doi:10.3788/gzxb20144307.0706009

用于可信任中继量子密钥分配网络的差异化服务提供机制

孙咏梅,程先柱,纪越峰

(北京邮电大学 信息与通信工程学院 信息光子学与光通信国家重点实验室,北京 100876)

摘 要:为了向用户提供差异化的密钥服务,研究了配备密钥池的可信任量子密钥分配网络.首先,理论分析了数据包时延和密钥池的关系,给出了具体关系式,指出带有密钥池缓存功能的量子密钥分配网络的平均数据包时延与密钥产生速率、密钥池的初始密钥长度、以及数据包的平均长度、到达时间和到达率密切相关.对比理论分析和软件仿真结果,验证了时延分析的正确性.其次,将密钥提供服务分为三类:保证提供型、优先提供型和尽力提供型,并提出了相应的技术实现方案,即提前预约、逐跳插队和逐跳排队;最后,仿真结果表明差异化密钥服务提供机制是有效的.

关键词:量子密钥分配; 差异化服务提供; 提前预约; 逐跳插队;逐跳排队

中图分类号:TN918.91 **文献标识码**:A **文章编号**:1004-4213(2014)07-0706009-5

A Differentialized Service Providing Scheme on Trusted Relay Quantum Key Distribution Networks

SUN Yong-mei, CHENG Xian-zhu, JI Yue-feng

(*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract: In order to provide different quantum key service, trusted relay quantum key distribution networks with quantum key pool was studied. Firstly, relationship between packet delay and quantum key pool was analyzed. The formula was given, which showed that the mean packet delay is related to the quantum key generation rate, the initial length of quantum key, the mean length, arrival time and arrival rate of packets. The theory and simulation results verified the accuracy of the delay analysis. Next, the key providing service was classified into three types: guaranteed, prioritized and best-effort key service. Correspondingly, pre-reserving, hop-by-hop jumping-queue and hop-by-hop queuing approaches were presented to realize the above differentialized key services. Finally, simulation results verified the efficiency of the differentialized service providing scheme.

Key words: Quantum key distribution; Differentialized service providing; Pre-reserving; Hop-by-hop jumping-queue; Hop-by-hop queuing

OCIS Codes: 270.5565; 270.5568; 060.0060; 060.4250; 060.5565

0 Introduction

With the rapid development of communication, information, computing and networking technologies, information security is becoming more and more important. Among all the existing encryption methods, only One Time Pad (OTP) has been proven to be information-theoretically secure. For OTP, the key should be as long as the message to be encrypted and be discarded after it is used once. However, the efficient distribution of such long keys is still an open issue. Quantum Key Distribution (QKD) is considered as a

Foundation item: Key Program of National Natural Science Foundation of China (No. 61331008)

First author(Contact author): SUN Yong-mei (1971—), female, associate professor, Ph. D degree, mainly focuses on optical switching and optical networking. Email:ymsun@bupt.edu.cn

Received: Oct. 23, 2013; **Accepted**: Jan. 8, 2014

promising technology to distribute key for OTP over an optical network. It can distribute key securely and detect any eavesdropping between two registered users, which is ensured by physical laws. Therefore, the combination of QKD and OTP can provide unconditionally secure communication.

QKD has been attracting more and more attention since the famous key distribution protocol, i. e. , BB84 protocol, was proposed in 1984[1]. Point-to-point QKD system has notably progressed, especially on extending the transmission distance and increasing the key generation rate. In the past decade, multi-user QKD networks have been extensively investigated in field environments, e. g. , the Defense Advanced Research Projects Agency (DARPA) Quantum Network in US[2], the Secure Communication using Quantum Cryptography (SECOQC) Quantum Network in Europe[3], the Tokyo QKD Network in Japan[4] and the metropolitan Quantum Cryptograph Network in China[5-7].

In the future, QKD network should be developed to support anybody-to-anybody key distribution at arbitrary distance. Optical switching technology can realize key distribution for many users with less complexity of key management, and trusted relay technology can realize key distribution on long distance[8-9]. However, to realize wider application of QKD and OTP, the great gap between the key generation rate and key request rate must be conquered. Although the potential for key generation rate of 1. 85 Mbit/s over more than 100 km of fiber has been reported[10], the typical secure key rate is a few kbps in the field metropolitan QKD networks[2-7,11]. A concept of pre-buffer was proposed to improve the delay performance[12], but there is no further study on it. Under such conditions, providing differentialized key service becomes necessary and important[13].

This paper focuses on trusted relay QKD networks with quantum key pool which is used to pre-buffer quantum keys for applications. Aiming to provide various secure applications using QKD and OTP in the future, we firstly analyze the relationship between packet delay and quantum key pool, which is a useful reference during the design and evaluation of service providing approach. Then, we classify the key providing service into three types: guaranteed, prioritized and best-effort key service. Correspondingly, pre-reserving, hop-by-hop jumping-queue and hop-by-hop queuing approaches are presented to provide the above differentialized key services. Finally, simulation results verify the accuracy of the delay analysis and the efficiency of the differentialized service providing scheme.

1 Trusted relay QKD networks

There are two kinds of traditional cryptography: symmetric and asymmetric key cryptography. Since the key distribution is extremely difficult for the former one, the latter one, also named public-key cryptography, is widely used. However, its security depends on the difficulty of solving mathematical problems in a finite time. Such computational security is facing challenge from the advances on computing technology.

QKD has physical security ensured by three physical laws: wave function collapse, Heisenberg′s uncertainty principle and non-cloning theorem. In point-to-point QKD system, two registered users, Alice and Bob, are connected by the QKD links: one quantum channel and one classical channel. Firstly, Alice generates a sequence of random bit and modulates it into a sequence of non-orthogonal quantum state by using randomly chosen basis, the sequence of quantum state is sent over the quantum channel in the form of single-photon transmission. Upon the reception of single photons, Bob measures the quantum state with also randomly chosen basis, which will be informed to Alice over the classical channel. Alice tells Bob which basis is right, then they establish the unconditionally secure key by keeping the bits measured by the right basis. If there is eavesdropping, the low correlation statistics result will imply that the key should be discarded.

Due to the attenuation induced by optical fiber or/and the low distribution efficiency, the maximum span of quantum channel is limited. On the other hand, optical amplifier is forbidden on quantum channel because of the perturbation to quantum states, and quantum repeater based on entanglement quantum is still at exploratory stage. To conquer the limit of the transmission distance, trusted relay was introduced to QKD networks where quantum keys are shared between each pair of adjacent nodes (ones directly connected by quantum channel)[8]. As shown in Fig. 1, the distance between any adjacent nodes is short enough, hence K_i ($i=1$, 2, 3) shared by adjacent nodes is quantum key. The key between nonadjacent node 0 and node 3 is called logical key K. K is encrypted into $K \oplus K_i$, which is transmitted from node $i-1$ to node i on classical channel. Each trusted relay node i gets K by K_i shared with upstream node $i-1$; then encrypts K into $K \oplus K_{i+1}$ by K_{i+1} shared with downstream node $i+1$. Node 3 gets the logical key K finally. To ensure the security of logical key, OTP should be used and the trusted relay nodes must be located in an absolutely safe place.

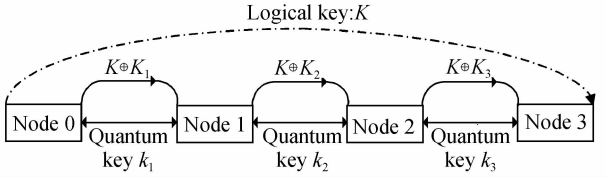

Fig. 1 Principle of key distribution on trusted relay QKD networks

2 Analysis of delay on QKD networks with quantum key pool

As mentioned in Section 0, there is a great gap between the key generation rate and key request rate for secure communication using QKD and OTP. It makes differentialized service providing necessary and important. The concept of quantum key pool can improve the delay performance of key providing service. Therefore, we firstly analyze the mean packet delay on QKD networks.

2.1 Queuing model

In QKD networks, each node has one or more quantum key pools to store quantum key generated at any time between itself and adjacent nodes. On each node, an arrival packet queues up for being encrypted using OTP method. The packet delay consists of waiting time and servicing time. Servicing time means the generation time of insufficient quantum keys. The assumptions for such queuing model are as follows: 1) The quantum key generation rate is constant; 2) There is no upper limit for quantum key pool, which means it can store infinite quantum keys; 3) The arrival of data packets obeys Poisson distribution, the length of data packets obeys exponential distribution; 4) Since OTP method is used, the length of quantum key consumed is as long as that of the data packet to be encrypted; 5) The time consumed by encryption and classical communication are short enough to be neglected.

2.2 Delay analysis

The parameters used for analysis are listed in Table. 1.

Table 1 Parameters for delay analysis

Parameter	Description
P	The mean length of data packets
λ	The arrival rate of data packets
R	The quantum key generation rate
t	Time point t from the initial time
p_i	The length of the ith data packet
Q_0	The initial length of key in quantum key pool at initial time
$Q(t)$	The length of key in quantum key pool at time point t
S_i	Servicing time of the ith data packet
W_i	Waiting time of the ith data packet
t_i	Delay of the ith data packet

By derivation and analysis, we get the mean delay for the $(i+1)$th data packet which arrives at time point t as follows.

$$E(t)=S(t)+W(t)=\int_{-(Q_0+Rt)}^{0} f(y)\frac{P}{R}e^{y(t)/P}dy+\int_{0}^{\infty} f(y)\frac{P+y(t)}{R}dy \quad (1)$$

The servicing time and waiting time can be expressed respectively as Eq. (2) and (3).

$$S(t)=\frac{P}{R}\int_{-(Q_0+Rt)}^{0} f(y)e^{y(t)/P}dy+\frac{P}{R}\int_{0}^{\infty} f(y)dy \quad (2)$$

$$W(t)=\int_{0}^{\infty} f(y)\frac{y(t)}{R}dy \quad (3)$$

where $y(t)$ is defined to denote the gap between the sum length of arrival data packets $x(t)$ and the length of quantum key generated by time point t as follows.

$$y(t)=x(t)-(Q_0+Rt) \quad (4)$$

And $f(y)$ is probability density function of $y(t)$ as follows.

$$f(y)=e^{-\lambda t}e^{-y+Q_0+Rt/P}\sum_{k=1}^{\infty}\frac{(\lambda t)^k(y+Q_0+Rt)^{k-1}}{P^k(k-1)!\ k!},\quad y\in(-(Q_0+Rt),\infty) \quad (5)$$

From the above formulae, we can observe that the mean packet delay is related to the arrival rate, arrival time point and mean length of data packets, the quantum key generation rate, and the initial length of quantum key.

The comparison between the theoretical results and simulation results is shown in Fig. 2, in which λ changes from 0.5 to 2 with $Q_0=0$, $p=1$ and $R=1$. Theoretical and simulation results are very similar.

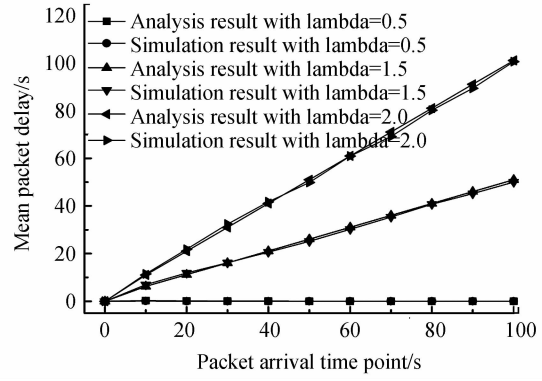

Fig. 2 Mean packet delay vs. packet arrival time point

Fig. 3 shows the mean delay of data packets which arrive at time point 10 s versus different initial length of key in quantum key pool. With the increase of initial length of key, the mean packet delay decreases obviously. The higher packet arrival rate is, the longer initial length of key should be.

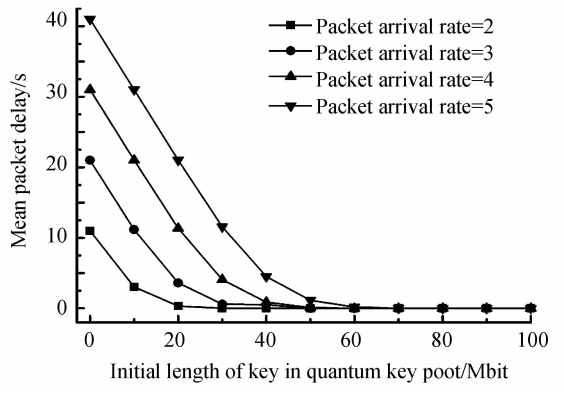

Fig. 3 Mean packet delay vs. the initial length of quantum key

3 Differentialized key service providing scheme

Unlike the reusable network resources, e. g., wavelength and fiber, key must be discarded once has been used according to the requirement of OTP. On the other hand, the quantum key generation rate is severely inadequate compared with the demand of many applications. Therefore, it is important to study how to provide different key services considering the characteristics of key and applications.

Various applications have different requirements, like low delay or/and high reliability. We propose three types of key service to meet the different requirements of applications, i. e., guaranteed, prioritized and best-effort key service. Here, the key means quantum key for adjacent nodes, and logical key for nonadjacent nodes on trusted relay QKD networks with quantum key pool. Key Distribution Time (T_{dist}), defined as the total processing time of key distribution from source node to destination node, is used as the evaluation metric.

3.1 Guaranteed key service

Guaranteed Key Service (GKS) is designed for the applications that have the highest priority on key distribution time and reliability.

To ensure the highest priority of GKS, we design a pre-reserving approach to provide key source. On receiving the key distribution request, a request massage is sent out from the source node to the destination node through the relay nodes. Each node checks the status of quantum key pool and reserves required amount of quantum keys. After that, logical key will be transmitted from source node to destination node as described in Section 1. Fig. 4 shows the principle of GKS provision, the length of key in quantum key pools always keeps same between two adjacent nodes. In this approach, the delay is mainly induced by generation of the insufficient quantum key, which occurs almost parallel on relay nodes. Therefore, T_{dist} of GKS can be expressed as the longest one of key processing times on each node, as analyzed in Section 2.

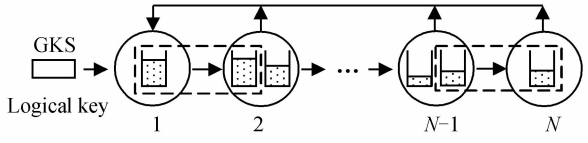

Fig. 4 Guranteed key service provision

In this approach, routing protocol can be adopted according to more detailed considerations. For example, route 1 has enough quantum keys which makes the delay lowest, but it must pass more relay nodes which makes more consumption of whole quantum keys. Route 2 has smallest number of relay nodes which makes lowest consumption of whole quantum keys, but it needs larger delay because there is no enough quantum key on some relay nodes. In QKD networks, stochastic routing is usually adopted for the purpose of hiding the routing information and decreasing the probability of being attacked. To guarantee the unconditional security in GKS provision, signaling information must be encrypted too. Fortunately, key consumption and reservation delay induced by signaling is not high.

3.2 Prioritized key service

Prioritized Key Service (PKS) is designed for the applications that can tolerate a reasonable time delay compared with the guaranteed key service.

To ensure the priority of PKS, we design a hop-by-hop jumping-queue approach to provide key source. In this approach, no quantum key is reserved in advance. Logical key is forwarded hop by hop and waits for quantum key on each relay node. Best-effort Key Service (BKS) adopts the same approach. However, PKS has the priority to jump the queue, which means PKS will be served ahead of BKS even if the logical key of PKS arrives later than that of BKS, as shown in Fig. 5. T_{dist} of PKS should be expressed as the sum of key processing times on each node.

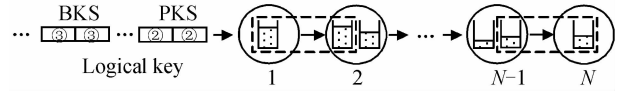

Fig. 5 Prioritized and best-effort key services provision

3.3 Best-effort key service

Best-effort Key Service (BKS) is designed for the applications that have the lowest priority. Generally, such applications are delay-insensitive.

BKS provision is similar as PKS, the difference is BKS does not have the priority to jump the queue, as shown in Fig. 5.

Note that, if the quantum key resource on a relay

node is sufficient for the logical key, the servicing time is 0, the delay is mainly the waiting time; otherwise the servicing time is the generation time of the insufficient quantum keys.

3.4 Simulation results

In simulation, we adopt network structure of CERNET while neglect the real distance between two adjacent nodes. The quantum key generation rate is 1.0 Mbit/s for any two adjacent nodes. Logical key request among nodes is evenly distributed, and request rates of three services are identical. For simplification, the shortest path is adopted.

Fig. 6 shows the simulation results of the above three services and Unified Key Service (UKS) where any key is treated in the same way. From this figure, we can verify the efficiency of the differentialized key service providing scheme. GKS has the shortest key distribution time; PKS is better than UKS when the key request rate is lower than 1.2 Mbit/s; while BKS has the longest key distribution time.

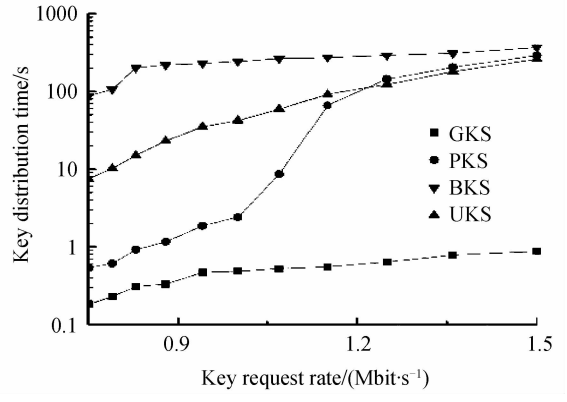

Fig. 6 Key distribution time vs. key request rate

4 Conclusions

This paper proposed a differentialized key service providing scheme for trusted relay QKD networks with quantum key pool. We analyzed the mean packet delay, indicated that it is related to characteristics of packets and quantum keys by formulae. Then, three types of key services and corresponding provision approaches were discussed. Simulation results showed the accuracy of delay analysis and the efficiency of differentialized key service providing scheme compared with unified key service. In the next works, scalability issue, further performance comparison of theory and simulation should be considered.

References

[1] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[C]. IEEE, 1984: 175-179.

[2] ELLIOTT C, COLVIN A, PEARSON D, *et al*. Current status of the DARPA quantum network[C]. SPIE, 2005, **5815**: 138-149.

[3] POPPE A, PEEV M, MAURHART O. Outline of the SECOQC quantum-key-distribution network in Vienna[J]. *International Journal of Quantum Information*, 2008, **6**(2): 209-218.

[4] SASAKI M, FUJIWARA M, ISHIZUKA H, *et al*. Field test of quantum key distribution in the Tokyo QKD network[J]. *Optics Express*, 2011, **19**(11): 10387-10409.

[5] CHEN Wei, HAN Zheng-fu, ZHANG Tao, *et al*. Field experiment on a "star type" metropolitan quantum key distribution network[J]. *IEEE Photonics Technology Letters*, 2009, **21**(9): 575-577.

[6] XU Fang-xing, CHEN Wei, WANG Shuang, *et al*. Field experiment on a robust hierarchical metropolitan quantum cryptography network[J]. *Chinese Science Bulletin*, 2009, **54**(17): 2991-2997.

[7] HAN Zheng-fu, XU Fang-xing, CHEN Wei, *et al*. An application-oriented hierarchical quantum cryptography network test bed[C]. IEEE, 2010.

[8] ELLIOT C. Building the quantum network[J]. *New Journal of Physics*, 2002, **4**(46): 1-12.

[9] MAEDA W, TANAKA A, TAKAHASHI S, *et al*. Technologies for quantum key distribution networks integrated with optical communication networks[J]. *IEEE Journal of Selected Topics in Quantum Electronics*, 2009, **15**(6): 1591-1601.

[10] DAULER E A, SPELLMEYER N W, KERMAN A J, *et al*. High-rate quantum key distribution with superconducting nanowire single photon detectors[C]. IEEE, 2010.

[11] SHIMIZU K, HONJO T, FUJIWARA M, *et al*. Performance of long-distance quantum key distribution over 90 km optical links installed in a field environment of Tokyo metropolitan area [J]. *IEEE Journal of Lightwave Technology*, 2014, **32**(1): 141-151.

[12] WEN Hao, HAN Zheng-fu, GUO Guang-can, *et al*. The queuing model for quantum key distribution network[J]. *Chinese Physics B*, 2009, **18**(1): 46-50.

[13] CHENG Xian-zhu, SUN Yong-mei, JI Yue-feng. A QoS-supported scheme for quantum key distribution[C]. IET, 2011: 220-224.