WDM 을 활용한 데이터와 QKD 동시 전송 시스템 구현 방안

김범일, 김종민, 고영채, 허준*
고려대학교

{bik0118, botboy0441, koyc, *junheo}@korea.ac.kr

A study on the implementation of a Data and QKD Simultaneous Transmission System Using WDM

Kim Bum Il, Kim Jong Min, Ko Young Chai, *Heo Jun
Korea Univ.

요 약

본 논문은 기존의 분리되어 있는 데이터 전송과 QKD 의 키 전송을 WDM 을 이용하여 하나의 채널을 통해서 전송하는 구현 방안을 소개한다. 또한, 구현 시 고려해야 되는 문제점을 분석하였다.

Ⅰ. 서 론

최근 IoT, Cloud computing 과 같은 기술의 발달로 인해 유무선 통신의 사용이 급속히 확대됨에 따라 통신에서의 보안은 더욱 중요해졌다. 기존의 수학적 복잡성에 기반하였던 비대칭 공개키 암호체계는 양자컴퓨터가 발전되어 감에 따라 다항시간안에 해가 구해질 것으로 예상되어 비대칭 공개키 암호체계의 안전성에 대한 의문이 제기되었다. 이로 인해 양자역학에 기반한 양자키분배(Quantum Key Distribution, QKD) 기법이 활발하게 연구되어 BB84, DPS QKD, MDI QKD, TF QKD 와 같은 다양한 QKD 프로토콜이 개발되고 실제 구현되어 왔다.[1~4]

그러나, QKD 를 이용하기 위해서는 기존 광통신망과 별개로 추가적인 채널이 필요하다는 단점이 있다.

본논문에서는 파장 분할 다중화 (Wavelength Division Multiplexing, WDM)기법을 이용하여 데이터 전송과 QKD 의 키 전송을 하나의 채널을 통해서 전송하는 구현 방안을 소개하고 구현 시 고려해야 되는 문제점을 분석하였다.

Ⅱ. 본론

A. WDM 를 이용한 데이터와 QKD 동시 전송 시스템

WDM 을 이용하여 데이터와 QKD 동시 전송 시스템은 두가지 기술을 접목한 방법이다.

먼저, WDM 은 유/무선 광통신에서 주로 사용되는 기법으로 서로 다른 파장을 여러 개 이용하여 각각 다른 데이터를 전송하는 기법이다. 여러 파장의 빛이 섞이더라도 각 파장의 굴절률에 따라 물리적으로 분리 및 합성되므로 인접한 채널사이 간섭이 적어 직교성이 보장된다. 이를 통해 하나의 회선을 통해 여러 개의 독립된 데이터를 전송할 수 있어 추가적인 회선 증설이 불필요하다는 장점이 있다. WDM 의 구현방법으로는 WDM 에 사용되는 파장 간격이 10nm 이상의 차이가 나는 CWDM 기법과 파장 간격이 0.4nm, 0.8nm, 1.6nm 등으로 밀집되어 있는 DWDM 기법이 있다.

QKD 는 비가역성, 중첩, 복제 불가능성의 양자역학적 성질을 이용하여 도청자가 양자 채널에 접근하여 도청을 시도하는 경우, QBER 을 통해 도청자를 감지할 수 있다. QBER 이 threshold 를 넘어가는 경우, 나누어 가진 키를 파괴하고 threshold 를 넘지 않는다면 후처리 과정을 통해 노출된 정보를 제거하여 도청을 차단한다. 일반적으로 키정보를 전송하는 양자 채널과 후처리과정에 필요한 정보를 주고받는 디지털 채널을 이용한다.

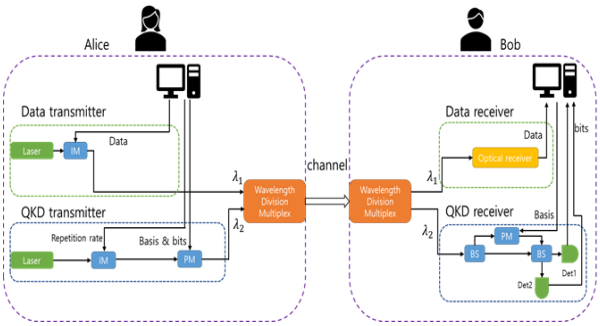

그림 1. WDM 을 이용한 데이터와 QKD 동시 전송 구현도

WDM 을 이용하게 되는 경우, 기존의 데이터를 전송하는 채널과 QKD 에서 키정보를 전송하는 양자채널, 비밀키를 얻기 위해 키 sifting, 오류정정과정등 후처리에 필요한 데이터를 주고받기 위한 디지털 채널을 통해

전송되는 정보를 서로 다른 파장으로 인가하고 Mux 를 모두 하나의 채널만 이용해서 전송할 수 있기 때문에 QKD 로 인해 발생하는 cost 를 줄일 수 있다는 장점이 있다. 그리고 이를 통해 1:1 이 아닌 N:N 으로 키분배도 가능하다.

B. WDM 를 이용한 데이터와 QKD 동시 전송 시스템의 고려사항

WDM 을 이용하여 데이터와 QKD 를 동시에 전송하는 시스템을 구현하기 위해서는 두가지 대표적인 잡음을 고려해야 한다.

첫번째로 고려해야 되는 잡음은 라만 스캐터링 (Raman scattering)이다. Raman scattering 은 비선형적 광학 (Non-linear optic) 현상으로 레이저 펄스가 광섬유 케이블 같은 주변 환경과 영향을 주고받아 본래의 생성 파장이 아닌 다른 파장의 광자가 발생되는 것을 말한다. 광섬유 케이블내에서는 Forward Raman Scattering 과 Backward Raman Scattering 이 발생하는데 Forward Scattering 은 레이저 펄스와 동일한 진행방향으로 발생하는 photon noise 이다. Backward Raman scattering 은 레이저의 펄스 진행방향과 반대 방향으로 생성되는 광자 잡음 (photon noise)으로 이후 전파되는 레이저 펄스에 영향을 주어 키 정보가 encoding 되어 있는 펄스를 왜곡시켜 키 정보를 주고받는데 어려움을 발생시킨다.

두번째로 고려해야 되는 잡음은 Four wave mixing 이다. Four wave mixing 또한 비선형적 광학 현상으로 서로 다른 2 개 이상의 광 파장을 갖는 빛이 광섬유 케이블을 따라 전파될 때, 다음과 같은 서로 다른 2 개의 파장을 갖는 빛이 생성되는 것을 말한다.

$$\lambda_3 = 2\lambda_1 - \lambda_2, \lambda_4 = 2\lambda_2 - \lambda_1$$

이를 극복하기 위해서는 협대역 필터 (narrow band filter)를 사용하여 설정한 파장만을 남겨 검출하고[5], 양자정보를 전송하는데 사용하는 레이저의 파장과 데이터를 전송하는데 사용되는 레이저의 파장 사이에 가드 대역 (guard band)을 두는 방식으로 Raman Scattering 을 피하는 방식 등을 사용한다.

Ⅲ. 결론

본논문에서는 WDM 기법을 이용하여 데이터와 QKD 를 동시 전송할 수 있는 시스템 구현 방안을 소개하였다. 이를 통해 QKD 를 이용하기 위해 추가적으로 필요한 회선 설치비용을 줄이고 N: N 통신이 가능해진다는 장점이 있다.

그러나, 이를 구현하기 위해서 고려해야 되는 잡음은 Raman Scattering noise 와 Four Wave mixing 이다. 이를 극복하기 위해서는 협대역 필터를 사용하여 기존 파장 외의 다른 파장을 갖는 광자를 제거하고 양자정보를 전송하는데 사용하는 레이저 파장과 데이터를 전송하는데 사용되는 레이저 파장 사이에 가드 대역를 두는 방식 등의 방법을 사용한다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] C. H. Bennet and G. Brassard, Quantum Cryptography: Public key distribution and coin tossing, Proceeding in IEEE international Conference on Computers, Systems, and Signal Processing, Bangalore: 175(1984).

[2] T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach-Zehnder interferometer," Opt. Lett. 29, 2797-2799 (2004)

[3] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” Phys. Rev. Lett., vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[4] Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature.(2018)

[5] P. Eraerds et al, “Quantum key distribution and 1Gbps data encryption over a single fibre”, New Journal of Physics 12, 063027(2010)

[6] Mao, Yingqiu, et al.,. ”Integrating quantum key distribution with classical communications in backbone fiber network.” Optics express 26, 6010-6020 (2018).