Multi-path based Quasi-real-time Quantum Key Distribution in Software Defined Quantum Key Distribution Networks (SD-QKDN)

Xiang Liu[1, 2], Xiaosong Yu[1], Yongli Zhao[1], Xiaotian Zhou[2], Shimulin Xie[3], Jincheng Li[3], Jie Zhang[1]

[1] State Key Laboratory of Information Photonics and Optical Communications, BUPT, Beijing, 100876, China
[2] Science and Technology on Communication Networks Laboratory, Heibei, 050081, China
[3] State Grid Info-Telecom Great Power Science and Technology Co., LTD., Fujian, 350003, China
E-mail: {xiaosongyu, yonglizhao, lgr24}@bupt.edu.cn

ABSTRACT

We propose a multi-path based quasi-real-time quantum key distribution scheme in software defined quantum key distribution networks (SD-QKDN). Simulation results show the proposed scheme performs well in terms of service successful probability and secret-key utilization.

Keywords: *quantum key distribution, quasi-real-time, multi-path, SD-QKDN*

1. INTRODUCTION

Quantum key distribution (QKD) [1,2] is a state-of-the-art technology of distributing information-theoretically secure secret keys based on the principles of quantum physics. It can ensure the unconditional security of encrypted communication between two nodes by combining one-time-pad (OTP) technology. Its combination with advanced encryption standard (AES) algorithm [3,4] is also much safer than other existing encryption methods. However, because of the insufficient generation rate of secret-key in current QKD networks, some studies have proposed the concept of quantum key pool (QKP) to improve the ability of the QKD networks to carry encrypted services [5]. However, the introducing of QKP also brings problems. Firstly, the QKP construction makes the secret-key resources form a unique feature of "gradual generation and accumulation, instantaneous occurrence of consumption". This will make QKD networks difficult to effectively respond to dynamic services; Secondly, there is different opinion on the storage of quantum keys. Some scholars believe that quantum keys should be used quickly after they are generated, and any attempt to store quantum keys will lead to the loss on its absolute security. The above two problems make it difficult to balance secret-key resource utilization, service successful probability and services security in the current QKD networks.

In this paper, a multi-path based quasi-real-time QKD scheme was proposed, which will distribute multiple sets of virtual quantum key pools (VQKPs) on multiple paths within a given secret-key security time limit. Unified control of network resources and splicing secret-key sequences can be achieved by introducing SDN technology [6, 7]. The simulation results show that the proposed scheme could achieve good performance in terms of service successful probability and secret-key utilization.

2. MULTI-PATH BASED QUASI-REAL-TIME QKD

Quasi-real-time QKD refers to using the quantum keys immediately after it is generated to ensure its absolute security. In this case, secret-key consumption and generation are coupled together, and the role of the QKP is to decouple the consumption and generation of the quantum keys. Note that constructing QKP of the QKD networks will of course sacrifice its security. However, the quasi-real-time QKD proposed in this paper means that the quantum keys can be absolutely secure during the available time after quantum keys are generated. These keys are only stored for a short time, and once they exceeds certain period, they will no longer be used in the highest level of encryption.

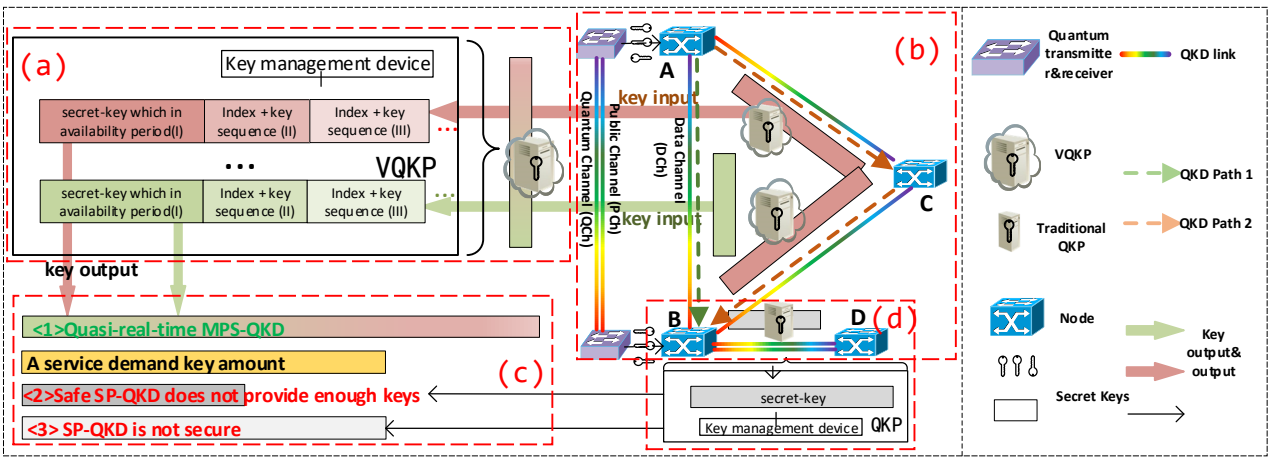

Fig. 1 The principle of multi-path based quasi-real-time QKD (a) logical structure of quasi-real-time VQKP based on multipath, (b) multi-path based quasi-real-time QKD, (c) an example of multi-path based quasi-real-time QKD and single-path based QKD, (d) the logical structure of traditional QKP.

978-1-7281-2764-4/19/$31.00 ©2019 IEEE

This paper proposes an VQKP logic structure to suit for the quasi-real-time QKD based on multi-path, as shown in Fig. 1(a). Unlike ordinary QKP in Fig. 1(d), each VQKP is divided into multiple virtual spaces, each virtual space stores secret-key resources from the corresponding secret-key path. The secret-key sequences in each secret-key space is divided and stored. the secret-key resources in (I) has a strict secret-key availability time limit, and it can provide the highest level of secure communication for the encryption services in combination with OTP encryption technology; The secret-key resources in (II) are transferred from a secret-key that is not used under the time limit in (I). The secret-key resources in (II) can combine with a traditional encryption algorithm (such as AES, etc.) to serve the next level of encrypted communication. If necessary, secret-key blocks of (III) or lower security levels can also be divided.

Fig. 1(b) is a schematic diagram of multi-path based quasi-real-time QKD. Fig. 1(c) shows the comparison of multi-path based quasi-real-time QKD scheme (*MPQ-QKD*) and single-path based QKD scheme (*SP-QKD*). We assume the secret-key generation capabilities of $link_{A\text{-}B}$ and $link_{B\text{-}D}$ are same. Compared with *SP-QKD*, *MPQ-QKD* can respond to the service (Fig.1(c)<1>), while the *SP-QKD* cannot respond to the service (Fig.1(c)<2>) if considering the security requirement. If secret keys with a long storage time to encrypt is used, the security requirements of the service cannot be guaranteed (Fig.1(c)<3>).

Fig. 2 is the workflow of multi-path based quasi-real-time QKD in SD-QKDN. Fig. 2(a) describes a typical SD-QKDN architecture while Fig. 2(b) shows its workflow. During *MPQ-QKD* operation, the quantum communication nodes (QCNs) will build multiple VQKPs between multiple alternate paths. The secret-key packages not only carry the QKD routing information, but also carry the path number label. After the QKD is completed, the verification of the secret-key sequences stitching is performed under the control of the control layer.

3. MATHEMATICAL MODEL OF *MPQ-QKD*

In this paper, Each QCNs in the SD-QKDN is denoted by $N=\{n_1, n_2, ..., n_n\}$, each QKD link is denoted by $E=\{e_1, e_2, ..., e_m\}$, $H=\{h_{e1}, h_{e2}, ..., h_{em}\}$ is used to indicate the number of relay hops on each QKD link and $V=\{v_1, v_2, ..., v_m\}$ is used to represents secret-key generation rate set for QKD links. p is used to represent the VQKP in SD-QKDN, $S=\{s_1, s_2, ...\}$ is the secret-key inventory in each VQKP. $r(s_r, d_r, k_r, t_r)$ for service request (s_r: source node of the service request, d_r: destination node of the service request, k_r: The number of service request secret keys). $I(t)$ for service whether it is responded, K represents the number of alternative paths, SP represents the successful probability of encrypt services, T_k represents the secret-key availability period, and E_k represents total amount of secret keys expired in VQKP. *KRU* means secret-key resources utilization.

$$M_{i,j} = (S(t)_{i,j}, \overline{V_{i,j}},) \quad (1)$$

$$k_r \le \sum_1^K S_{P_{s,d(n)}}(t_r) \quad (0 < n \le K) \quad (2)$$

$$M^C_{S_{i,j}}(t) = \sum_{0\le t<T} I(t) * R_{i,j}(t), (0 \le t < T) \quad (3)$$

$$M^V_{S_{i,j}}(t) = \int_0^t V(t)_{i,j} \; (0 \le t < T) \quad (4)$$

$$s_{P_{s,d(n)}}(t) = \min\left(s(t)_{s,m}, \dots s(t)_{p,d}\right), (e_{s,m}, \dots, e_{p,d} \in p_{s,d}) \quad (5)$$

$$KRU = \frac{\int_0^T [\sum_0^m (V_{i,j} * h_e - Ek_p - S_p)]}{\int_0^T \sum_0^m (V_{i,j} * h_e)} \quad (6)$$

Eq.(1) represents the secret-key resources state model in SD-QKDN. *Eq.(2)* indicates the condition when *I(t)* is true in Eq.(3), indicating that the service request can be responded. *Eq.(3)* and *Eq.(4)* represent the consumption and generation model of secret-key resources in SD-QKDN. *Eq.(5)* indicates the amount of secret keys that can be provided by a path in the SD-QKDN. *Eq.(6)* is the formula for calculating *KRU*.

In fact, *MPQ-QKD* is based on the *Yen's Algorithm* . *H* was used as weight in *Yen's Algorithm* to pre-processing the networks paths and then stored the results in the corresponding nodes. When determining whether the service request can be responded, multiple QKD paths will be selected to provide the secret keys at the same time. If the amount of secret keys is sufficient, the service can respond, otherwise the service cannot respond.

4. SIMULATION AND RESULTS

To compare the performances of *MPQ-QKD* and *SP-QKD*, we adopt *NSFNET* topology with 14 nodes and 21 bidirectional links for simulation. We set the maximum available distance from point to point QKD to 400 km [8], and the relay nodes setting are also based on it. The secret-key generation rate of each point-to-point QKD system has a certain negative correlation with its physical distance. The services request moment is subject to a negative exponential distribution (λ=5u,

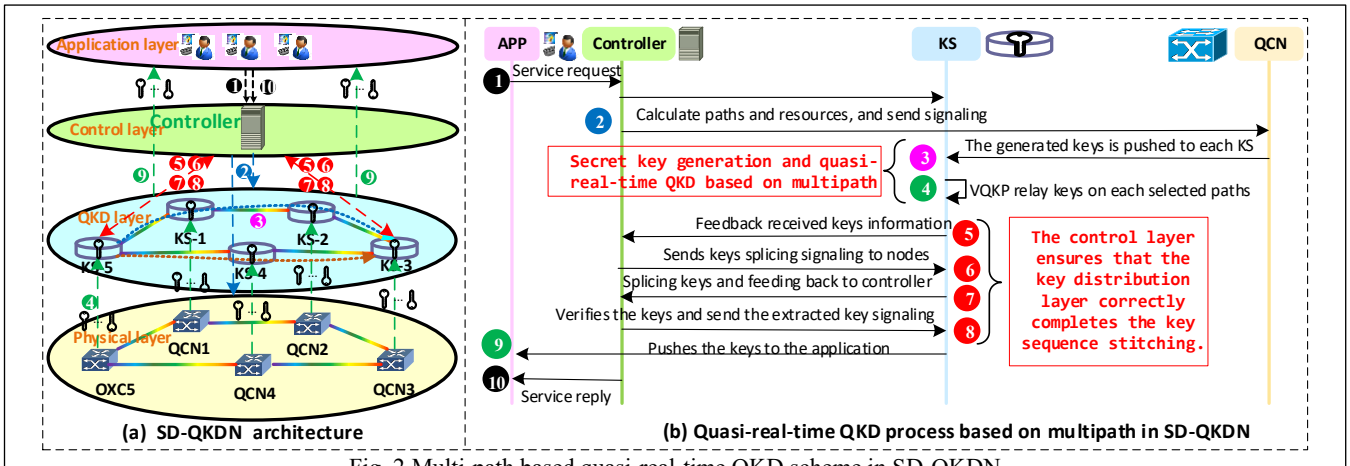

Fig. 2 Multi-path based quasi-real-time QKD scheme in SD-QKDN

978-1-7281-2764-4/19/$31.00 ©2019 IEEE

u is the smallest time unit in the simulation). We define the *service intensity* as the secret-key range required by the services (For example, if the *service intensity* is *500κ*, the secret keys range required for is *500±50κ*,κ is the smallest secret-key unit in the simulation). Select the alternative path *K=1/2/3/4*, select T_k*=100u/50u/30u*.

As can be seen from Figs. 3(a)(b)(c) where T_k*=100u/50u/30u*, as the *service intensity* increases, the *SP* of *SP-QKD* will be greatly reduced, while the *SP* of *MPQ-QKD* declines slowly. At the same time, the larger the candidate path *K*, the more obvious the effect. Figs. 3(a)(b)(c) also show the comparison where T_k*=100u/50u/30u*, respectively. The abscissa T_k in the figure gradually decreases, indicating that the safety requirements are constantly increasing. As the security requirements become more stringent, the *SP* of *SP-QKD* declines rapidly, while the *SP* of *MPQ-QKD* declines slowly, indicating that the performance of *MPQ-QKD* is much better than *SP-QKD*.

As can be seen from Fig. 3(d), when select T_k*=50u* to monitor the usage of secret-key resources, as the *service intensity* increases, the *KRU* increases. The reason is that if *service intensity* is too low, the secret-key requirement is much smaller than the secret-key supply. The generated secret keys were stored in the VQKP for a long time, exceeding the secret-key availability period. At the same time, it can be seen from the Fig. 3(d) that the *KRU* of *MPQ-QKD* is much higher than *SP-QKD*.

Figs. 3(e)(f) show the results under the condition that *service intensity* is *500κ*. As the security level and K change, the *SP* and *KRU* of the two scenarios change in the QKD networks. When the security requirements continue to increase, the *SP* of the *SP-QKD* drops significantly. While the *SP* of *MPQ-QKD* is slightly reduced, the performance is relatively stable. At the same time, as the value of *K* increases, *MPQ-QKD* is always better than *SP-QKD* and the advantage continues to expand. The integrated results show that *MPQ-QKD* can better satisfy the successful probability of the services and secret-key resources utilization of the services than *SP-QKD* with higher security requirements.

5. CONCLUSION

This paper proposes a multi-path based quasi-real-time QKD scheme in SD-QKDN. Simulation results demonstrate that the proposed scheme significantly outperforms single-path based QKD in terms of service successful probability and secret-key utilization.

Acknowledgement: This work is supported by NSFC project (61601052, 61571058), Fund of Science and Technology on Communication Networks Laboratory (6142104180405), Fund of State Key Laboratory of Information Photonics and Optical Communications, BUPT (IPOC2017ZT10), and the Fundamental Research Funds for the Central Universities (2018RC24).

6. REFERENCES

[1] H.-K. Lo et al., "Secure quantum key distribution," Nature Photon. 8(8), 595–604 2014.
[2] Q. Zhang et al., "Large scale quantum key distribution: challenges and solutions [Invited]," Opt. Express 26(18), 24260–24273 2018.
[3] P. Eraerds, et al., New J. Phys., vol. 12, no. 6, pp. 063027, 2010.
[4] P. Jouguet, et al., Opt. Express, vol. 20, no. 13, pp. 14030–14041, 2012.
[5] Y. Cao et al., "Time-scheduled quantum key distribution (QKD) over WDM networks," J. Lightwave Technol. 36(16), 3382–3395 2018.
[6] E. Hugues-Salas et al., Proc. OFC2018, paper M2A.6 2018.
[7] Y. Zhao et al., IEEE Commun. Mag. 56(8), 130–137 2018.
[8] https://www.idquantique.com/quantum-key-distribution-qkd-achieved-over-record-421-km

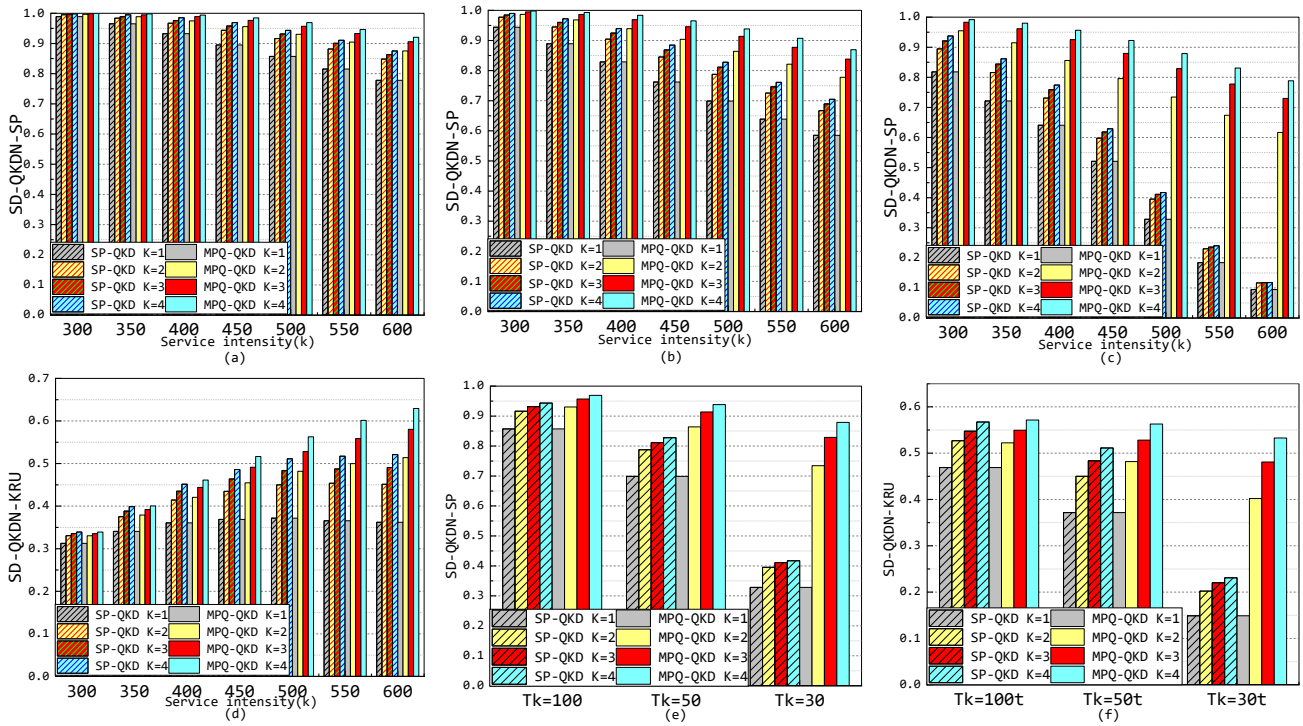

Fig. 3 Simulation results. (a) T_k = *100u SP*, (b) T_k = *50u SP*, (c) T_k = *30u SP*, (d) T_k = *50 KRU*, (e) *service intensity = 500κ SP*, (f) *service intensity =500κ KRU*

978-1-7281-2764-4/19/$31.00 ©2019 IEEE