Vol 18 No 1, January 2009
1674-1056/2009/18(01)/0046-05

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

The queueing model for quantum key distribution network*

Wen Hao(温 浩)[a], Han Zheng-Fu(韩正甫)[a]†,
Guo Guang-Can(郭光灿)[a], and Hong Pei-Lin(洪佩琳)[b]

[a] *Quantum Information Key Laboratory, University of Science & Technology of China, Hefei* 230026, *China*
[b] *Information Network Laboratory, University of Science & Technology of China, Hefei* 230027, *China*

(Received 29 May 2008; revised manuscript received 18 June 2008)

This paper develops a QKD (quantum key distribution)-based queueing model to investigate the data delay on QKD link and network, especially that based on trusted relays. It shows the mean packet delay performance of the QKD system. Furthermore, it proposes a key buffering policy which could effectively improve the delay performance in practice. The results will be helpful for quality of service in practical QKD systems.

Keywords: quantum key distribution, quantum cryptography, quantum network, queueing model
PACC: 0367

1. Introduction

Quantum key distribution (QKD) is the scheme providing two users, Alice and Bob at distinct locations, with on-demand secure sequence of random bits (key). Based on physical laws instead of mathematical complexities, quantum communication with perfect secrecy could be guaranteed over an insecure public channel. Therefore technological advances, such as enhanced computational power, should not affect the security of quantum cryptography. The Bennett–Brassard 1984 (BB84) protocol[1] and other protocols,[2] have been widely used in short distance experiments[3,4] and commercial applications.[5]

In QKD-based applications, there exist data flow's time delay since the secure key generation cannot always fulfil the encryption demands. Delay performance is discussed extensively in classical communication, especially packets-switching network, such as internet based on TCP/IP protocols. It relates to the quality of service (QoS) of QKD systems. Here we introduce this concept to QKD applications to improve the data packets delay performance of QKD systems. Combining two different fields, quantum cryptography, and communication (in particular, networking engineering), we have made an effort to adopt a language understandable by both and finally obtain the creative results. The remains of this paper are organized as follows: in Section 2 we develop the queueing model from single QKD link, and this result is easily extended to QKD network based on trusted relays in Section 3. In Section 4 we propose the key prebuffering policy which could effectively improve the delay performance of practical QKD systems. Finally conclusions are given in Section 5.

2. Single QKD link queueing model

A single QKD link is depicted as shown in Fig.1.

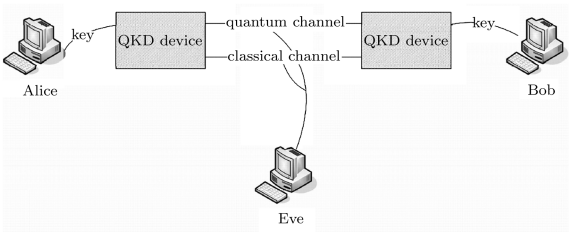


Fig.1. Scheme of a single QKD link.

Two communication channels are needed, one is the classical channel to transmit encrypted data and communicate QKD protocols, the other one is the quantum channel to distribute the quantum signals. Eve can eavesdrop on both channels, but attacks

*Project supported by National Fundamental Research Program of China (Grant No 2006CB921900), National Natural Science Foundation of China (Grant Nos 60537020 and 60621064) and Knowledge Innovation Project of Chinese Academy of Sciences.
†Corresponding author. E-mail: zfhan@ustc.edu.cn

on the quantum channel will inevitably bring more QBER (quantum bit error rate) and so exposure.

In the classical channel, data is encrypted by the One-Time-Pad (OTP) encryption algorithm,[6] which needs QKD's secure key as long as the data length. It seems that the quantum channel serves the classical data in the QKD process. This framework is similar to the classical communication process, in which the communication system (such as network router) serves the data flow (see Fig.2). To achieve a better QoS in such a system,

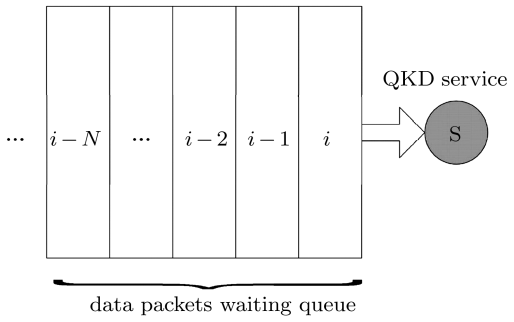


Fig.2. QKD service for data packets.

the data delay performance caused by the server's capability (such as bandwidth) is usually analysed. Before we start in the QKD environment, some assumptions are given as follows:

(i) The sifted key generation rate is depicted by the function[7]

$$K = \frac{1}{2} q f_{\text{req}} t_{\text{link}} \mu \eta, \tag{1}$$

where the 0.5 factor is the protocol loss (for BB84), q is (typically 1/2) the noninterfering path loss in some phase-coding setups,[3] f_{rep} is the repetition frequency of pulses, t_{link} is the transmission coefficient (the probability that a photon sent by Alice and received by one of Bob's detectors), μ is the mean number of photons per pulse, and η is the detector's efficiency, typically 10% for InGaAs detector. Thus for a given distance and given setup, the K is almost constant, which can be viewed as the bandwidth of a single QKD link.

(ii) The data needed to be encrypted is gathered as a packet form, and the process of packets arrival is Poisson process, which means a totally stochastic process. This assumption is naturally and widely used in the classical network model.

(iii) The data packet's length is considered as an exponential distribution.

(iv) Data encryption is considered as a very fast process so that the time spared on it is rather small, and we can just ignore it.

2.1. The service process

Let us start by introducing the random variable Q_n, which denotes the nth packet's length. According to assumption (iii), this variable has the exponential distribution, that is, the probability of nth packet's length is

$$p(Q_n) = \beta \mathrm{e}^{-\beta Q_n}, \tag{2}$$

where the constant

$$\beta = \frac{1}{\overline{Q}} \tag{3}$$

is the reciprocal of mean packet's length. Because OTP needs that the key's length is as long as data packet's length, the corresponding probability of key's length is identical. Then the time of key's generation(service time) is defined as

$$S_n = \frac{Q_n}{K}, \tag{4}$$

which also fulfills the exponential distribution:

$$p(S_n) = \mu \mathrm{e}^{-\mu S_n}, \tag{5}$$

where the constant

$$\mu = \frac{1}{\overline{S}} = \frac{K}{\overline{Q}} \tag{6}$$

is service rate (a reciprocal of mean service time), representing the mean frequency of service done in unit time.

2.2. The arrival process

$A(t)$ denotes the arrived data packet's number at time point t. This is a stochastic process, typically Poisson process, which means that, between time points $t+\tau$ and t, the probability of n packets arriving is

$$p(A(t+\tau) - A(t) = n) = \mathrm{e}^{-\lambda\tau} \frac{(\lambda\tau)^n}{n!}, \tag{7}$$

where λ is the arrival rate, representing the mean number of arrival in unit time. The arrival process is independent from the service process.

2.3. The mean time delay of data packets

By combining the service process and arrival process, we can obtain a typical M/M/1 queueing model,[8] where the first letter denotes the form of

the inter-arrival time distribution, which is Poisson process, the second letter denotes the form of the service-time distribution, which is the exponential distribution, and the third value denotes the number of servers, for single quantum channel, that is one.

Define that $\rho = \dfrac{\lambda}{\mu}$ is the load of queue, which means the load level of a queue. In general, it should be less than 1, which is sustainable for the system. Otherwise, the number of users in system will become infinite along with the increase of time. From M/M/1 model, we know that mean packet's delay equals mean service time plus mean waiting time:

$$\bar{T_{\rm d}} = \bar{S} + W. \tag{8}$$

According to the well-known Little theorem,[9] the mean number of packets in system (the sum of packets waiting and served) is the product of arrival rate and mean packet's delay:

$$\bar{N} = \lambda \bar{T_{\rm d}} = \frac{\lambda}{\mu} + \lambda W, \tag{9}$$

the waiting queue length is

$$N_{\rm Q} = \lambda W. \tag{10}$$

It is important to calculate the mean waiting time of packets W. We consider it as follows.

When the ith packet arrives, the packet being served has the residual service time R_i, and the queue has N_i waiting packets. Let S_l be the lth packet's service time, then the ith packet's waiting time is

$$W_i = R_i + \sum_{l=i-N_i}^{i-1} S_l, \tag{11}$$

$$\begin{aligned} \bar{W_i} &= E\{R_i\} + E\left\{\sum_{l=i-N_i}^{i-1} S_l\right\} \\ &= E\{R_i\} + \bar{S}E\{N_i\}, \end{aligned} \tag{12}$$

$$\begin{aligned} W &= \lim_{i\to\infty} \bar{W_i} = R + \bar{S}N_Q \\ &= R + \frac{1}{\mu}\lambda W = R + \rho W, \end{aligned} \tag{13}$$

where $R = \lim\limits_{i\to\infty} E\{R_i\}$, $N_{\rm Q} = E\{N_i\}$, $\rho = \dfrac{\lambda}{\mu}$.

So we can obtain

$$W = \frac{R}{1-\rho}, \tag{14}$$

and the question is, how can we compute the mean residual service time R? Suppose system is ergodic and has stable analytic result. Figure 3 depicts the residual service time $r(\tau)$. Let t be the time when $r(t) = 0$, then mean residual service time on $[0, t]$ is

$$\begin{aligned} R_t &= \frac{1}{t}\int_0^t r(\tau){\rm d}\tau = \frac{1}{t}\sum_{i=1}^{M(t)} \frac{1}{2}S_i^2 \\ &= \frac{1}{2}\frac{M(t)}{t}\frac{\sum_{i=1}^{M(t)} S_i^2}{M(t)}, \end{aligned} \tag{15}$$

where $M(t)$ denotes the number of packets that have been served on $[0, t]$.

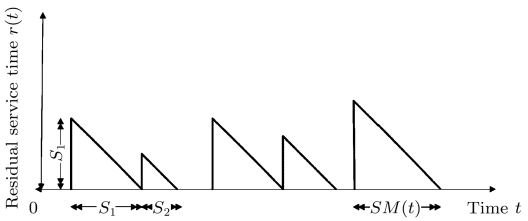


Fig.3. Residual service time curve.

Let $t \to \infty$, then

$$R = \frac{1}{2}\lambda \bar{S^2}, \tag{16}$$

and we know

$$\bar{S^2} = \frac{2}{\mu^2}. \tag{17}$$

From Eqs.(14), (16), (17), we obtain

$$W = \frac{\lambda \bar{S^2}}{2(1-\rho)} = \frac{\rho}{\mu(1-\rho)}, \tag{18}$$

thus

$$\bar{T_{\rm d}} = \bar{S} + W = \frac{1}{\mu} + \frac{\rho}{\mu(1-\rho)} = \frac{1}{\mu-\lambda}. \tag{19}$$

This result is the same as the classical one. We calculate the mean packet's delay performance (see Fig.4.) under the conditions listed in Table 1.

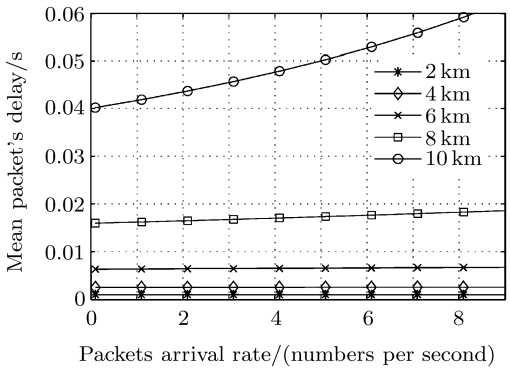


Fig.4. The mean packet's delay performance.

Table 1. Parameters' values by calculations.

parameters	values
pulse repetition frequency (f_{rep})	100 MHz
detector quantum efficiency (η)	10%
mean photon number per pulse (μ)	0.1
fibre loss coefficient (α)	0.2dB/km@1550nm
mean packet's length ($\bar{Q}$)	100bits

Key generation rate K is determined by the function (1). It is obvious that mean packet's delay will increase along with mean packet's length, the packet arrival rate and the transmission distance.

3. QKD network queueing model

3.1. QKD networks based on trusted relays

QKD, despite of its promising security against traditional schemes, has however several limitations, most prominently, throughput and range. To overcome the distance limitations, one can use a chain of QKD trusted relays, which can build QKD network.[10] A QKD trusted relay is not a quantum repeater,[11] it is a terminal that establishes a QKD link with the previous element of the chain and another with the following elements. By the trusted relays chained with QKD links, the end-to-end key will establish with OTP (XOR operation) encryption within each node (see Fig.5).

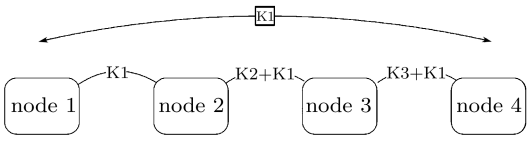


Fig.5. Hop by hop key relay scheme.

The roles of node are as follows:

(i) Node 1 establishes an encrypted communication, a QKD link, with node 2. Thus they share secure key K1.

(ii) Node 2 also establishes a QKD link and shares K2 with node 3. K2 is as long as K1.

(iii) Node 2 uses OTP encryption with K2 to transport K1, and node 3 gets the K1.

(iv) Node 3 does the same with node 4.

(v) Finally node 1 will share K1 with node 4. Key relay process is successful.

It is obvious that all the nodes should be trusted since they all know the global key, which may become a security loophole. Nevertheless, the trusted relay network is still attractive and practical. In 2008, SECOQC will show their trusted relay based QKD network in Vienna.[12]

3.2. Network queueing model

We can easily extend the single link's queueing model to the network queueing model. According to the Kleinrock Independency Approximation,[13] if packets' number in each link is huge, the arrival interval is less dependent from the service interval of last queue, then we can use M/M/1 model to describe each link. It should be mentioned that this result is only suitable for middle or heavy load ($\rho \to 1$) networks.

The mean number of packets in Link(i, j) is

$$N_{ij} = \frac{\lambda_{ij}}{\mu_{ij} - \lambda_{ij}}. \tag{20}$$

The mean number of packets in network is

$$N = \sum_{(i,j)} \frac{\lambda_{ij}}{\mu_{ij} - \lambda_{ij}}. \tag{21}$$

The mean packets delay is $T = \dfrac{N}{\gamma}$, where γ is the system total arrival rate.

4. Key pre-buffer policy

We have shown the queueing model from the classical data processing view. But QKD service has different characteristics, that is, the quantum channel is independent of the classical channel. The secure key generated by the quantum channel can be generated at any time, not just at the time when data packets arrive. This policy could make use of the bandwidth of quantum channel maximally.

Assuming that the packet's arrival process is still a Poisson process with parameter λ, we find that the data packet's length still fulfils the exponential distribution with parameter β. The system initial key amount is Q_0. When any packet arrives, it can be served instantly without waiting time and service time if it needs key less than the residual amount of key buffer, otherwise it must wait for enough key. A secure key can be also generated at spare time when the system has no data packets until the buffer is full.

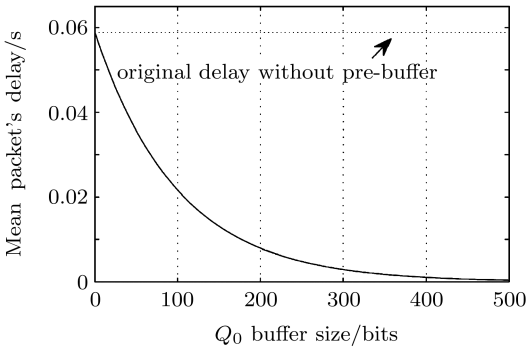


Fig.6. Improved delay performance with pre-buffering policy.

It is difficult to give an analytic function of the mean packet's delay in this situation. If a packet's length is larger than the buffer size, then it must wait. The probability of these 'large' packets is

$$P(Q_i > Q_0) = \int_{Q_0}^{\infty} \beta \mathrm{e}^{-\beta Q} \mathrm{d}Q = \mathrm{e}^{-\beta Q_0}, \qquad (22)$$

thus

$$\bar{T}_{\mathrm{d}}(Q_0) \leq P(Q_i > Q_0)\bar{T}_{\mathrm{d}}(0) = \mathrm{e}^{-\beta Q_0}\bar{T}_{\mathrm{d}}(0). \qquad (23)$$

It is obvious from Fig.6 that the delay will decrease as the buffer size increases. If $Q_0 \to \infty$, then the mean delay decreases close to zero. But a larger buffer will bring more cost. In practice, it will be a balance between the packet's delay and buffer size.

5. Conclusions

Efforts should be made to improve QKD application's service. We have proposed a queueing model both for QKD link and network to consider the data packet delay problem, which relates to the QKD application's QoS. Assuming the data packet's length distribution and the arrival process, we can obtain the mean packet's delay from the M/M/1 model. However, quantum channel may operate independently from classical channel. We give the key pre-buffer policy to improve the delay performance. It will be helpful for practical QKD system.

Acknowledgments

We thank Zhao Yi-Bo and Chen Wei for helpful discussions.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing* Bangalore, India p175

[2] Xia Y and Song H S 2007 *Phys. Lett.* A **364** 117

[3] Han Z F, Mo X F, Gui Y Z and Guo G C 2005 *Appl. Phys. Lett.* **86**(22) 221103

[4] Peng C Z, Zhang J, Yang D, Gao W B, Ma H X, Yin H, Zeng H P, Yang T, Wang X B and Pan J W 2007 *Phys. Rev. Lett.* **98** 010505

[5] http://www.magiqtech.com
http://www.idquantique.com
http://www.qinetiq.com

[6] Vernam G S 1926 *J. American Institute of Electrical Engineers* **45** 109

[7] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[8] Kleinrock L 1975 *Queueing Systems* Vol. I: *Theory* (New York: Wiley)

[9] Little J D C 1961 *Oper. Res.* **9** 383

[10] Elliott C 2002 *New J. Phys.* **4** 46.1

[11] Cirac J I, Zoller P, Kimble H J and Mabuchi H 1997 *Phys. Rev. Lett.* **78** 3221

[12] Poppe A, Peev M and Maurhart O 2008 arXiv/quant-ph:0804.0122

[13] Kleinrock L and Gail R 1996 *Queueing Systems: Problems and Solutions* (New York: Wiley)