Attacking the Quantum Internet

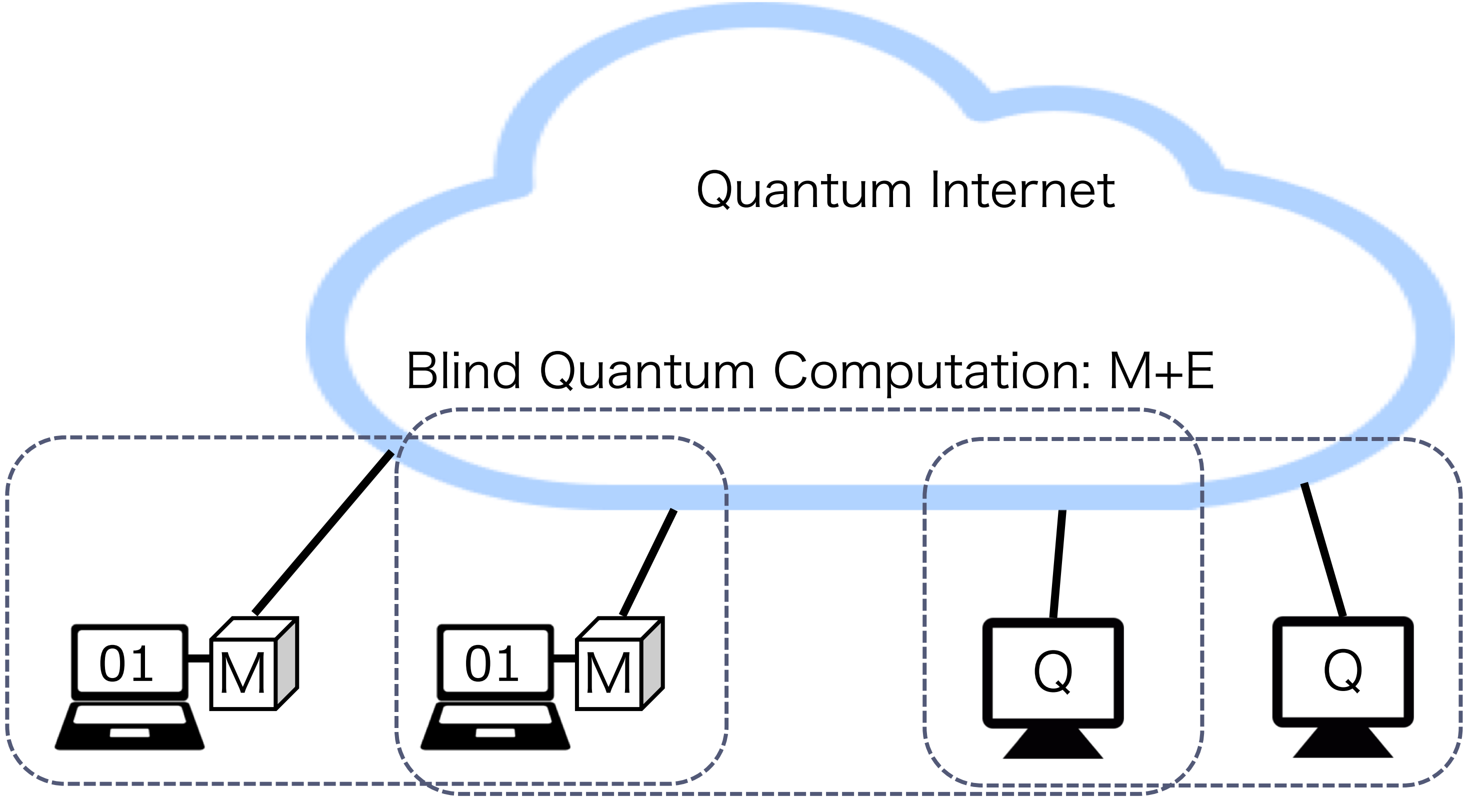
arxiv:2005.04617

Takahiko Satoh (Keio University), Shota Nagayama (Mercari, Inc.)

Shigeya Suzuki (KU), Takaaki Matsuo (Softbank), Rodney Van Meter (KU)

- Multi QDDOS
- Summary
- Education

Quantum Internet Application



Quantum Internet

Blind Quantum Computation: M+E

Fast byzantine agreement: M+M

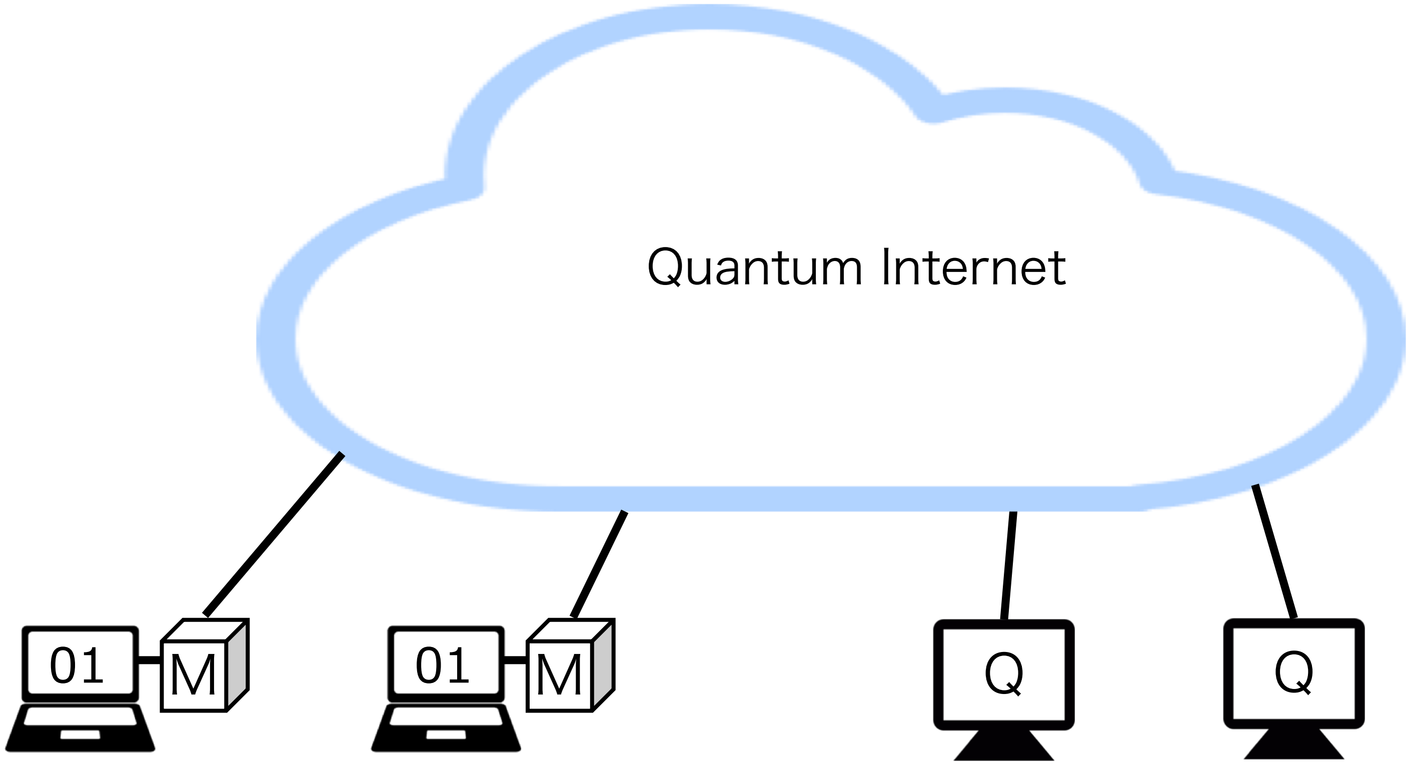
Distributed Quantum Computation: E+E

Classical computer with measurement device (MNode)

Quantum End node (ENode)

Attacking the Quantum Internet

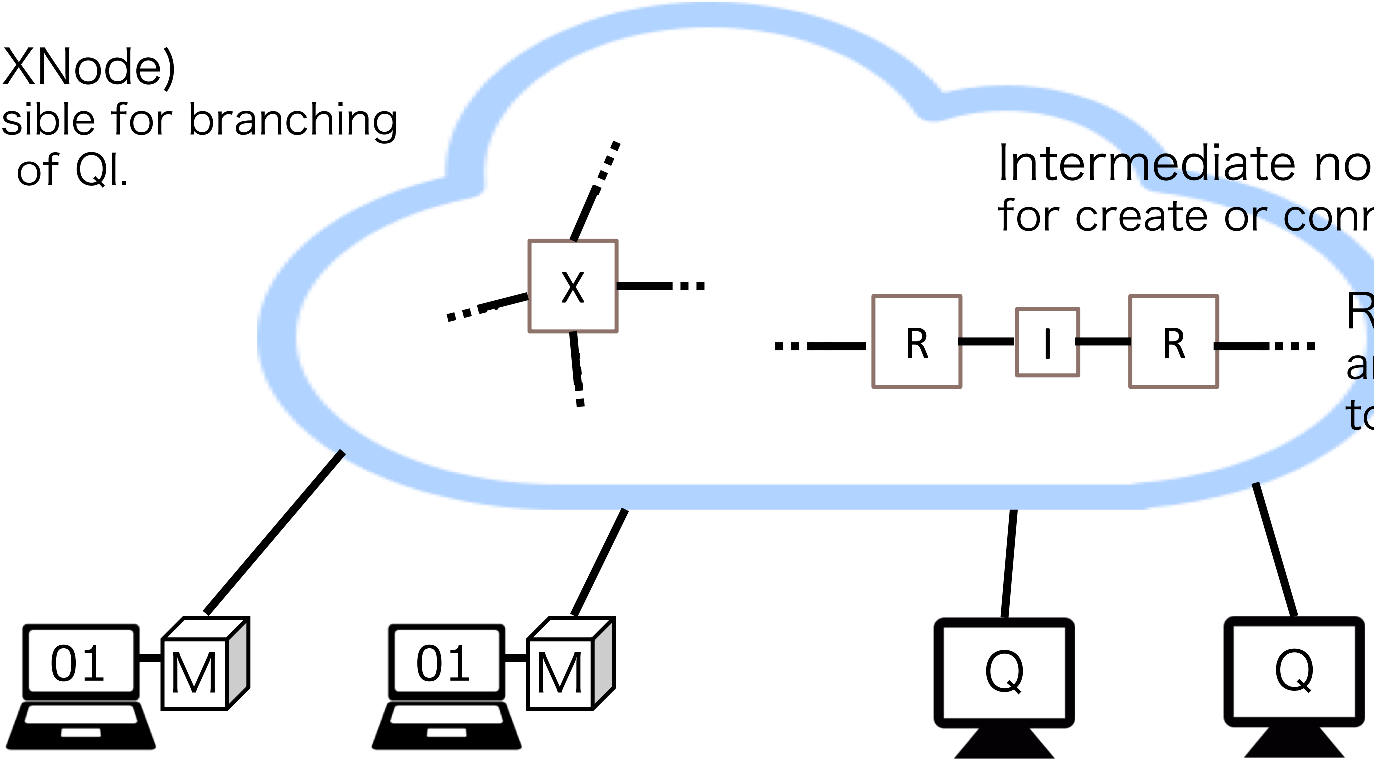
1. How can attackers attack elements of the Quantum Internet?
2. What attacker(s) can do if they successfully hijack full control of Quantum Node(s)?



Classical computer with measurement device (MNode)

End node Quantum computer (ENode)

Quantum Internet nodes (QNodes)



Router (XNode)
is responsible for branching
the route of QI.

Intermediate node (INode)
for create or connect Bell pairs.

Repeater (RNode)
are installed at fixed distances
to improve network performance.

Classical computer with
measurement device (MNode)

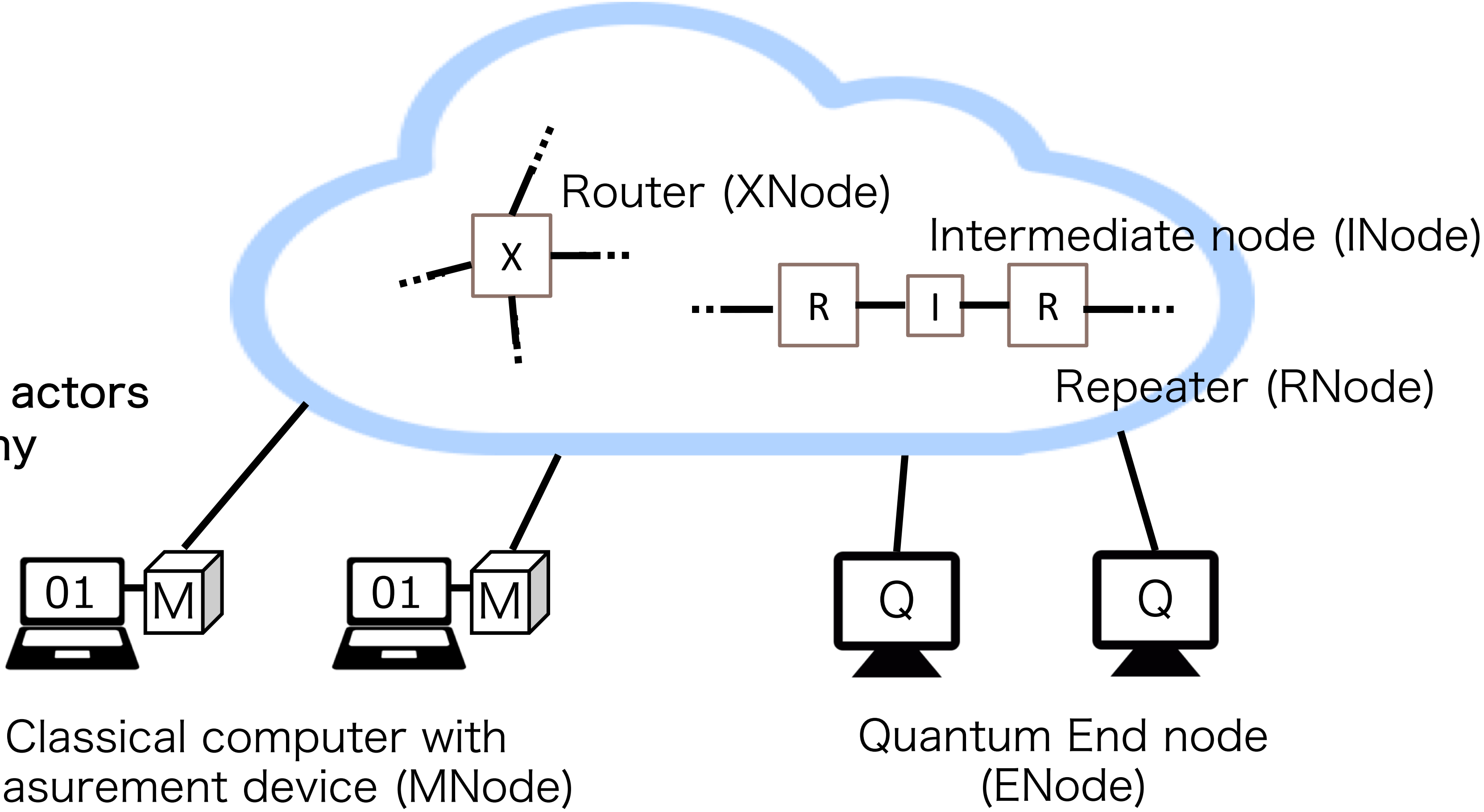
Quantum End node
(ENode)

Management of Quantum Internet

Crucial points

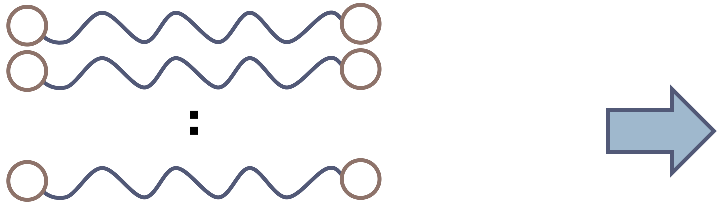
- Topology (out of scope)
- Routing (out of scope)
- **Tomography**
- **The presence of malicious actors**

=> Quantum state tomography


Router (XNode)
X
Intermediate node (INode)
R
I
R
Repeater (RNode)
01
M
01
M
Q
Q
Classical computer with measurement device (MNode)
Quantum End node (ENode)

Quantum state tomography

- By consuming a large number of copies, we can estimate the quantum state.

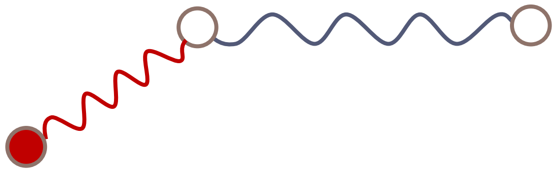


We cannot know actual states $\hat{\rho}_{actual}$.

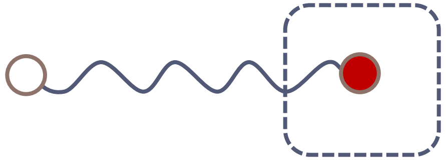
By tomography, we can find $\hat{\rho}_{estimated}$!

Application examples:

1. We can monitor the optical fiber status between QNodes.
2. We can detect a **rogue quantum manipulation**.



Creating illegal entanglements.

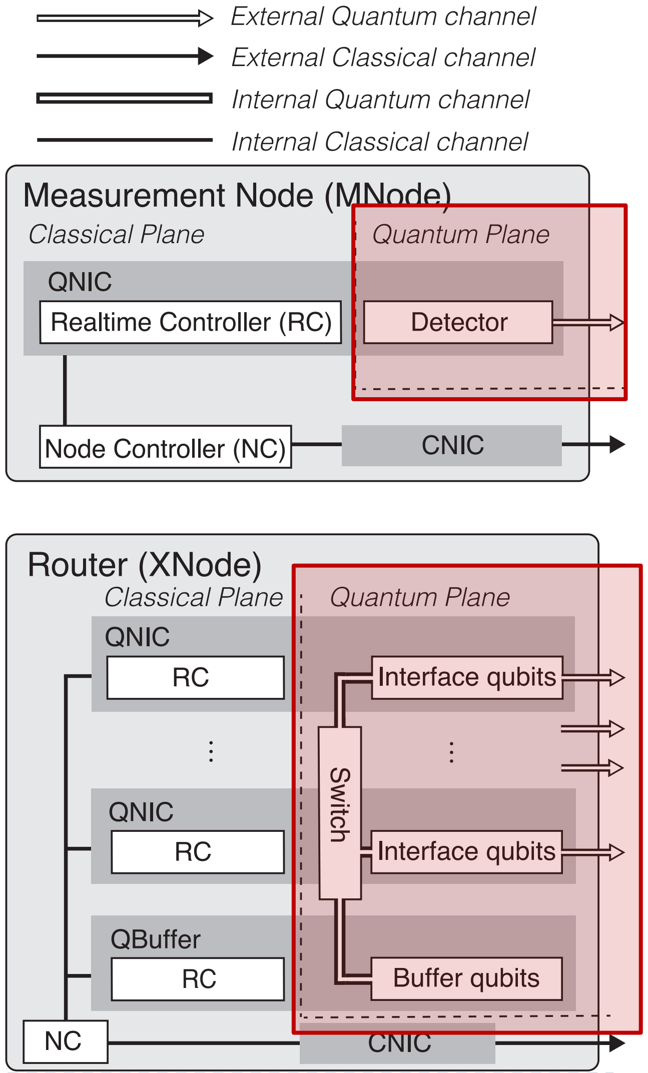


Illegal modification

Primitive attacks on QNodes

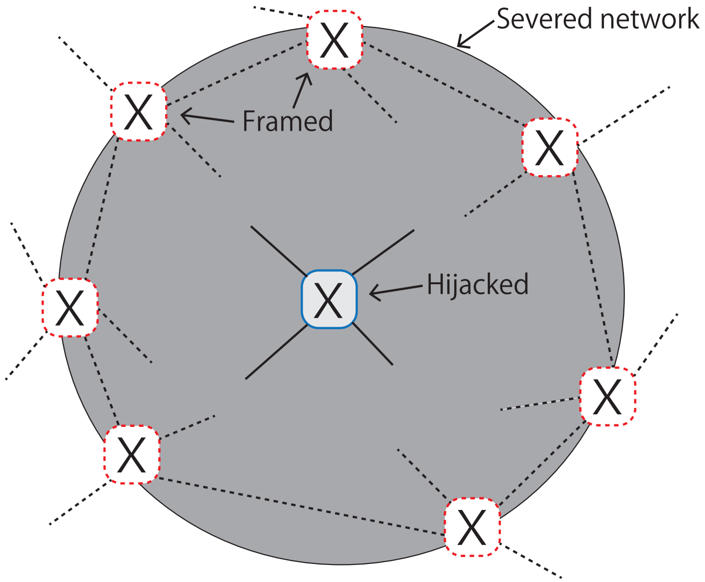
- We introduced the elemental classification planes.
  - Classical Plane
    - Realtime controller, Classical channel to Internet and more…
    - Not much different from an attack on *classical* Internet device.
  - Quantum Plane
    - Qubits, Detector, Quantum channel and more…
    - Since Qubit **cannot be copied**, proper tomography keep confidentiality.
      - ✓ No-cloning theorem.
    - Integrity and availability: QNodes may not be much different from classical network systems.
  - Composite attack violates the confidentiality of quantum plane.
    - Ex. Qubit theft + eavesdropping on classical channel

QNodes internal structures



Attacks using hijacked QNode

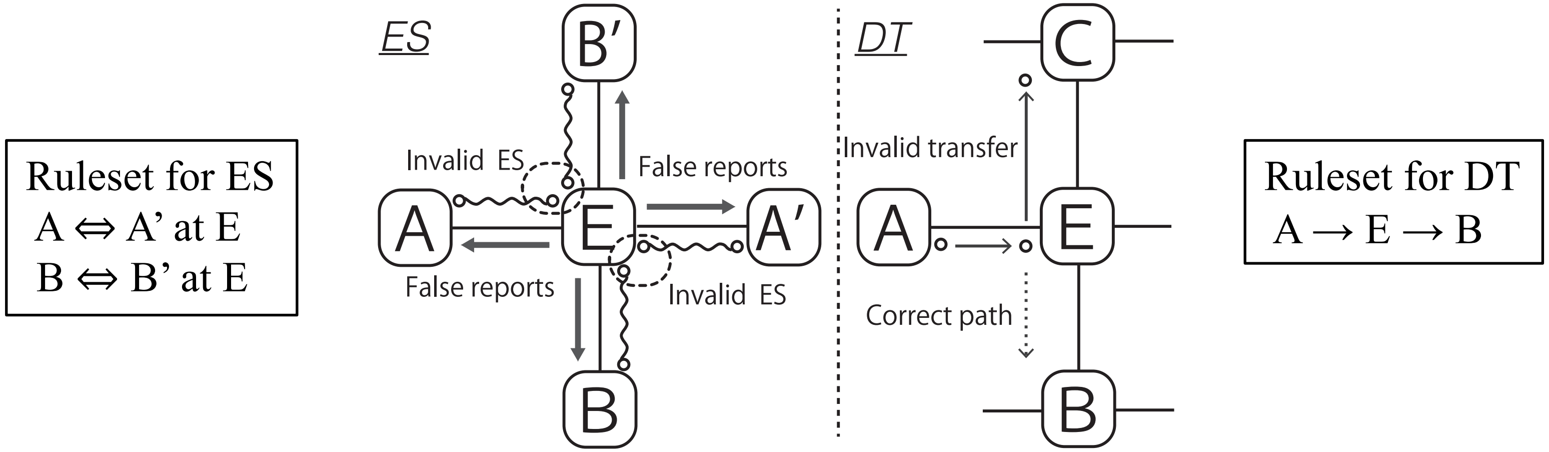
- Framing innocent Qnodes [TS, SN, T.Oka, RDV (QST 2018), arXiv:1701.04587]
  - A malicious router can "frame" other repeaters or routers by subverting tomography.
  - Prompt verification and response to tomography results is important.



A network partitioned by the isolation of innocent QNodes.

Attacks using hijacked QNode

- Switching disruptions by a malicious router node
  - Entanglement Swapping and transfers without following pre-shared rulesets.
    - ✓ Ruleset [TM, Clément Durand, RDV (PRA 2019), arXiv: 1904.08605]
  - The impact of packet loss is greater than classical Internet.
    - ✓ We cannot copy quantum states.



Ruleset for ES
A ⇔ A’ at E
B ⇔ B’ at E

Ruleset for DT
A → E → B

Monitoring entanglement swapping (ES) is important.
The impact of packet loss is more severe in direct transfer (DT) than in ES.

Attacks using multiple hijacked QNodes

- QDDoS: the DDoS in the Quantum Internet
  - The possible attack methods for cooperating malicious ENodes and MNodes.
  - More serious QDDoS (QDoS) by future improved bandwidth quantum computer (ENode).
  - A system down due to (classical) DDoS to the classical plane may cause irreparable damage to the quantum state.

- Framing using multiple hijacked QNodes
  - False reports from multiple QNodes could more easily fool the network.

Summary

- We provide the first attempt to summarize the safety of the quantum repeater architecture.
  - Based on current knowledge, by referring to proposed classical system taxonomies.

- Quantum tomography is a key technology for detecting the presence of attacker.

- The confidentiality of the quantum state is difficult to violate by *only* quantum plane attacking.
- From the point of view of integrity and availability,

  a quantum repeater system seems to be not so different from a classical network system.
- 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.

- This work represents **only** the first step in assessing the security of quantum networks.

Education