WDM QKD channel 환경에 대한 noise 분석

곽혜린, 윤승호, 허준*
고려대학교

lynkwak12@korea.ac.kr, seunghyoon@korea.ac.kr *junheo@korea.ac.kr

Noise Analysis for WDM QKD Channel Environment

Kwak Hyelyn, Yoon Seungho, Heo Jun*
Korea Univ., Korea Univ., *Korea Univ.

요 약

본 논문은 QKD 신호를 WDM channel 환경으로 송신했을 시 생길 수 있는 noise 의 종류 및 영향에 대해 설명한다. 다른 파장대역과의 상호작용으로 인한 Raman scattering, four wave mixing 을 통해 신호 detection 시 error rate 가 증가할 수 있다. 따라서 유선 환경 BB84 protocol 에 대해 실제 key rate 수식에 어떤 변화가 생기는지 확인한다.

Ⅰ. 서론

QKD(Quantum Key Distribution; 양자 키 분배)는 양자역학의 원리를 이용하여 암호키를 분배하는 방식으로, 이론상 도청이 불가능한 통신환경을 제공한다[1]. WDM channel 에 QKD 신호를 같이 전송한다면 기존의 광통신망을 이용할 수 있으므로 효율적인 통신 방법이 될 수 있다.

그러나 QKD channel 은 single photon state 를 요구하므로 다른 파장대역의 간섭이 많은 WDM 환경에서 전송하기엔 어려움이 많다. 본 논문에서는 WDM 환경에서 발생하는 Raman scattering 과 Four Wave Mixing(FWM) 이 QKD channel 에 미치는 영향을 분석하여 key rate 변화를 확인한다.

Ⅱ. 본론

A. 단일 channel 에서의 QKD security

QKD 의 efficiency 는 Bob 의 detector equipment transmittance, fiber attenuation, 등으로 판단할 수 있다[2,3].

$$\eta = 10^{-\frac{\alpha L}{10}} t_{Bob} \eta_{Det}$$

i-photon state 에 대한 yield 는 다음과 같이 나타낼 수 있다.

$$Y_i \cong Y_0 + 1 - (1-\eta)^i$$

Phase 가 randomized 된 attenuated laser pulse 는 weak coherent pulse 를 쓰는 것과 동치이므로 Poisson 분포를 따른다. Gain Q는 다음과 같이 나타낼 수 있다.

$$Q = \sum_{i=0}^{\infty} Y_i \frac{\eta^i}{i!} e^{-\eta} = Y_0 + 1 - e^{-\eta\mu}$$

i-photon state 에 대한 QBER(Quantum Bit Error Rate)는 다음과 같이 나타낼 수 있다.

$$e_i = \frac{e_0 Y_0 + e_{det}[1-(1-\eta)^i]}{Y_i}$$

전체 photon state 에 대한 QBER 은 다음과 같이 나타낼 수 있다.

$$EQ = \sum_{i=0}^{\infty} e_i Y_i \frac{\eta^i}{i!} e^{-\eta} = e_0 Y_0 + e_{det}(1 - e^{-\eta\mu})$$

[2]에서 정의하는 QKD 최종 key rate 는 다음과 같다.

$$R > q\{-Qf(E)H_2(E) + Q_1(1 - H_2(e_1))\}$$

$f(\cdot)$함수는 post-processing 에 의해 잃는 정보량을 나타내며, $H_2(\cdot)$는 binary entropy function 이다. q는 공개되는 key 의 비율을 나타낸다. QKD protocol 에 따라 변동될 수 있으며, BB84 protocol 은 $q = \frac{1}{2}$이다.

B. Raman Scattering

Raman Scattering 은 전송되는 광과 fiber 내의 optical phonon 과의 상호작용으로 발생한다. Raman scattering 은 신호의 진행방향과 관계없는 방향으로 생길 수 있으며(co-propagating/counter-propagating scattering), 전송 신호보다 낮은 파장대역에 발생하는 noise 를 Stokes Raman scattering, 높은 파장대역에 발생하는 noise 를 anti-Stokes Raman scattering noise 라 한다.

Raman scattering 에 의해 발생하는 noise 로 detection gate 당 count 되는 photon number 은 다음과 같다[4].

$$\begin{cases} C_{co} = z\exp(-\bar{\alpha}z)\,\eta\dfrac{\Delta t}{h\nu}\sum_i \beta_i P_{0,i} \\ C_{counter} = \dfrac{1}{2\alpha}[1-\exp(-2\bar{\alpha}z)]\eta\dfrac{\Delta t}{h\nu}\sum_i \beta_i P_{0,i} \end{cases}$$

이때 z는 fiber length, P_0 는 data channel 의 초기 power, $\bar{\alpha}$는 파장대역의 fiber attenuation 정도의 평균, β는 km 당 effective Raman scattering coefficient, Δt는 detection gate 의 길이이다.

β는 Stokes scattering, anti-Stokes scattering 여부에 따라 바뀌며, 다음과 같이 표현될 수 있다[4].

$$\begin{cases} \beta_i = s(i - i_q)\ if\ i < i_q \\ \beta_i = a(i_q - i)\ if\ i > i_q \end{cases}$$

이때 s, a는 frequency 에 따른 slope 이다.

이러한 coefficient 는 yield 에 영향을 끼친다. BB84 protocol 의 경우 vacuum state yield 는 다음과 같다[5].

$$Y_0 = 2p_{darkcount} + p_{afterpulse} + p_{crosstalk} + \kappa p_{RS}$$

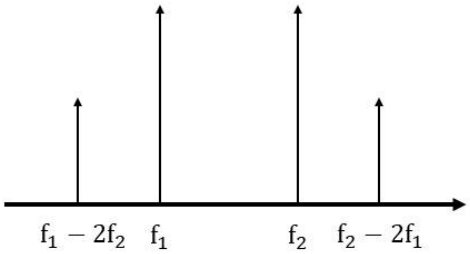
이때, κ 는 WDM modulation 방법에 따라 달라지는 수치이다.

C. Four Wave Mixing (FWM)

Four wave mixing 은 비선형 매질에서 나타나는 효과로 두 종류의 파장대역 광이 존재할 때 그 외의 다른 두 파장대역에도 광이 생성되는 현상이다.

임의의 주파수 f_1, f_2에 대해 Four wave mixing 현상이 일어날 시 다음과 같은 추가적인 주파수가 생성될 수 있다. 생성되는 추가적인 두 주파수는 다음과 같다.

$$f_3 = 2f_1 - f_2, \qquad f_4 = 2f_2 - f_1$$



FWM 의 영향으로 QKD 신호의 phase misalignment 를 야기할 수 있다. BB84 protocol 의 경우 유선 환경에서 phase 에 encoding 을 하므로 FWM 현상이 error rate 를 높이게 된다. Non-linear misalignment 에 의한 parameter γ는 다음과 같이 정의된다[6].

$$\gamma = \frac{n_2 \omega_0}{c(A_{eff})}$$

이때, ω_0는 angular frequency, n_2는 fiber 3rd non-linear susceptibility $\chi^{(3)}$에 의한 parameter, A_{eff}는 작용하는 넓이를 나타낸다.

FWM 만이 misalignment 에 의한 error 에 영향을 미친다고 가정한다면, $e_{det} = \gamma$로 나타낼 수 있고,
따라서 i-photon state 에 대한 QBER e_i는 다음과 같다.

$$e_i = \frac{e_0 Y_0 + \gamma[1 - (1-\eta)^i]}{Y_i}$$

따라서 Raman scattering 에 의한 yield 변화와 FWM 에 의한 misalignment 요소를 고려한 QBER 은 다음과 같다.

$$E = \frac{1/2 Y_0 + \gamma(1 - e^{-\eta\mu})}{Q}$$

이 QBER 을 적용한 BB84 protocol 의 최종 key rate 는 다음과 같다.

$$R > \frac{1}{2}\{-Q_\mu f(E) H_2(E) + Q_1\left(1 - H_2\left(\frac{1/2 Y_0 + \gamma\eta}{Y_1}\right)\right)\}$$

Ⅲ. 결론

본 논문에서는 WDM QKD channel 환경에서 발생할 수 있는 noise 의 종류에 대해 논하고, 유선환경 BB84 protocol 에 대한 key rate 의 변화를 알아보았다. 가장 큰 noise 두 종류는 Raman scattering, four wave mixing 이며, 이는 single-photon level 의 power 를 가진 QKD 신호에 큰 영향을 끼칠 수 있다. 따라서 narrow bandpass filter 를 사용하는 등 noise 를 제거하는 작업이 필요하다.

ACKNOWLEDGMENT

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396) 이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. RS-2023-00225385, NISQ 환경에서 저부하, 고효율 양자 오류 경감 기술 개발 및 응용)

참 고 문 헌

[1] Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." Theoretical computer science 560 (2014): 7-11.

[2] Gottesman, Daniel, et al. "Security of quantum key distribution with imperfect devices." International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.. IEEE, 2004.

[3] Ma, Xiongfeng, et al. "Practical decoy state for quantum key distribution." Physical Review A 72.1 (2005): 012326.

[4] da Silva, Thiago Ferreira, et al. "Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems." Journal of lightwave technology 32.13 (2014): 2332-2339

[5] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," New J. Phys. 12, pp. 063027, 2010.

[6] Lin, Q., F. Yaman, and Govind P. Agrawal. "Photon-pair generation in optical fibers through four-wave mixing: Role of Raman scattering and pump polarization." Physical Review A 75.2 (2007): 023803.

[7] Chapuran, T. E., et al. "Optical networking for quantum key distribution and quantum communications." New Journal of Physics 11.10 (2009): 105001.

[8] Nielsen, Michael A., and Isaac L. Chuang. Quantum computation and quantum information. Vol. 2. Cambridge: Cambridge university press, 2001.,

[9] Hwang, Won-Young. "Quantum key distribution with high loss: toward global secure communication." Physical review letters 91.5 (2003): 057901.