양자인터넷 연구 동향

노광석(고려대학교), 허준(고려대학교)*

ks_noh@korea.ac.kr, junheo@korea.ac.kr

Quantum Internet Research Trends

Kwangseok Seok Noh(Korea Univ.), *Heo Jun(Korea Univ.)

요 약

본 논문에서는 양자인터넷 정의와 구성요소, 양자인터넷 주요 동향을 확인하고, 양자정보 전송 네트워크 발전 단계와 최근 발표된 미국 에너지부의 양자인터넷 개발 청사진을 살펴본다.

Ⅰ. 서 론

양자정보과학(QIS)은 고전 세계의 한계를 뛰어 넘는 정보 감지, 처리 및 통신을 달성하는 것을 목표로 양자 시스템의 연구, 제어 및 조작에 관한 것이다. QIS는 수십 년 동안 연구되어 왔지만 지난 6 년 동안 엄청난 발전과 돌파구를 가져왔다. 최근 트위터 등 SNS 해킹 사건, 코로나백신 정보유출 시도, 2016년부터 2020년까지 우리나라 정부 부처에 대한 해킹 시도 41만건 발생 등으로 정보보안에 대한 필요성은 더욱 커지고 있는 상황이다. 전 세계적으로 양자 역학을 활용한 통신 시스템 구축이 21세기의 가장 중요한 기술극복 과제 중 하나로 여겨지고 있다.

2020년 미국 에너지부(DoE)에서 국가 양자인터넷 개발을 위한 청사진을 제시하는 전략 보고서를 발표했고 [1], 2019년 EU QIC project에서는 2028년까지 유럽 대륙내 양자통신이 가능한 infrastructure를 개발하고, 이를 2035년까지 quantum information networks로 의 확장 계획을 발표[2]하는 등 관련 연구 및 prototype 제작 및 네트워크 구축이 활발히 진행되고 있다.

본 논문에서는 양자인터넷 정의와 구성요소, 양자인터넷 주요 동향을 확인하고, 양자정보 전송 네트워크 발전 단계[3]와 미국 에너지부의 양자인터넷 개발 청사진을 살펴본다.

Ⅱ. 본 론

A. 양자인터넷

양자인터넷은 양자 채널로 연결된 각 노드를 각각의 독립된 물리적인 시스템으로 간주하고, 이러한 물리적인 시스템이 양자 채널을 통해 서로 상호작용을 함으로써 quantum many-body system을 이루는 것을 정의한다 [4]. 즉, 정보와 양자 자원을 분배하는 양자 네트워크를 통해 양자 컴퓨터, 시뮬레이터 및 센서를 상호 연결하여 작동하는 것으로 규정할 수 있다[2].

양자인터넷의 주요 요소는 각 노드로서 qubit을 저장하고 연산을 수행할 양자 프로세서, 양자 채널 역할을 수행할 양자통신 라인, 네트워크 상에서 원하는 노드로 qubit을 보내기 위한 path를 구성하는 스위치, qubit을 먼 거리에 존재하는 노드로 보내기 위한 양자 중계기, 양자정보의 도청 방지를 위한 양자 얽힘, 불안정한 양자 상태로 인해 발생한 오류를 수정하는 오류정정부호로 구성된다.

양자인터넷을 위한 양자 네트워크 및 구성요소 동향은 다음과 같다.

- 2012년 오스트리아 빈 대학의 연구진이 양자 중계기를 이용한 143킬로미터(㎞) 유선 통신에 성공
- 2017년 SKT 112km 실험망에 양자 중계기를 적용하여 양자암호키 전송 성공
- 2019년 네덜란드에서 단일 큐비트에 대해 75초, 두 큐비트의 양자 얽힘에 대해 10초간 유지 가능한 양자 레지스터 구현
- 2019.04. ESnet, SBU, Brook-haven National Lab의 협업으로 11mile 양자 얽힘 분배실험 성공
- 2020.02. 미국 DOE산하 아르곤 국립 연구소와 시카고 대학 시카고 교외에서 얽힘 광자를 52mile 유선 전송 성공
- 2020.02. Fermi lab과 연결하여 3개의 노드를 가진 80mile test-bed 구성 예정 발표
- 2020.11. SBU, Brook-haven National Lab의 협업으로 Long Island에서 뉴욕까지 양자 중계기를 적용하여 양자 네트워크 확장목표를 발표
- 2021년 University of Science and Technology of China, Tsinghua University, University of Oxford의 협업으로 12 qubit 규모의 초전도 양자 프로세서를 이용하여 오류정정부호 ⟦5,1,3⟧ 코드를 실험적으로 구현

B. 양자정보 전송 네트워크 발전 단계[3]

2018년 네덜란드 QuTech사는 양자인터넷을 실현할 수 있는 과정을 담은 포괄적인 내용의 논문을 발간하였고, qubit를 이용해 양자인터넷을 완성하는 여섯 단계의 세부적인 과정을 제시하였다.

1. Trusted repeater networks (Quantum repeater)

- 각 인접 노드는 QKD를 사용하여 암호화 키를 교환하며, 모든 중간 노드 간 통신 과정이 신뢰할 수 있을 때 end-to-end 통신의 신뢰성이 보장된다. 이를 위해 trusted repeater의 개발 또는 untrusted repeater를 보완할 수 있는 안전한 QKD 프로토콜에 대한 연구가 이뤄지고 있다.

2. Prepare and measure networks

- 이 단계에서는 모든 노드가 1-qubit 상태를 준비할 수 있고, 결과 상태를 다른 노드로 전송한 다음 이를 측정한다.

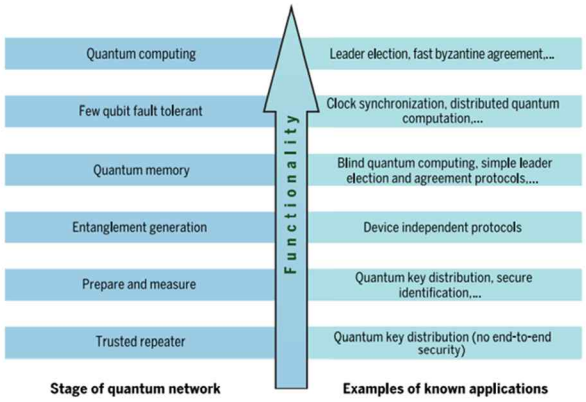

그림 1. 양자인터넷 발전 단계[3]

3. Entanglement distribution networks

- end-to-end에서 양자 얽힘 생성을 허용하면서 양자 메모리가 필요하지 않은 유형이며, 대부분의 양자 장치는 신뢰할 수 없는 것을 고려한다. 해당 네트워크에서는 Device-independent 프로토콜을 실현할 수 있으며 Device-independent QKD에 대한 연구를 요구한다.

4. Quantum memory networks

- 양자 메모리가 지원될 경우, 양자 상태를 임시로 저장하거나 더 복잡한 연산을 필요로 하는 프로토콜 구현 가능한 상태이다. 두 node가 통신하는데 걸리는 최대 시간을 뒷받침할 만한 저장 시간을 지닌 메모리 개발이 요구된다.

5. Few-qubit fault-tolerant networks

- Qubit의 일부 오류가 발생하더라도 시스템 동작이 가능한 Fault-tolerant gate가 지원될 경우, 높은 depth의 양자 회로를 구동 할 수 있으며 더 복잡한 통신 프로토콜이 가능해진다.

6. Quantum computing networks

- 임의의 시스템간 양자 통신이 가능한 양자 컴퓨터들로 구성된 네트워크이고, 이를 이용할 수 있는 문제와 해답을 찾는 과정이 요구된다.

7. Photonic communication channels

- Photonic channel은 멀리 있는 repeater와 end node 사이에 존재하는 양자 채널을 의미하고, 광자 손실과 decoherence 최소화가 필요하다. 일반적으로 fiber-based 채널과 위성을 이용하는 free-space 채널 두 타입으로 분류한다.

C. 미국 에너지부(DoE) 양자인터넷의 청사진 전략[1]

4가지 최우선 연구 분야와 5가지의 최우선 해결 과제(Roadmap milestones)를 규정하였다.

4가지 최우선 연구 분야로는 ①양자인터넷을 위한 기본적인 빌딩블록 제공 ②복수의 양자 네트워킹 디바이스 통합 ③양자 얽힘을 위한 리피터/스위칭/라우팅 기술개발 ④ 양자 네트워킹 함수의 오류 수정 기능 설정으로 규정하였다.

5개의 최우선 해결 과제로는 ①기존 광섬유 네트워크를 통한 안전한 양자 네트워크 프로토콜 검증 ②캠퍼스간 및 도시간 얽힘정보 배분 ③양자 swapping을 통한 도시 간 양자 네트워크 확장 ④양자 리피터를 이용한 미국 각 state간 양자 얽힘 분포 ⑤산·학·연을 아우르는 복수기관 환경(ecosystem) 조성

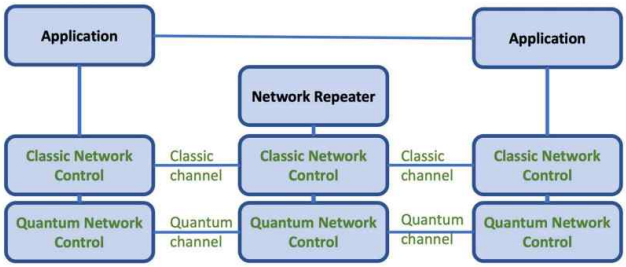

그림 2. 고전 통신 채널과 함께 양자 채널이 사용되는 양자 네트워크의 개략도 [1]

등으로 규정하였다. 이 때, ④에서는 기존 인터넷 기술 및 양자 인터넷 기술의 통합이 이루어지고, 양자 중계기를 이용한 연속적인 규모의 거리에 대한 손실 및 운용 오류에 관한 양자 오류 수정 통신이 성공적으로 이루어진다. 따라서, 더 먼 거리를 커버하는 운영상의 얽힘 분배 네트워크를 구축할 수 있는 길을 열어 사상 최초의 양자 인터넷을 만들 수 있다.

Ⅲ. 결론

본 논문에서는 양자인터넷 정의와 구성요소, 양자인터넷 주요 동향을 확인하고, 양자정보 전송 네트워크 발전 단계와 미국 에너지부의 양자인터넷 개발 청사진을 살펴보았다. 현재 trusted repeater를 사용하는 양자 네트워크 구성과 그에 적합한 양자암호 프로토콜을 이용한 prototype 뿐만 아니라 large-scale의 다양한 네트워크 구축이 활발히 이루어지고 있고, 양자 얽힘과 양자 메모리는 간단한 형태의 prototype 수준의 연구와 실험이 진행되고 있다.

양자인터넷은 소규모 양자 네트워크를 통합함으로써, 향후 10년간 개발 가능한 수천~수만 qubit 이하 규모의 다수 양자컴퓨터를 분산 네트워크로 연결하여 수만 qubit 이상의 효과를 나타낼 수 있다. 또한, 양자컴퓨터의 qubit 수가 증가할 때마다 디지털 제어부의 복잡도가 크게 증가하므로 수만 qubit 양자컴퓨터 1대 제작보다 용이한 수천 qubit 양자 컴퓨터 여러 대를 연결하여 동일한 성능을 이끌어 낼 수 있는 잠재력이 있다.

ACKNOWLEDGMENT

이 성과는 2021 년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2019R1A2C2010-061)

참 고 문 헌

[1] https://www.energy.gov/sites/prod/files/2020/07/f76/QuantumWkshpRpt20FINAL_Nav_0.pdf

[2] http://www.qtspace.eu/sites/testqtspace.eu/files/other_files/IndustryWhitePaper_V3.pdf

[3] Wehner, Stephanie, David Elkouss, and Ronald Hanson. "Quantum internet: A vision for the road ahead." Science 362.6412 (2018).

[4] Kimble, H. The quantum internet. Nature 453, 1023-1030 (2008).