Security for Quantum Networks

Salini Karuvade and Barry C. Sanders
salini.karuvade@ucalgary.ca

Institute for QUANTUM SCIENCE AND TECHNOLOGY at the University of Calgary

UNIVERSITY OF CALGARY

Context

- Quantum networks enhance information and communications technology.
- Reliable and efficient network-communication depends on identifying and mitigating security risks such as unauthorised access or data corruption.
- Security mechanisms as a part of the communication protocols need to be incorporated at the network development stage itself.

Motivation and Aim

Absence of a realistic security framework renders a quantum network vulnerable to attacks and affects its reliability and efficiency [1].

Potential security threats pertaining to various quantum networks proposed in the literature:

Network	Threat	Security Mechanism
Quantum Key Distribution	Network congestion due to unauthorised access	User authentication
Clock synchronisation	Data corruption	Message authentication
Distributed quantum computing	Eavesdropping	Encryption

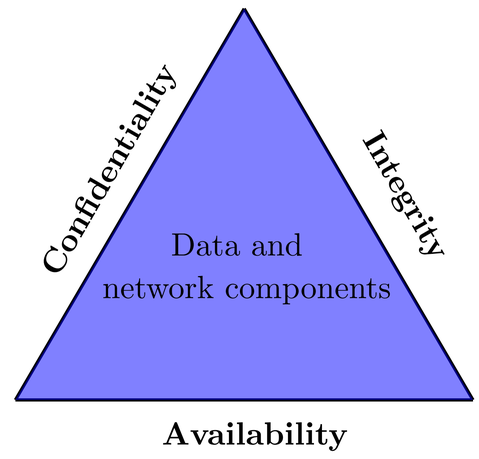
Aim: Construct a framework for developing and assessing secure quantum networks by building on security practices used in classical layered network architectures.

Quantum Network Architecture: State of the art

- Quantum key distribution networks are generally developed as overlay networks built on top of an existing classical network such as the internet [2].
- Quantum networks capable of end-to-end transmission of quantum states generally rely on teleportation using shared entanglement to transmit quantum information [3].
- Layered architecture for teleportation-based networks is introduced in [4].

Classical network security

Set of practices built into network communication protocols for protecting data from unauthorised access and modification, and facilitating authorised access of network-services [5].



Information security practices can be formulated following the CIA triad model.

Security for Layered Quantum Networks

Weak Quantum Network: Capable of direct transmission of quantum states without generating entanglement within the network.
Applications: Quantum key distribution based on BB84 protocol, two-party quantum cryptography, cloud-based quantum computing.

Strong Quantum Network: Teleportation-based quantum network capable of generating entanglement within the network.
Applications: Quantum key distribution, distributed quantum computing, sensing.

Dividing a quantum network into abstraction layers based on its functionality and identifying security threats pertaining to each layer:

Layer	Functions in weak quantum network	Modified/added functions in strong quantum network	Security threats
Application layer	Generate quantum data for transmission Manipulate quantum data received Measure quantum states	Assign address to application qubits	Unauthorised service requests Malicious entanglement
Transport layer	Support end-to-end delivery of quantum data Support end-to-end cryptographic protocols Key management	Support end-to-end quantum teleportation Assign address to terminal qubits	Session hijacking Man-in-the-middle attacks
Network layer	Routing Assign address to devices in a network	Generate end-to-end entanglement	Switching disruption Corrupting routing table Network sniffing
Link layer	Controlling physical transmission of quantum data Support point-to-point cryptographic protocols Perform quantum demolition measurement of quantum states to ensure data delivery	Ensure reliable point-to-point entanglement generation Assign address to qubits involved in point-to-point entanglement	Unauthorised entanglement-generation requests Malicious entanglement
Physical layer	Point-to-point delivery of quantum states	Generate point-to-point entanglement	Fault-injections Blinding of detectors

Security framework

Road to establishing a comprehensive framework for quantum-network security:

1. **Augmenting:** Construct a model describing the functions and structure of a general quantum network by augmenting the capabilities of a classical telecommunication network to support quantum communication.
2. **Layering:** Construct a layered architecture for the general quantum network based on a classical network reference model such as the OSI model.
3. **Formulating security objectives:** Identify the security threats to the data communicated by each layer, contextualised by the CIA triad model.
4. **Securing communication:** Construct secure communication protocols that carry out the network functions specific to each abstraction layer. The protocols incorporate necessary quantum or post-quantum cryptography, depending on the type of data communicated, to achieve the network security objectives.

References:

[1] Satoh T, Nagayama S, Suzuki S, Matsuo T, Van Meter R 2020 *arXiv:2005.04617v1*
[2] Dianati M 2008 *Security Comm. Networks.* **1** 1.
[3] Van Meter R 2012 *IEEE Netw.* **26** 4.
[4] Dahlberg A et al. 2019 *Proc. ACM Spec. Interest Group Data Commun.* 159–17.
[5] Tannenbaum AS 2003 *Computer Networks* Fourth (Pearson, Upper Saddle River, N.J.)

Alberta