양자암호통신 시뮬레이터 동향

노광석, 허준*
고려대학교, 고려대학교

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

A study on the Quantum Key Distribution Software Simulato

Noh Kwang Seok, Heo Jun*
Korea Univ., *Korea Univ

요 약

양자암호통신의 동작을 이해하고 응용하기 위해 다양한 소프트웨어 시뮬레이터가 개발 중이다. 본 논문에서는 다양한 QKD 시뮬레이터의 특징을 살펴보고 개선할 점을 살펴본다.

Ⅰ. 서 론

양자암호통신(QKD)는 양자정보기술 중 상용화에 가장 근접한 기술로써 의료, 금융 등의 정보 보호를 위해 다양한 실제 적용이 이루어지고 있는 분야이다. QKD 분야의 시장 활성화를 위해서는 양자기술 개발, 구현, 응용 등 양자분야 전문가 이외에 다양한 배경 지식을 갖은 인원의 참여가 필요하다.

양자암호통신(QKD)의 동작을 이해하기 위한 접근 방법은 이론적 분석, 하드웨어 실험 그리고 소프트웨어를 기반으로 시뮬레이션이다. S/W 시뮬레이터는 디지털 통신, 제어 등 많이 분야에서 이미 사용해왔으며 최근에는 양자암호통신을 위한 S/W 시뮬레이션을 다양한 방식으로 시도하고 있다. 디지털 분야에서 많이 사용한 매틀랩을 이용 [1], python 프로그램[2]을 이용하거나 광학 시뮬레이터를 활용[3]하기도 한다. 이러한 시뮬레이터는 양자분야 전문가뿐만 아니라 비전문가에게도 QKD 를 이해하는데 도움을 준다.

본 논문에서는 양자암호통신을 위한 소프트웨어 시뮬레이터의 특징을 살펴보고 활용을 위한 개선방향을 살펴본다.

Ⅱ. 본론

A. QKD 시뮬레이터 특징

양자암호통신 시뮬레이터는 광학 소자를 개념적 또는 수학적으로 모델링하여 신호가 전송되는 과정에 집중하는 physical layer 시뮬레이터와 양자인터넷을 포함하는 네트워크 시뮬레이터로 구분할 수 있다. QKD phy-layer 시뮬레이터는 대부분 Discrete-Event System (DES)으로 분류되는 dynamic, time-invariant, non-linear, discrete-state, event-driven, stochastic, discrete-time 특징을 가진다 [4].

B. 시뮬레이터 솔루션

현재 양자암호통신 시뮬레이터는 특정된 플랫폼을 사용하지 않는다. 본 장에서는 최신 시뮬레이터 중 위 특징에 맞는 일부를 살펴본다.

- SeQUeNCe: 오픈 소스로 제공되는 Python 기반 양자 네트워크 시뮬레이터이며, 양자, 하드웨어, 네트워크 계층으로 분리하여 설계할 수 있다. 양자메모리 등 양자 네트워크에 필요한 구성 요소를 개념적으로 사용할 수 있으며, phy-layer 단에서는 암호키 길이와 light 소스의 주파수, 광자 delay time 만을 설정할 수 있는 BB84 프로토콜을 제공한다. 양자암호통신은 양자전송부와 후처리부로 구성되며, 대다수 phy-layer 시뮬레이터는 주로 양자 전송부만을 다루며 BB84 와 같은 유명한 프로토콜을 제공한다.

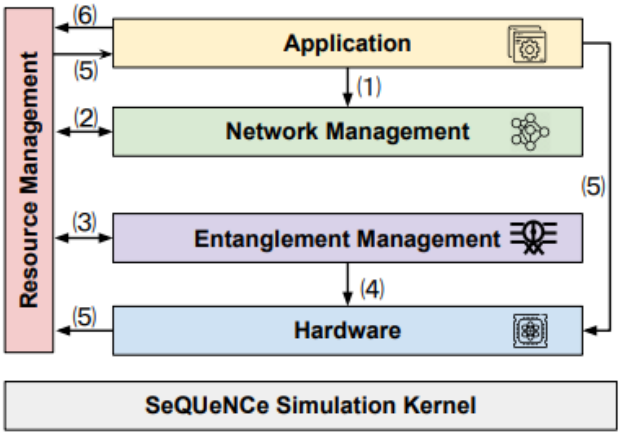

그림 1.Sequence 를 이용한 네트워크 아키텍쳐 개념 구성도

- qkdSim: Python 기반 QKD 시뮬레이터이며, VPItoolkit 에 추가되는 API 를 통해 소자의 왜곡 특성을 반영한 광학 소자 일부를 제공한다. 사용자는 discrete variable (DV) 및 continuous variable (CV) 프로토콜의 양자전송부를 구성하는 소자 선택으로 정해진 프로토콜만 구현 가능하다.

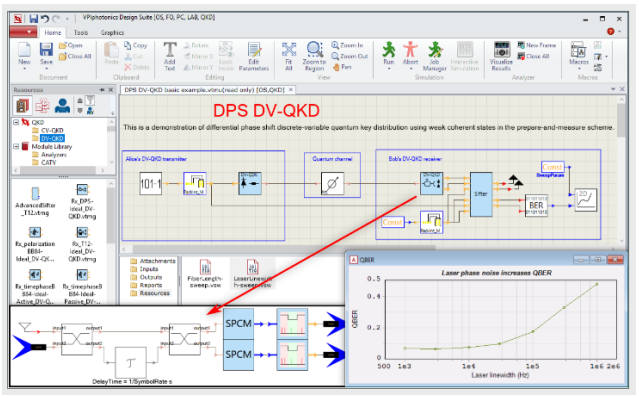

그림 2.VPItookit 을 사용한 양자암호통신 회로 구성도

- QSIMpro: QSIMpro[5]는 그래픽 기반 시뮬레이터로써 제공되는 광소자와 후처리 기능 블록을 조합하여 QKD 프로토콜을 구성할 수 있다. 그림 3 은 QSIMpro 를 이용하여 one-way BB84 프로토콜을 구성한 예시를 나타낸다 양자전송부와 후처리부 기능뿐만 아니라 전기 신호를 이용한 제어 기능을 제공한다. 다양한 광소자를 모델링하여 광소자 단위로 사용자가 기능을 설정할 수 있으며, 사용자 인터페이스를 그래픽으로 제공한다.

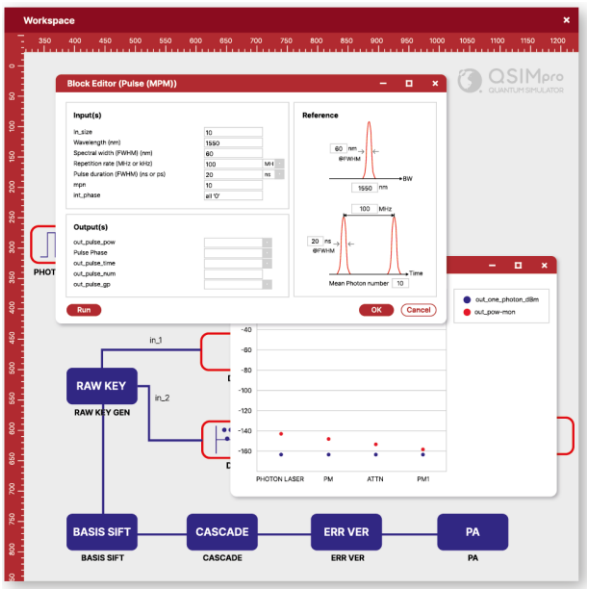

그림 3. QSIMpro 를 이용한 양자암호통신 회로 구성 및 입출력 예시

C. 시뮬레이터 문제점

WDM 을 이용하여 데이터와 QKD 동시 전송 시스템은 두가지 기술을 접목한 방법이다. 대부분의 양자암호통신 phy-layer 시뮬레이터는 BB84, DPS 같은 잘 알려진 프로토콜을 시뮬레이션을 할 수 있다하더라도 정해진 동작만 가능하며, 변형하는 것이 매우 어렵다. 즉, 기존 기술의 성능 검증에 치중되어 있는 한계가 있다. 예를 들어, plug & play BB84 프로토콜에서 Delay-line 은 정해진 계산된 길이안에서만 동작이 보장된다. QKD 활용을 위해서는 기존 기술의 확장과 변형이 가능해야 하며, 성능 검증뿐만 아니라 설계툴로써의 역할이 요구된다. 또한, 접근을 위해 사용자 사용 난이도를 낮춰야 한다

Ⅲ. 결론

QKD 시뮬레이터는 QKD 동작에 대한 phy-layer 시뮬레이터와, QKD 활용에 대한 네트워크/인터넷 시뮬레이터로 구분할 수 있다. 본 논문에서는 다양한 형태의 시뮬레이터의 특징을 살펴보았고, QKD 활용을 위한 phy-layer 시뮬레이터의 개선 방향을 소개하였다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 정보통신·방송 연구개발사업의 일환으로 수행하였음. [2021-0-01810, 양자세계를 연결하는 초신뢰 양자인터넷 요소기술개발]

참 고 문 헌

[2] X. Wu, A. Kolar, J. Chung, D. Jin, T. Zhong, R. Kettimuthu, and M. Suchara, SeQUeNCe: A Customizable Discrete-Event Simulator of Quantum Networks, arXiv:2009.12000, (2020).
[2] R. Chatterjee, et al. "qkdSim: An experimenter's simulation toolkit for QKD with imperfections, and its performance analysis with a demonstration of the B92 protocol using heralded photons. arXiv:1912.10061v1 (2019)
[3] https://www.vpiphotonics.com/Tools/QKD/.
[4] J. D. Morris, D. D. Hodson, M. R. Grimaila, D. R. Jacques, and G. Baumgartner, Towards the modeling and simulation of quantum key distribution systems, Department of the Air Force Air University 4, 47 (2014).
[5] https://www.qsimplus.com