CREATE
CONNECT
LIVE
inspire

Introduction to IRTF Study on Applications and Use Cases for the Quantum Internet

Chonggang Wang, Principal Engineer/IEEE Fellow
InterDigital, USA

May 26, 2021

interdigital

IRTF Quantum Internet Research Group (QIRG)

- **IETF:** Internet Engineering Task Force
- **IRTF:** Internet Research Task Force

- **The IETF is an SDO, while the IRTF is the research wing of the IETF**

- **Our draft on "Applications and Use Cases for the Quantum Internet" is an output of the IRTF**

IRTF Quantum Internet Research Group (QIRG)

CHAIRS

The QIRG is chaired by Rod van Meter and Wojciech Kozlowski.

MAILING LIST

The QIRG mailing list is qirg@irtf.org. To subscribe or access the list archives, visit the mailman page.

DATATRACKER

Documents and meeting materials for the QIRG can be found on the IETF datatracker.

TIMELINE

The QIRG was chartered on 2018-09-19.

- Overall the goal of the QIRG is to address the question of how to design and build quantum networks. Some of the problems that need to be addressed include: Routing, Resource Allocation, Connection Establishment, Interoperability, Security, API Design, Applications for a Quantum Internet, etc.

Quantum Internet Research Group (qirg)

About | Documents | Meetings | History | Photos | Email expansions | List archive »

Document	Date	Status
Active Internet-Drafts (2 hits)		
draft-irtf-qirg-principles-06 **Architectural Principles for a Quantum Internet**	2021-02-19 38 pages	I-D Exists IRTF stream
draft-irtf-qirg-quantum-internet-use-cases-06 **Applications and Use Cases for the Quantum Internet**	2021-05-03 28 pages	New I-D Exists IRTF stream

interdigital

Applications and Use Cases for the Quantum Internet

- **Quantum Internet Applications**
  - Classification by Application Usage
    - Quantum Cryptography Applications
    - Quantum Sensor Applications
    - Quantum Computing Applications
  - Control vs Data Plane Classification
- **Selected Quantum Internet Use Cases**
  - Secure Communication Setup
  - Secure Quantum Computing with Privacy Preservation
  - Distributed Quantum Computing

draft-irtf-qirg-quantum-internet-use-cases-06

Credits to Co-Editors and QIRG:

Chonggang Wang (InterDigital, USA)
Akbar Rahman (InterDigital, Canada)
Ruidong Li (Kanazawa University, Japan)
Melchior Aelmans (Juniper Networks, The Netherlands)

Classification by Application Usage

- **Quantum Cryptography Applications**
  - Refers to the use of quantum information technology for cryptographic tasks such as quantum key distribution.
- **Quantum Computing Applications**
  - Refers to the use of quantum information technology for supporting remote quantum computing facilities (e.g., distributed quantum computing).
- **Quantum Sensors Applications**
  - Refers to the use of quantum information technology for supporting distributed sensors (e.g., clock synchronization).

Quantum Cryptography Applications

- **Secure Communication Setup**
  - Refers to secure cryptographic key distribution between two or more end-nodes.
- **Fast Byzantine Negotiation**
  - Refers to a quantum-based method for fast agreement in Byzantine negotiations, for example, to reduce the number of expected communication rounds and in turn achieve faster agreement, in contrast to classical Byzantine negotiations.

Quantum Computing Applications

- **Distributed Quantum Computing**
  - Refers to a collection of remote small capacity quantum computers (i.e., each supporting a relatively small number of qubits) that are connected and working together in a coordinated fashion so as to simulate a virtual large capacity quantum computer.
- **Secure Quantum Computing with Privacy Preservation**
  - Refers to private, or blind, quantum computation, which provides a way for a client to delegate a computation task to one or more remote quantum computers without disclosing the source data to be computed over.

Quantum Sensors Applications

- **Network Clock Synchronization**
  - Refers to a world-wide set of atomic clocks connected by the Quantum Internet to achieve an ultra precise clock signal with fundamental precision limits set by quantum theory.
- **High Sensitivity Sensing**
  - Refers to applications that leverage quantum phenomena to achieve reliable nanoscale sensing of physical magnitudes. For example, an entangled quantum network can be used for measuring the average phase shift among multiple distributed nodes, to achieve high-sensitivity and distributed quantum sensing.

Control Plane and Data Plane Classification

	Classical Internet Examples	Quantum Internet Examples	Hybrid Internet Examples
Control Plane	ICMP; DNS	Quantum ping; Signalling for controlling entanglement distribution;	QKD-based secure communication setup
Data Plane	Video conference	QKD; Entanglement distribution	Video conference using QKD-based secure communication setup

interdigital

Secure Quantum Computing with Privacy Preservation

```
+----------------+      /--------\      +----------------+
|                |--->( Quantum  )--->|                |
|                |    ( Internet )    |    Remote      |
|   Terminal     |     \--------/     |    Computation |
|   Node         |                    |    Node        |
|  (e.g., Home   |      /--------\    |    (e.g., QC   |
|   Gateway)     |    ( Classical)    |    in Cloud)   |
|                |<-->( Internet )<-->|                |
+----------------+     \--------/     +----------------+
```

- A client node with source data delegates the computation of the source data to a remote computation node (i.e., a server).
- Furthermore, the client node does not want to disclose any source data to the remote computation node and thus preserve the source data privacy.
- Note that there is no assumption or guarantee that the remote computation node is a trusted entity from the source data privacy perspective.

Distributed Quantum Computing

- **Scientists can leverage connected NISQ computers to solve highly complex scientific computation problems such as analysis of chemical interactions for medical drug development**
  - In this case, qubits will be transmitted among connected quantum computers via quantum channels, while classic control messages will be transmitted among them via classical channels for coordination and control purpose.

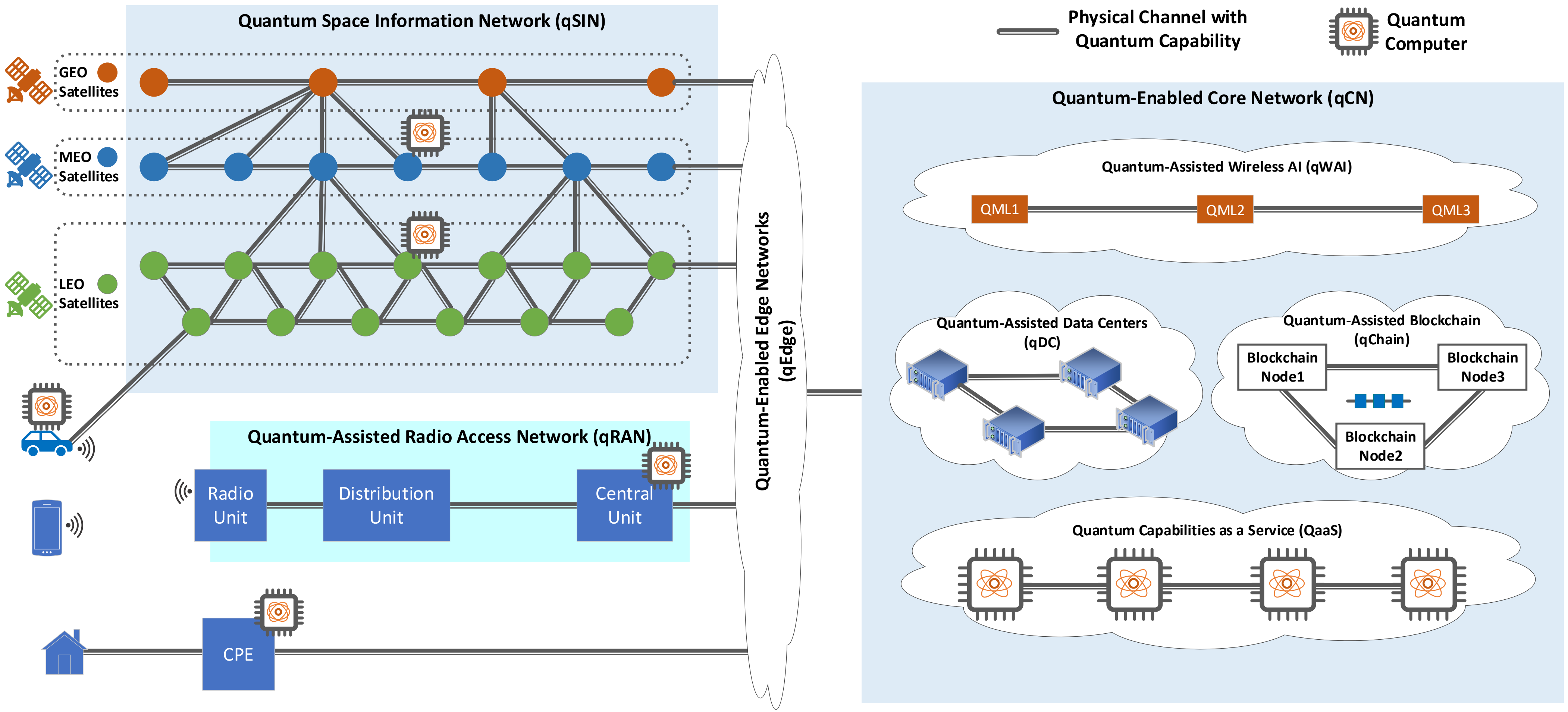
- **Another example of distributed quantum computing is secure Multi-Party Quantum Computation (MPQC), which can be regarded as a quantum version of classical secure Multi-Party Computing (MPC).**
  - In secure MPQC, multiple participants jointly perform quantum computation on a set of input quantum states, which are prepared and provided by different participants.
  - One of primary aims of secure MPQC is to guarantee that each participant will not know input quantum states provided by other participants. Secure MPQC relies on verifiable quantum secret sharing.

```
                         +-----------------+
                         |     End-User    |
                         |(e.g., Scientist)|
                         +-----------------+
                                  ^
                                  |User Interface (e.g. GUI)
                                  |
            +---------------------+---------------------+
            |                                           |
            |                                           |
            V                                           V
+-----------------+     /--------\     +-----------------+
|                 |--->( Quantum  )--->|                 |
|                 |    ( Internet )    |                 |
|    Quantum      |     \--------/     |    Quantum      |
|    Computer A   |                    |    Computer B   |
| (e.g., Site #1) |     /--------\     | (e.g., Site #2) |
|                 |    ( Classical)    |                 |
|                 |<-->( Internet )<-->|                 |
+-----------------+     \--------/     +-----------------+
```

Requirements from Quantum Internet Use Cases

- Methods for **facilitating quantum applications to interact efficiently with entanglement qubits** are necessary in order for them to trigger distribution of designated entangled qubits to potentially any other quantum node residing in the Quantum Internet.
- **Quantum repeaters/routers** should support robust and efficient entanglement distribution in order to extend and establish entanglement connection between two quantum nodes.
- Quantum end-nodes must **send additional information on classical channels** to aid in transmission of qubits across quantum repeaters/receivers.
- Methods for **managing and controlling the Quantum Internet** including quantum nodes and their quantum resources are necessary.

Quantum-Enabled 6G System



Quantum-Enabled 6G System

Features	Leverage Quantum Communication	Leverage Quantum Computing	Leverage Entanglement	Improve Quantum Communications
Quantum-Assisted Radio Access Network (qRAN)	Yes	Yes		
Quantum Space Information Network (qSIN)	Yes	Yes	Yes	Yes
Quantum-Assisted Edge Networks (qEdge)	Yes	Yes		
Quantum-Assisted Data Centers (qDC)	Yes	Yes		
Quantum-Assisted Blockchain (qChain)	Yes	Yes	Yes	
Quantum-Assisted Wireless AI (qWAI)	Yes	Yes	Optional	
Quantum as a Service (QaaS)	Yes	Yes	Optional	
Quantum-Enabled Novel Applications (qApp)	Yes	Yes	Yes	

Thank you for your attention

Chonggang (CG) Wang, PhD, IEEE Fellow
Principal Engineer | InterDigital
T: (610) 878.5731
E: Chonggang.Wang@InterDigital.com

interdigital