Auxiliary Graph based QKD Key Provisioning for End-to-End Security Service in Optical Networks

Qingcheng Zhu[1], Xiaosong Yu[1,*], Yongli Zhao[1,*], Avishek Nag[2], Hua Wang[1], Liquan Chen[3], Jie Zhang[1]
[1]State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, 100876, China; [2]School of Electrical and Electronic Engineering, University College Dublin, Belfield, Dublin 4, D04 V1W8, Ireland; [3]School of Cyber Science and Engineering, Southeast University, Nanjing 211100, China.
**e-mail:{yonglizhao, xiaosongyu}@bupt.edu.cn*

Abstract: We propose a quantum-key-distribution (QKD) key provisioning scheme by applying auxiliary graph for end-to-end security service in optical networks. Simulation demonstrates the good performance in terms of security level and key provisioning latency. © 2022 The Author(s)

1. Introduction

Nowadays, numerous sensitive and confidential data is carried over optical networks and face security threats such as eavesdropping and jamming. It is essential to enhance end-to-end (E2E) service security, so as to reduce the threats by security attacks. Different from classical cryptography where security is based on the high complexity of the mathematical problem, quantum key distribution (QKD) provides information-theoretically secure (ITS) key distribution between two remote parties by applying the uncertainty principle and the no-cloning theorem of quantum mechanics [1]. Remarkable progress on practical QKD has been achieved in terms of secure key-rate improvement [2] and QKD networking [3,4]. However, limited by high costs of QKD systems and the required critical environment, large-scale QKD deployment for all users over optical networks is tough. A practical scenario is that parts of optical nodes and links are likely to be equipped with QKD modules and QKD links, while the other cannot. Because a large number of services in optical networks have E2E secure communication requirements, the challenge is how to provide enough QKD keys for E2E services securely under such practical scenario, especially for services in the network edge. In this paper, we propose a QKD-key-provisioning (QKPR) scheme for E2E security services over optical networks, where nodes and links are partially equipped with QKD modules and links. Simulations are conducted for demonstrating the performance of the scheme in terms of security level and key provisioning latency.

2. Network Model and Problem Statement

Due to the cost of QKD deployment, partial-QKD-deployment-based optical networks (pQKD-ONs) are likely to be more practical. The functional architecture of pQKD-ONs is in Fig. 1(a). Apart from traditional optical equipment (e.g., optical cross connect), a QKD node (QN) has a local key manager (LKM), key store (KS) and QKD transceiver (QKD Tx/Rx) for QKD key generation, storing, and management, respectively; whereas, an optical node (ON) has an LKM and a KS. QKD Tx/Rxs are interconnected by QKD links and LKMs are interconnected by key management (KM) links. A network has secure domains (SDs) where QKD keys can be distributed again. Secure links among SDs are guaranteed by secure technologies such as physical layer security. The pQKD-ON is denoted by $G_p=\{\boldsymbol{V_p}, \boldsymbol{E_p}\}$, where $\boldsymbol{V_p}$ is the set of physical nodes including QNs $\boldsymbol{V_Q}$ and ONs $\boldsymbol{V_{NQ}}$, $\boldsymbol{E_p}$ is the set of physical links, $e_{pi}(s_{pi},d_{pi},w_{pi})\in \boldsymbol{E_p}$, where s_{pi} and d_{pi} are the two vertices and w_{pi} is the weight of the link. The E2E service across SDs is denoted by $s_{E2E}(s, d, R_k)$, where s is source, d is destination and R_k is the required number of secure keys. A key pool (KP) [5] can be constructed between two nodes to manage keys (including key exchange, storage, assignment, and destruction).

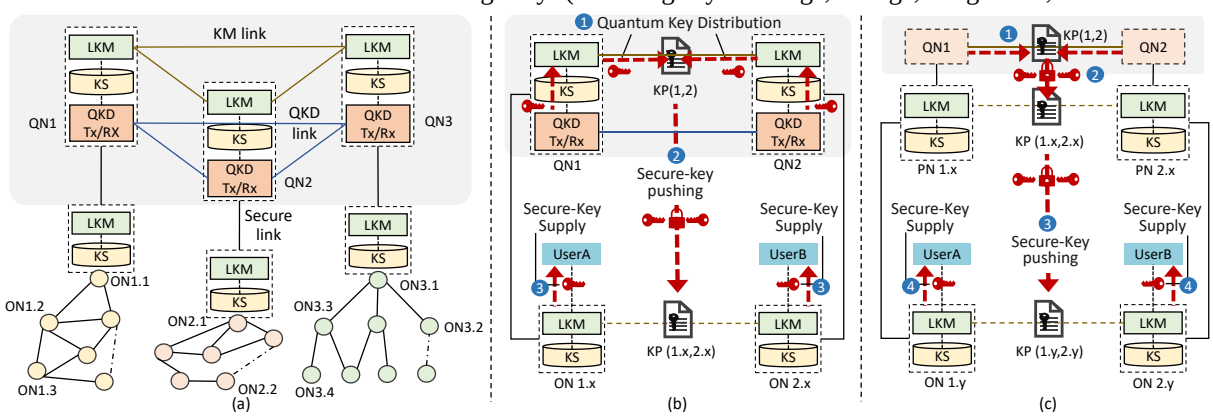

Fig. 1. (a) Functional architecture of pQKD-ONs; (b) *2*-level QKPR; (c) *3*-level QKPR.

In pQKD-ONs, to satisfy the key requirements of E2E services, the QKPR problem needs to be solved. A QKPR process has basic stages including QKD stage, secure-key pushing (SKP) stage, and secure-key supply (SKS) stage: **1) QKD stage** is to generate and manage QKD keys in KP between two QNs. **2) SKP stage** is to distribute secure keys from a KP to another KP within a SD securely. SKP before service arrival is referred as pre-SKP stage, and SKP after service arrival is aft-SKP stage. More pre-SKP stages will reduce service latency. **3) SKS stage** is to supply keys for E2E services from local KS. Two typical QKPR cases are shown in Figs. 1(b-c). Fig. 1(b) describes a *2*-level QKPR, where QKD keys are distributed twice including one QKD stage and one SKP stage before key supply for two users. Fig. 1(c) describes a *3*-level QKPR, where pre-key-store node (PN) $\boldsymbol{V_{PKS}}$ is enabled among ONs for pre-storing the pushed keys before service arrival, and QKD keys are distributed three times totally including one QKD stage and two SKP stages. In general, *N*-level QKPR contains one QKD stage and (*N-1*) SKP stages. Since that more SKP stages will reduce more security, N_1-level QKPR has higher security than N_2-level QKPR, $N_1<N_2$.

3. Auxiliary Graph based QKPR Scheme in pQKD-ONs

To solve QKPR problem for E2E services in pQKD-ONs, the auxiliary graph (AG) based QKPR scheme is designed, where AG is constructed to embody different basic key-provisioning stages according to the secure key requirement of the service and the key resource status of the network. By applying path calculation algorithms based on the AG, the QKPR scheme is derived. When s_{E2E} (s, d, R_k) arrives, the AG $G_v=\{\boldsymbol{V_v}, \boldsymbol{E_v}\}$ is constructed, where $\boldsymbol{V_v}=\{v_{v1},\ldots, v_{vi},\ldots,v_{v|\boldsymbol{V_v}|}\}$ is the set of vertices and $\boldsymbol{E_v}=\{e_{v1},\ldots, e_{vi},\ldots,e_{v|\boldsymbol{E_v}|}\}$ is the set of bi-directional edges. For $\boldsymbol{V_v}$, three types of vertices including QN, PN, and ON are generated corresponding to $\boldsymbol{V_p}$; For $\boldsymbol{E_v}$, three types of edges including QKD edge (QKDE), SKP edge (SKPE), and KP edge (KPE) are generated, which present QKD, aft-SKP and pre-SKP stages, respectively. An example of auxiliary graph is shown in Fig. 2 and the detailed procedures of AG-based EQKP algorithm is illustrated in Table 1. A QKDE between two QNs is added to $\boldsymbol{E_v}$ when the number *K* of keys in KP between the QNs is larger than R_k; A KPE between two PNs is added to $\boldsymbol{E_v}$ when the number *K* of keys in KP between the PNs is larger than R_k (*Lines 3-9*). Then, the shortest paths are calculated on G_p including $\boldsymbol{p_{PQ}}$ from each v_j, $v_j \in \boldsymbol{V_{PSK}}$ to each v_k, $v_k \in \boldsymbol{V_Q}$, the shortest paths $\boldsymbol{p_O}$ from *s* (*d*) to each v_k, $v_k \in \{\boldsymbol{V_Q} \cup \boldsymbol{V_{PSK}}\}$ in the SD $\boldsymbol{D_s}$ ($\boldsymbol{D_d}$) that *s* (*d*) belongs to. SKPEs are established according to edges on $\boldsymbol{p_{PQ}}$ and $\boldsymbol{p_O}$ and are added to $\boldsymbol{E_v}$. Hence, G_v can be constructed based on $\boldsymbol{E_v}$ and the related vertexes (*Lines 10-12*). Finally, the shortest paths $\boldsymbol{p_v}$ are calculated on G_v and the QKPR scheme is decided by $\boldsymbol{p_v}$. For example, the calculated $\boldsymbol{p_v}$ is shown using red bold arrows in Fig. 2. The corresponding strategy is that KP(*2*,*3*) between QN*2* and QN*3* push key-pairs to KP(*2.1*,*3.1*) between PN*2.1* and PN*3.1* firstly; PN*1.1* and PN*3.1* get the same keys by key relaying on PN*2.1* secondly; user A (ON*1.3*) and user B (ON*3.4*) of the service get the required keys through SKP finally. Let F_s denote the flag whether the service is success or failed. If $\boldsymbol{p_v}$ includes QKDE or KPE, keys in the corresponding physical nodes are provisioned according to $\boldsymbol{p_v}$ and F_s is marked as $SUCCEED$; otherwise, F_s is marked as $FAILED$.

The weight assignment for virtual edges in AG influences the calculated final paths $\boldsymbol{p_v}$. The weights of edges can be adjusted for different QKPR strategies. In the scenario with PN setting, **1) for QKPR considering maximal security level (*MSL*),** SKP from KPs between QNs is maximized where the weight of QKDE is smaller than KPE; **2) for QKPR considering minimal latency (*MLA*)**, SKP from KPs between PNs is maximized where the weight of KPE is not larger than QKDE; **3) for QKPR considering maximal key availability (*MKA*)**, key availability awareness is enabled where the weight of QKDE and KPE is set to be negatively correlated with the number of the keys stored in the KP. In the scenario without PN setting, QKPR is realized only by SKP from KPs between QNs, the strategy is referred as **QKPR without PNs (*WOP*)** where KPE doesn't exist in the constructed AG.

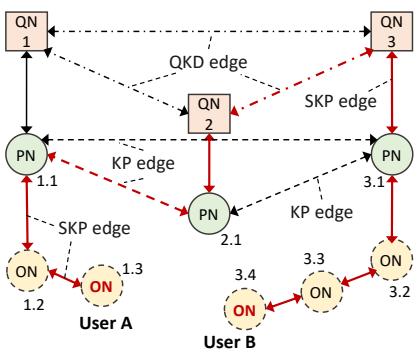

Fig. 2. Auxiliary graph.

Table 1. Procedures of QKPR scheme based on AG

QKPR Scheme based on Auxiliary Graph in pQKD-ONs			
Input: $s_{E2E}(s,d,R_k)$, $G_p(\boldsymbol{V_p},\boldsymbol{E_p})$,$\boldsymbol{V_Q}$,$\boldsymbol{V_{NQ}}$, $\boldsymbol{V_{PSK}}$;		**Output:** $\boldsymbol{p_v}$, $\boldsymbol{F_s}$.	
1	**For** each service $s_{E2E}(s,d,R_k)$ **then**	10	Calculate shortest paths $\boldsymbol{p_{PQ}}$ and $\boldsymbol{p_O}$ on G_p;
2	$G_v(\boldsymbol{V_v},\boldsymbol{E_v}) \leftarrow \emptyset$;	11	Add edges on $\boldsymbol{p_{PQ}}$ and $\boldsymbol{p_O}$ as SKPEs to $\boldsymbol{E_v}$;
3	**For** each $e_{pi}(s_{pi},d_{pi},w_{pi}) \in \boldsymbol{E_p}$ **then**	12	Construct $G_v(\boldsymbol{V_v},\boldsymbol{E_v})$ based on $\boldsymbol{E_v}$;
4	**If** $s_{pi},d_{pi} \in \boldsymbol{V_Q}$ **and** $K_{e_{pi}} \geq R_k$ **then**	13	Calculate the shortest paths $\boldsymbol{p_v}$ on G_v;
5	Add QKDE(s_{pi},d_{pi},w_Q) to $\boldsymbol{E_v}$;	14	**If** $\boldsymbol{p_v}$ includes QKDE/KPE **then**
6	**Else If** $s_{pi},d_{pi} \in \boldsymbol{V_{PSK}}$ **and** $K_{e_{pi}} \geq R_k$ **then**	15	QKPR and Mark $\boldsymbol{F_s} = SUCCEED$;
7	Add KPE(s_{pi},d_{pi},w_k) to $\boldsymbol{E_v}$;	16	**Else** Mark $\boldsymbol{F_s} = FAILED$;
8	**End If**	17	**End If**
9	**End For**	18	**End For**

4. Simulation Analysis

Simulations are conducted on a network topology in Fig. 3(a) to demonstrate the performances of the proposed QKPR strategies. Three QNs connect to three SDs with mesh, ring and tree topology and each SD has one PN. 10^5 services arrive dynamically, which follow Poisson process uniformly distributed among PNs and ONs across SDs. The number of the required keys is randomly generated in range of $[u_k,5u_k]$, where u_k is a key unit. *8* channels are set for QKD links and the average QKD key generation rate per link is $200u_k$ per time unit. The proportion ρ is the keys pre-distributed to KPs between PNs over the total keys generated between QNs in two SDs. The weights of QKPE, KPE and SKPE in AG are set for strategies: *MSL*$\{1,10,1\}$, *MLA*$\{10,1,1\}$, *MKA*$\{a/(b+K), a/(b+K),1\}$, *WOP*$\{1,\infty,1\}$, where a, b are constants and K is the number of the stored keys. To quantitively evaluate the QKPR security, we define security level to embody the negative correlation between security and the times of SKP and is calculated by $1-\sum_i \alpha_i c_i$, where α_i is the coefficient, c_i is the security reduction cost of the i^{th} stage in QKPR after service arrival. The key provisioning latency for a service is calculated mainly according to aft-SKP latency, and its unit is u_t.

Figs. 3(b-f) compares the performances of different strategies in terms of key consumption ratio R_{kc}, average security level SL_a, and average latency LA_a. The R_{kc} is the number of the consumed keys by services over the total number of the generated QKD keys. The SL_a (LA_a) is the sum of security levels (key provisioning latency) of services over the number of services. Fig. 3(b) is the R_{kc} versus traffic load when ρ=*0.5*. It can be seen that the R_{kc} of *MKA* is around *6*% (*225* Erlang) lower compared with *MSL* and *MLA*. The reason is that *MKA* is aware of the available keys. Figs. 3(c-d) are the SL_a and LA_a versus traffic load when $\rho = 0.5$. It shows that *MSL* has higher security level but higher key provisioning latency, while *MLA* has lower latency but lower security level. The reason is that the more *2*-level QKPR processes for services will increase both SL_a and LA_a. As for *WOP*, since it doesn't set PNs and all keys are stored in KP between QNs, R_{kc} are the minimized (*6*% lower than *MKA* at *225* Erlang) and the SL_a and LA_a are both the highest. Figs. 3(e-f) shows the SL_a and LA_a under different proportion ρ when the traffic load is *175* Erlang and *275* Erlang. When ρ increases, a larger part of the total generated QKD keys is distributed to KPs between PNs. The SL_a (LA_a) of *MLA* and *MKA* are *31*% (*75*%) and *27*% (*73*%) lower than *MSL* respectively at *175* Erlang when $\rho = 0.45$. The SL_a and LA_a performance differences of strategies are relatively large when ρ is *0.45* and *0.6*.

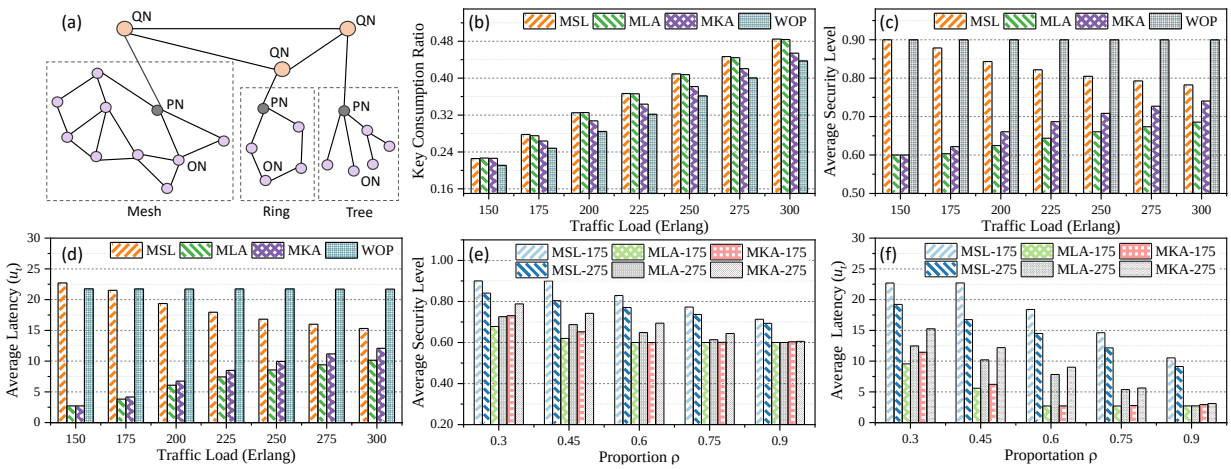

Fig. 3. (a) Network topology; Simulation results of (b) key consumption ratio versus traffic load ($\rho = 0.5$); (c) average security level versus traffic load ($\rho = 0.5$); (d) average latency versus traffic load ($\rho = 0.5$); (e) average security level versus proportion ρ; (f) average latency versus proportion ρ;

5. Conclusion

An optical network partially equipped with QKD modules and links is a practical scenario during QKD deployment. This paper presented a QKD key provisioning scheme for satisfying the E2E secure key requirements by constructing auxiliary graphs. The performance of the proposed scheme is demonstrated on security level and latency.

Acknowledgement: this work is supported by National Key Research and Development Program of China (2020YFE0200600), NSFC project (61971068, 61822105, 62021005), and BUPT Excellent Ph.D. Students Foundation (CX2021139).

6. References

[1] P. Kumavor *et al.*, "Comparison of four multi-user quantum key distribution schemes over passive optical networks," in *OFC*, Feb. 2004.
[2] Z. Yuan *et al.*, "10-Mb/s quantum key distribution," *J. Lightwave. Technol.*, 36(16), 3427-3433 (2018).
[3] Y. Chen *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature, 589(7841),214-219 (2021).
[4] Y. Zhao *et al.*, "Resource Allocation in Optical Networks Secured by Quantum Key Distribution," *IEEE Commun Mag*,56(8),130-137(2018).
[5] Y. Cao *et al.*, "Time-scheduled quantum key distribution (QKD) over WDM networks," *J. Lightwave Technol.*, 36(16), 3382–3395 (2018).