Architectural Principles of a Quantum Internet

https://datatracker.ietf.org/doc/draft-irtf-qirg-principles/

QIRG Singapore 19 November 2019

Wojciech Kozlowski
Stephanie Wehner
Rodney Van Meter
Bruno Rijsman

Recap

- First version of draft prepared and presented at IETF 104 in Prague on 26 March
- Main motivation is to address charter point:

  An architectural framework delineating network node roles and definitions, to build a common vocabulary and serve as the first step toward a quantum network architecture.
- Also want to create a good starting point for people with no quantum background

Recap

- Draft was adopted by QIRG at the meeting
- Received lots of comments after the meeting by email - mostly editorial and open-ended questions
- Had 4 web calls across Sep/Oct/Nov to discuss draft contents – better feedback loop and more changes introduced (side-note: Jitsi Meet is great)

GitHub

- A GitHub repo is maintained at https://github.com/Wojtek242/draft-irtf-qirg-principles
- A more convenient way to share updates at a finer granularity than datatracker allows
- However, all discussions are still done on the mailing list so no fancy CI/CD

Overview of changes

- Three new authors: Stephanie Wehner, Rodney Van Meter, Bruno Rijsman
- Multiple small editorial changes
- Update to security section
- Reworked sections 4 and 5 to better address readers with a networking background, but no quantum background

Pipeline

- Not all contributions are reflected in draft yet
- Still need to work through:
  - Remaining RDV comments from https://mailarchive.ietf.org/arch/msg/qirg/z4-e6t11iVvJAMRDyjSwr5BPLyo
  - Subsection on link generation from Angela Sara Cacciapuoti, Marcello Caleffi
  - Pull request from Patrick Gelard about encodings

Major updates

- Security in quantum networks
- Section 4: life cycle of entanglement – how is it created, used, delivered
- Section 5: relation to classical networks, dual quantum/classical data plane

Security

- User data does not enter the network, but the delivered pairs are used for user data
- Furthermore, fidelity < 1 means information has leaked (possibly to malicious party)
- However, a quantum network must only match the theoretical models of quantum crypto – it does not have to provide these guarantees itself
- Applications do E2E security by using quantum channels in conjunction with classical channels

Security

- However, security of network against network level threats not considered at all yet
- No consideration for attacks such as DoS
- Likely to piggy-back on classical solutions
- Is it worth looking into and addressing in draft?

Life cycle of entanglement (sec. 4)

- Re-written to clarify the process of creating, distributing, and delivering entanglement
- Changes based on discussion on mailing list and web calls (see minutes published on mailing list and datatracker)

Life cycle of entanglement (sec. 4)

- Challenges
  - Measurement problem
  - No-cloning theorem
  - Fidelity
- Makes direct transmission difficult
- Instead distribute Bell pairs using entanglement swaps
- Bell pairs enable quantum teleportation

Life cycle of entanglement (sec. 4)

- Link generation to create Bell pairs on links
- Entanglement swaps to combine Bell pairs
- Deliver two qubits to the two end-points
  - Pauli corrections
  - Bell pair identifier
  - Fidelity estimate

Life cycle of entanglement (sec. 4)

```
+---------+      +---------+      +---------+
|    A    |      |    B    |      |    C    |
|         |------|         |------|         |
|      X1~~~~~~~~~~~X2   Y1~~~~~~~~~~~Y2     |
+---------+      +---------+      +---------+
```

```
+---------+      +---------+      +---------+
|    A    |      |    B    |      |    C    |
|         |------|         |------|         |
|      X1~~~~~~~~~~~~~~~~~~~~~~~~~~~~X2     |
+---------+      +---------+      +---------+
```

Network model (sec. 5)

- Re-written to clarify the challenges involved and the key differences to the classical Internet
- Changes based on discussion on mailing list and web calls (see minutes published on mailing list and datatracker)

Network model (sec. 5)

- New challenges
  - There is no quantum equivalent of a payload carrying network packet
  - An entangled pair is only useful if the locations of both qubits are known
  - Generating entanglement requires temporary state
  - Generating end-to-end entanglement is a parallelisable operation

Network model (sec. 5)

- Classical communication is necessary
  - To communicate classical bits of information as part of distributed protocols such as entanglement swapping and teleportation
  - To communicate control information within a network – e.g. routing and signalling protocols to set up end-to-end entanglement generation

Network model (sec. 5)

- Elements of a quantum network
  - Quantum repeaters
    - Automated and controllable quantum nodes
  - Quantum routers
    - Controllable quantum nodes
  - End-nodes
  - Non-quantum nodes
  - Quantum links
  - Classical links

Network model (sec. 5)

```
+------+                                        +------+
| App  |...................CC...................| App  |
+------+                                        +------+
   ||                                              ||
+------+                +------+                +------+
|      |.......CC.......|      |.......CC.......|      |
|  EN  |.......QC.......|  QR  |.......QC.......|  EN  |
|      |-------PL-------|      |-------PL-------|      |
+------+                +------+                +------+


  App - user-level application
  QR - quantum repeater
  EN - end-node
  QC - logical quantum channel
  CC - logical classical channel
  PL - physical link (CC and QC might share or use separate).
```

Looking forward

- Finalise updates to sections 4 and 5 based on last call from 11 Nov
- Incorporate pipelined changes

Looking forward

- Physical constraints that have implications on architecture (communication qubits, memory lifetimes, etc.)
- Goals of a quantum internet
- Principles for a quantum internet
- Network-level security?