.
[2] Takafumi Oka, Takahiko Satoh, and Rodney Van Meter. A classical network protocol to support distributed quantum state tomography. In Proc. Quantum Communications and Information Technology, 2016.
[3] L. Kleinrock. Queueing systems. volume I, Theory. New York: Wiley, 1974.

Acknowledgement

- **This work was supported by the Air Force Office of Scientific Research under award number FA2386-16-1-4096.**

INTERNATIONAL CONFERENCE ON CHALLENGES IN QUANTUM INFORMATION SCIENCE, APRIL 9–11, 2018