Proceedings of the 4th International Conference on Computing and Data Science (CONF-CDS 2022)
DOI: 10.54254/2755-2721/2/20220544

Effect of classical data signals on quantum key distribution in industrial internet of things

Zhenzhi Lai

The University of Melbourne, Grattan Street, Parkiville, Victoria, 3010, Australia

zhenzhil@student.unimelb.edu.au

Abstract. Facing the increasing need of data transmission security, encrypting data through cryptography is a key solution. In an industrial Internet of things, cryptography based on quantum key distribution provides perfect secrecy with lower resource requirements of both computational power and storage compared with traditional cryptography. To explore how to deploy this technology, this paper proposes an industrial Internet of things network architecture embedded with quantum key distribution systems, combines it with the noise model of spontaneous Raman scattering and the evaluation model of quantum key distribution systems theoretically, simulates the performance in a normally used industrial environment, and works out instructions to the deployment of the raised architecture. The results also show that a better choice to avoid performance descending is to duplicate classical channels and quantum channels with the same direction instead of moving classical channels backward, while noises have the strongest influence at the transmission distance of 25 km.

Keywords: quantum key distribution, industrial internet of things, quantum cryptography, spontaneous Raman scattering.

1. Introduction

The Report of the Ministry of Industry and Information Technology of the People's Republic of China shows that due to the high value and influence of industrial data [1], the number of attacks to industry networks in 2020 increases more than 3 times than that in 2019, with the main break-point of Industrial Internet of Things (IIoT) devices because of low-defense. Because of this situation, encryption is a way to protect data. Although traditional cryptography could reach a perfect secrecy through the one-time-padding symmetric-key algorithm, the problem of its key distribution prevents the wide deployment in use. To solve this, quantum key distribution (QKD) is raised to share keys based on quantum mechanics [2].

The secrecy of QKD is based on the properties of quantum: no-cloning, collapse after measurement, and uncertainty [2]. With those properties, what the receiver receives is indeed what the sender sends, with any middle eavesdropping easy to be aware of. However, there are many challenges to deploying QKD systems into industrial networks. Compared with the high cost of constructing new fibers for QKD only, reusing the existing fibers by multiplexing the quantum channel with classical information channels through the wavelength division multiplex (WDM) technology is a more realistic method. Unfortunately, because the power of quantum signals is much lower than classical signals', those classical signals produce strong noises, performing as spontaneous Raman scattering (SpRS), to quantum channels. What's more, because of the low power of quantum signals, they are much harder to be detected after a transmission loss in fibers. All of those lead to a decrease of QKD performance, giving a secure key rate [3]. This paper is aimed to explore the environment of the QKD system where the influence of noises is lower.

To work out the low-noise schemes of WDM discrete variable QKD systems, this paper proposes an IIoT network architecture based on QKD systems and explores the influence caused by SpRS noises in theory. Then it constructs the model to illustrate how the system performance is influenced by SpRS noise and simulates those influences numerically. Finally, based on the comparison and discussion results, it concludes those low-noise schemes.

2. Related works

Many researchers have explored the feasibility of multiplexing quantum channels with classical channels. Kawahara et al. used 20% degradation of DPS-QKD system key rate as the criterion and showed the upper-bound noise of forward and backward SpRS with different detectors in carriers of 1536 nm (classical channel) and 1626 nm (quantum channel) separately through simulation [4]. Similarly, Zavitsanos et al. indicated that channel separation is essential and the accumulated Raman scattering photons are the dominant noise source through experiment [5], showing that an essential influence appears when the noise is greater than -10 dBm per channel in 3 km fibers.

Both of the above have shown the main noises and the way that those noises influence the QKD system's performance, but lack a combination of real industrial channels. In this paper, those results would be combined with real industrial environments to work out the QKD system performance through simulation.

3. Simulation methods

3.1. Network architecture

This paper proposes an IIoT network architecture based on quantum mechanics security shown in Figure 1. In this architecture, industrial data signals and quantum signals are transmitted in one single fiber based on WDM, where the transmission direction of quantum signals is the same as forward industrial data signals', but opposite to the backward's. This system architecture could provide a highly reliable and secure solution which meets the requirement of both encrypted data transmission and secure keys distribution.

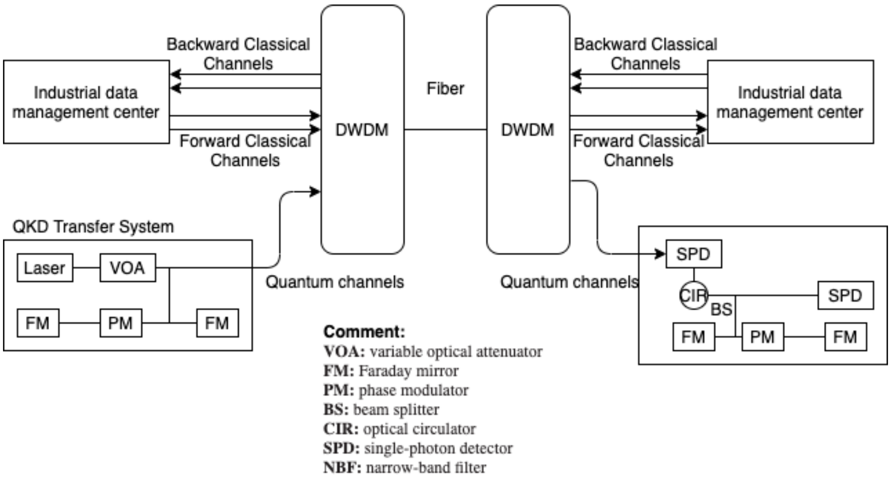
Backward Classical Channels
Industrial data management center
Forward Classical Channels
DWDM
Fiber
DWDM
Backward Classical Channels
Industrial data management center
Forward Classical Channels
QKD Transfer System
Laser
VOA
FM
PM
FM
Quantum channels
Quantum channels
SPD
CIR
BS
SPD
FM
PM
FM
Comment:
VOA: variable optical attenuator
FM: Faraday mirror
PM: phase modulator
BS: beam splitter
CIR: optical circulator
SPD: single-photon detector
NBF: narrow-band filter

Figure 1. IIoT Network Architecture with QKD Systems.

3.2. SpRS

Data are normally transmitted uni-direction or bi-direction in an industrial network. As a result, quantum channels may face noises as forward SpRS, backward SpRS, or bidirectional SpRS from classical channels in different situations. Suppose a light pumper p at point 0 generates lights with pumping power $P_p(z)$, the pump power at point z is [4]:

$$P_p(z) \ = P_p(0)\ exp[-\alpha_p z] \tag{1}$$

where α_p is the loss coefficient of the pump light. Let d_z be the distance of point z and 0 and η be the Raman efficiency, the SpRS generating power ($dP(z)$) at point z is [4]:

$$dP(z) \ = \eta P_p(0)\ exp[-\alpha_p z] d_z \tag{2}$$

Let L be the destination point and α_r be the fiber loss coefficient for SpRS lights, the total forward scattering power over the whole fiber length is [4]:

$$P_{raman}^{f} = \int_0^L \eta P_p(0)\ exp[-\alpha_p z] * exp[-\alpha_r (L-z)]\ d_z$$

$$P_{raman}^{f} = \frac{\eta P_p(0)}{\alpha_r - \alpha_p}\{exp[-\alpha_p L] - exp[-\alpha_r L]\} \tag{3}$$

If $\alpha_r \approx \alpha_p$, Eq. (3) is rewritten as [4]:

$$P_{raman}^{f} \approx \eta P_p(0) exp[-\alpha_p L] L \tag{4}$$

Similar to the forward scattering, the total power of backward scattering is [4]:

$$P_{raman}^{b} \approx \frac{\eta P_p(0)}{2\alpha_p}\{1 - exp[-2\alpha_p L]\} \tag{5}$$

3.3. Performance Evaluation of QKD

3.3.1. Secure key rate. The GLLP formula [6] assumes that for imperfect pumpers which may produce multiple photons signals, only the single-photon signals could be used to generate secure keys. Based on its assumption and results, the secure key rate S of a BB84 protocol system is computed as [2,7]:

$$S \geq Q_\mu \{H_2(e_\mu) + \Omega[1 - H_2(e_1)]\} \tag{6}$$

where Q_μ and e_μ are the gain of signal states and quantum bit error rate (QBER) for μ photons. $\Omega = Q_1/Q_\mu$ and $H_2(x) = -x\log_2(x) - (1-x)$. Let η_n be the detector which detects the signal if an n-state photon is sent, the probability that the receiver could detect the signal if the sender sends n photon states indeed Y_n is expressed as [7]:

$$Y_n = Y_0 + \eta_n \tag{7}$$

where Y_0 is the background noise assumed independent with signal states. This paper only considers that the background noise only contains SpRS noises (P_{raman}^{f} and P_{raman}^{b}) and dark count noise. The loss coefficient of an l length fiber is α dB and the detection efficiency of the detector is η_D, then Y_0 and η_n are written as [7]:

$$Y_0 = 2p_{dark} + P_{raman}^{f} + P_{raman}^{b}$$

$$\eta_n = 1 - (1 - 10^{\alpha/10}\eta_D)^n \tag{8}$$

Let Q_n (the detection expectation) be the production of the probability of sending n photon states and the probability of having a detection result based on whether photons sent, it is computed as [7]:

$$Q_n = Y_n P_\mu(n) = Y_n \frac{\mu^n}{n!} e^{-\mu} \tag{9}$$

3.3.2. Quantum bit error rate. The error bit on receiver's side comes from the background noises and measurement errors. When the sender sends n photon states, the error bit e_n based on a measurement error probability e_{det} is computed as [7]:

$$e_n = \frac{e_0 Y_0 + e_{det}\eta_n}{Y_n} \tag{10}$$

combined with Eq. (7) and Eq. (9), the total bit error rate is [7]:

$$E_\mu Q_\mu = \sum_{n=0}^{\infty} e_n Y_n P_\mu(n) = e_0 Y_0 + e_{det}(1 - e^{-\eta\mu}) \tag{21}$$

4. Result and discussion

4.1. Result and analysis

This paper demonstrates the secure key rate and quantum bit error rate depending on the variety of transmission distance, power of classical signals, and channel location. All simulated channels are around the C-band where the attenuation of fibers is the lowest. For initialized settings, 97 channels are initialized from 192.40 THz to 197.20 THz (0.05 THz for each channel spacing) and are numbered from 1 to 97. Then, to consider the worst situation, the length of the transmission is set to 25 km where the forward SpRS produces the highest noise (shown in Figure 2) with the pumping power of 10−5 W according to the normal requirements of industrial usage [8]. Finally, only the secure key rate above 0 is considered as a negative key rate is meaningless.

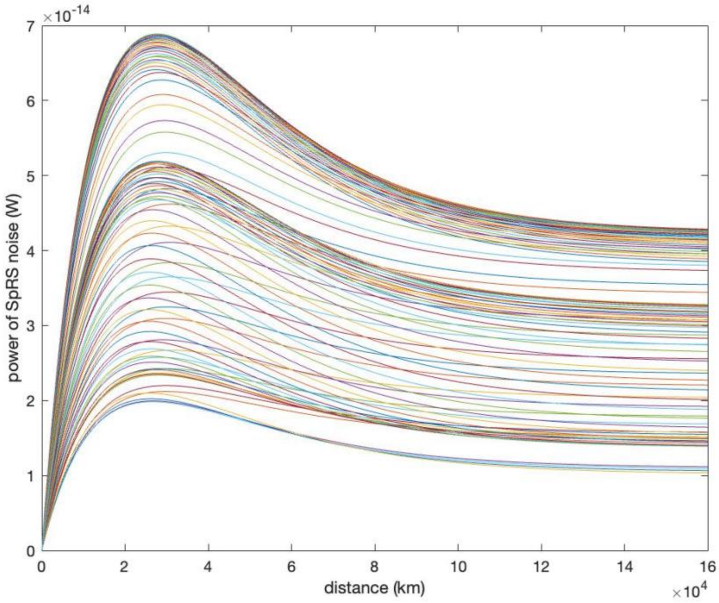

Figure 2. Power of SpRS Noise Varying with Distance (Each line represents a single channel)

To simulate a real fiber situation with multicommunications, totally 16 channels are set at the same time (4 forward and 4 backward for classical channels, 8 forward for quantum ones). 4 forward channels and 4 backward channels are set from 194.50 THz (45) to 194.90 THz (51) and from 195.00 THz (53) to 195.30 THz (59) separately with a spacing of 0.1 THz for each channel. In this situation, Raman efficiency for all 97 channels is computed and illustrated in Figure 3.

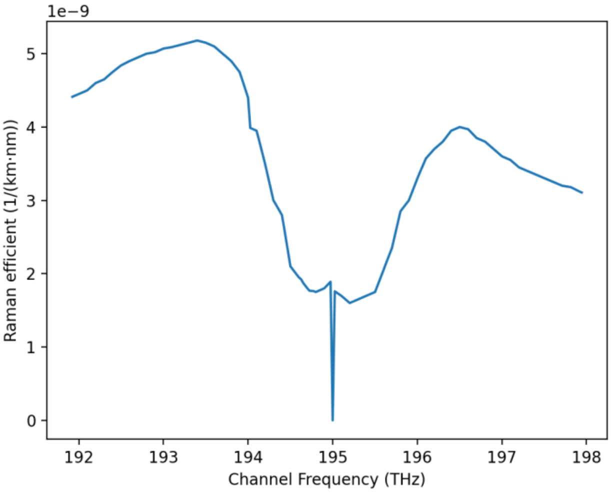

Figure 3. Raman efficient/channel.

Firstly, this paper explores the SpRS influence with the transmission distance. 8 quantum channels are set between 29-41 with pumping power of 10^{-5} W for all classical signals. The distance varies from 0 to 160 km and the secure key rate and quantum error bit rate for none of the classical channels activated, forward channels activated only, backward channels activated only, and all classical channels activated are illustrated in Figure 4.

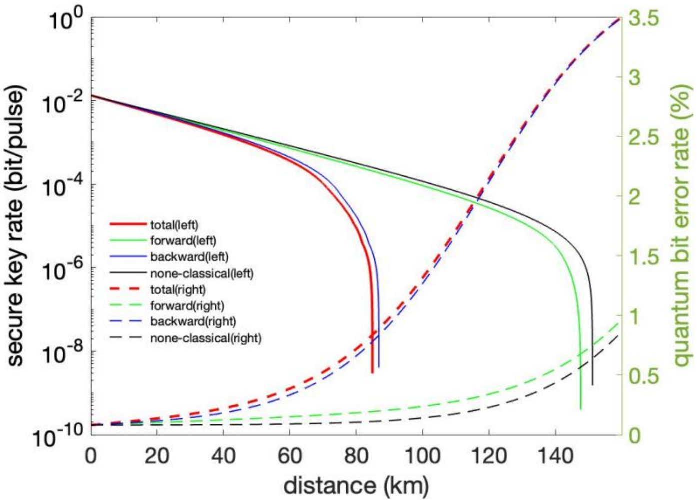

Figure 4. Key Rate/Error Rate Varying with Distance.

From Figure 4, it is obvious that quantum error bit rate increases with the increasing of transmission distance, and the secure key rate decreases with the heavier and heavier SpRS noise. The lowest acceptable secure key generating rate for a QKD system should be no less than 10^{-8} bit/pulse [9]. Due to this limitation, the QKD system with a bidirectional communication fiber works well within around 85 km, while the key rate is higher than 0.00375 bit/pulse in 25 km and drops quickly after 68 km. What's more, this figure also tells that the main noise is caused by the backward channels, and the bidirectional SpRS noise reduces the performance to around only 57% of its original (without any classical channels).

Next, SpRS influence with the strength of classical signal power is simulated. In this simulation, channels are set at the same position as before distance simulation. The transmission distance is fixed to 25 km. Then Figure 5 represents the secure key rate and quantum bit error rate with classical signal power varying from 10^{-7} W to $5 * 10^{-4}$ W.

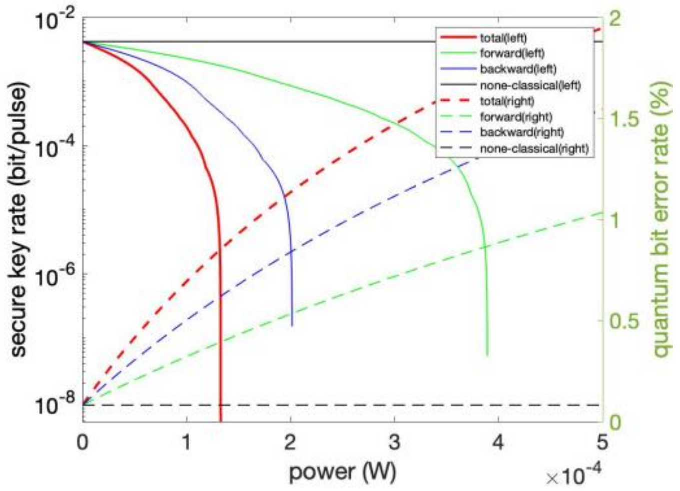

Figure 5. Key Rate/Error Rate Varying with Classical Signal Power.

From Figure 5, power of classical signals less than $1.27 * 10^{-4}$ W of bidirectional classical channels could be tolerant in this QKD system, where the key rate is 0.00356 bit/pulse when the power is 10^{-5} W and fails dramatically when the power is greater than 10^{-5} W. Same as before, the SpRS of backward channels is much larger than that of forward channels.

Finally, SpRS influence with different positions of classical channels is simulated by changing the quantum channels in the range of channel 1 to channel 97 with a spacing of 0.1 THz for each channel where all the 8 classical channels keep unchanged as before (45-51, 53-59). This time, the power of classical signals is fixed at 10^{-5} W and the transmission distance is fixed at 25 km. The x-axis in Figure 6 is the start channel number for the following 3 channels (e.g. 1 represents channels numbered 1, 3, 5, 7).

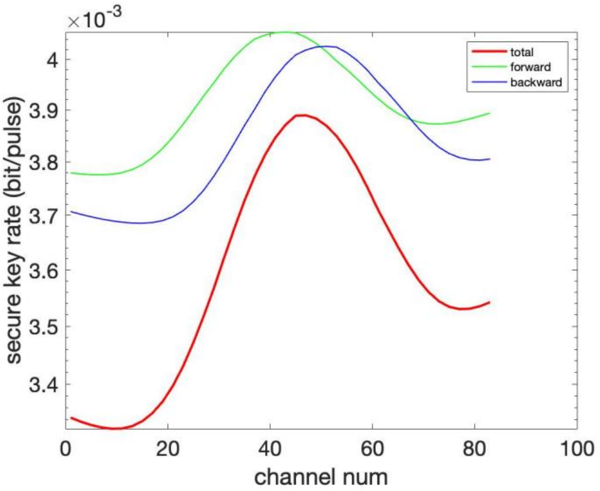

Figure 6. Key Rate Varying with Quantum Channel Position.

The reason for the secure key rate going down first, then increasing to the peak point, dropping down again, and finally increasing is shown in Figure 3 as the Raman efficiency for each channel is negatively correlated to the key rate. Figure 6 shows the closer quantum channels to classical channels and the higher performance of the QKD system it would have. Also, it is obvious that compared with the frequency of classical channels, quantum channels in higher frequency perform better than those in lower frequency.

The reason for all three curves' peak points' channels (the channel owing the highest key rate/facing the lowest noise influence) are not exactly the channel of 53 is that those channels are not single channels but a group of channels. For the group of forward channels, they range from 45-51, where the peak should be between this range, which is the same as backward channels.

4.2. Discussion

To conclude in the C-band frequency based on industrial environment settings with a situation of 4 forward, 4 backward classical channels and 8 forward quantum channels, suggestions of settings are listed as follows:

- Backward classical channels produce much more SpRS noise than forward ones normally. As a result, multiplex quantum signals with forward signals but avoid backward transmitting when quantum channels are activated as much as possible.
- The transmission distance within 85 km with classical signal power of 10^{-5}W makes the use of advantages of QKD systems, while for a fixed distance of 25 km (where the SpRS noise is the maximum), classical signals could be generated within the power of $1.27 * 10^{-4}$ W for each channel.
- For the choice of channels, classical channels and quantum channels should be as much closer as possible. Also quantum channels are suggested to be placed in higher-frequency channels rather than lower-frequency channels compared with classical channels' frequency.

5. Conclusion

To meet the requirement of highly secure IIoT network data transmission, this paper designs an system architecture based on QKD systems, simulates the expecting performance of this system under the normal industrial network conditions and raises instructions of settings to deploy this system. Through the result based on the proposed system architecture, QKD system works well in IIoT network conditions and takes advantages of it in a situation of transmission distance less than 85 km and classical signals strength less than $1.27 * 10^{-4}$ W of each channel generally. However, with different usage requirements, the number and kind (forward/backward) of classical channels used are different. As a result, companies could adjust their network architecture and settings based on figures in this paper and put quantum channels as much closer to classical channels with a higher frequency as they can to increase QKD system performance. Finally, to avoid a huge performance drop, it is suggested that transmission distance and pumping powers for one single pair of QKD transmitting/receiving devices should not be closed to their acceptable limitations.

References

[1] Ministry of Industry and Information Technology.: 2020 Industry and Information Technology Security Report (1999).

[2] Bennett, C. H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Theoretical Computer Science (560), 7-11 (2014).

[3] Xiaofan, M.: Experimental Research on Quantum Cryptography, PhD thesis, University of Science and Technology of China (2006).

[4] Kawahara, H., Medhipour, A., Inoue, K.: Effect of Spontaneous Raman Scattering on Quantum Channel Wavelength-Multiplexed with Classical Channel. Optics Communication 284(2), 681-696.

[5] Zavitsanos, D., Giannoulis, G., Raptakis, A., Papapanos, C., Avramopoulos, H.: Coexistence of discrete-variable qkd with wdm classical signals in the c-band for fifiber access environments. In: 2019 21st International Conference on Transparent Optical Networks (ICTON). (2019).

[6] Gottesman, D., Lo, H.-K., Lutkenhaus, N., Preskill, J. Security of quantum key distribution with imperfect devices. In International Symposium on Information Theory, ISIT 2004. 136. IEEE, (2004).

[7] Wei, C.: Experimental Research on Fiber Quantum Key Distribution, PhD thesis, University of Science and Technology of China (2008).

[8] Cheng, N., Wang, L., Liu, D., Gao, B., Gao, J., ZHou, X., Lin, H., Effenberger, F.: Flexible TWBM PON with Load Balancing and Power Saving. In 39th European Conference and Exhibition on Optical Communication (ECOC). 1-3. (2013).

[9] Ma. X., Zeng, P., Zhou, H.: Phase Matching Quantum Key Distribution. Phys. Rev. X 8(3), 31-43 (2018)