Routing and Key Allocation against Eavesdropping attack (RKA-aEav) in Multi-Domain Quantum-Key-Distribution Networks (MD-QKDN)

Peiyi Li
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
m13011067088@163.com

Xiaosong Yu
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
xiaosongyu@bupt.edu.cn

Yongli Zhao
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
yonglizhao@bupt.edu.cn

Jie Zhang
State Key Lab of Information Photonics and Optical Communications
Beijing University of Posts and Telecommunications
Beijing, China
lgr24@bupt.edu.cn

***Abstract*—In this paper, a routing and key resource allocation method against eavesdropping in Multi-Domain Quantum Key Distribution Networks is proposed. Simulation results indicate that RKA-aEav has better performance in terms of decreasing ratio of eavesdropping.**

Keywords—Security, eavesdropping attack, quantum key distribution networks

I. INTRODUCTION

With the rapid development of network information technology, more and more advanced technologies (such as 5G, Internet of Things' applications) enter people's lives and provide convenient services for them. Information plays an increasingly important role in today's world, and its security is gradually mentioned and valued by both academy and industry. Quantum-Key-Distribution (QKD) technology is derived from the fundamental principles, including the Heisenberg uncertainty principle and quantum no-cloning theorem, can ensure the security of point-to-point communication. It enables the two parties of the communication to generate and share a pair of random and secure keys to encrypt and decrypt information [1]. The number of network users has increased and the network scale has extended, which make network structures become more and more complex. In this context, multi-domain QKDN is a better choice for networking, which contains multiple technologies and different QKDN providers [2, 3].

However, the unconditional security of QKD is difficult to guarantee in the actual networking. In order to provide quantum keys for users located to distant QKD nodes, trusted relay technology is used in QKDN. The local keys are stored in trusted relays, and establish the global keys between source and destination nodes by hop-by-hop transmission [4, 5]. It should be noted that "trusted" in trusted relay is assumed, therefore, there must be several security weak points in practice. For example, the eavesdropper can use potential flaws in trusted relays to attack them, and steal important key information in internal structures of trusted relays [6-8]. If attackers also set eavesdropping points in key relay links, things will get worse: attackers can easily decode secure keys that provided to users and then they can crack encrypted information between users. Finally, these attacks will turn into more serious risks (e.g. loss or corruption of information, spoofing, repudiation and forgery). Thus, how to ensure that the keys can resist the above threats during the relay process and make information more secure, are urgent issues to be solved.

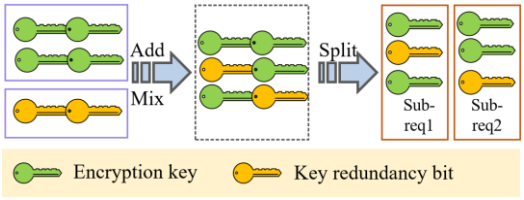
In recent years, some scholars have proposed schemes to resist eavesdropping attacks in several scenarios. For instance, X. Xu et al. analyzed the existing routing randomization methods, and proposed a routing randomization defense method based on deep reinforcement learning, which realizes routing randomization on packet-level granularity using programmable switches [9]. W. Bai et al. proposed eavesdropping-aware routing and spectrum allocation algorithms in elastic optical network. They firstly described eavesdropping issue by introducing probability theory, and then they employed multi-flow virtual concatenation to further improve security and network performance [10]. But these methods do not make available for QKD networks, and due to information privacy of each domain for other domains, methods of against eavesdropping in multi-domain QKDN should be redesigned.

II. NETWORK MODEL

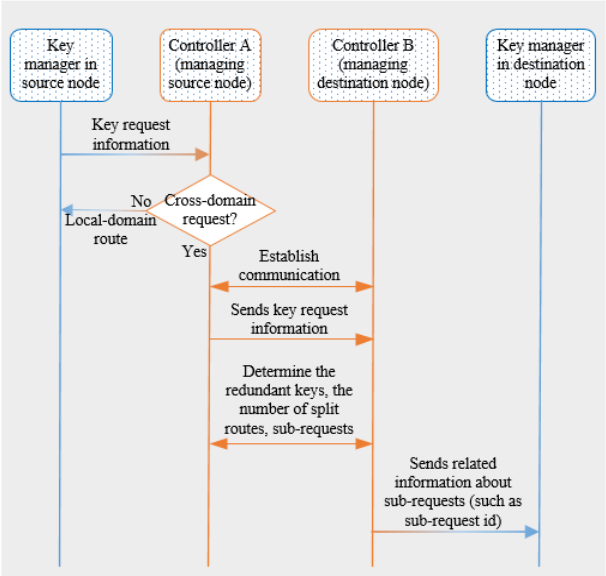
Let *G(V, E, P, C)* donate the network, where *V* is the set of quantum key manager nodes, *E* is the set of key relay links and *P* represents different QKD domains . There are two kinds of nodes in *V* : intra-domain nodes (IDNs) and gateway nodes (GWNs). Just as their names suggest, intra-domain nodes are completely in a domain while gateway nodes connect adjacent domains. Similarly, *E* also contains two kinds of links: intra-domain links and inter-domain links. Two adjacent domains have one or more inter-domain links. Each domain is managed by a QKDN controller *C*, which is connected to other controllers through east-west links. *R(s, d, p, key, key')* is the arrival request requiring secret keys. *S* represents the source node of the request, *d* represents its destination node, *p* represents which domain the destination node belonging to, *key* is the number of keys the request needs, and *key'* is the number of redundant keys. *Key'* has a specific value only when the controllers determine that the key needs to be split and calculate the specific number of split keys.

Since the eavesdropping attack in QKDN has no obvious characteristics, it cannot be identified in time. In order to reduce the risk of eavesdropping, controllers first process the requested keys. This step is named as key redundancy bit consultation. Controllers of source node and destination node calculate the amount of redundant keys according to the set redundancy rate, and split keys after adding redundant bits according to the set key split threshold.

Fig. 1 shows the schematic diagram of adding key redundancy bits and the procedure of key redundancy bit consultation. Keys that have been added with redundancy and split are transmitted on different relay routes. Even if eavesdroppers set eavesdropping points on some relay links and have attacked some trusted relays, the probability of getting the original state of the keys is still reduced, which improves the security of MD-QKDN in eavesdropping attacks to a certain extent. But due to the low rate of quantum key generation, key resources are very precious, so the above operations are only for cross-domain key service requests.



(a)



(b)

Fig. 1 (a) Schematic diagram of adding key redundancy bits; (b)The procedure of key redundancy bit consultation.

III. Routing and Key Allocation Against Eavesdropping Attack In MD-QKDN

This part is mainly about how to relay keys processed by controllers in the previous stage. Unlike single-domain QKDN, MD-QKDN has strong privacy among domains. Non-local domain members cannot obtain important information of the local domain, such as topology details. It makes that the routing of cross-domain key request cannot be calculated by one QKDN controller, and needs to be completed by controllers in different domains. In addition, GWNs are only responsible for key relay, and they are not used as nodes to generate key requests.

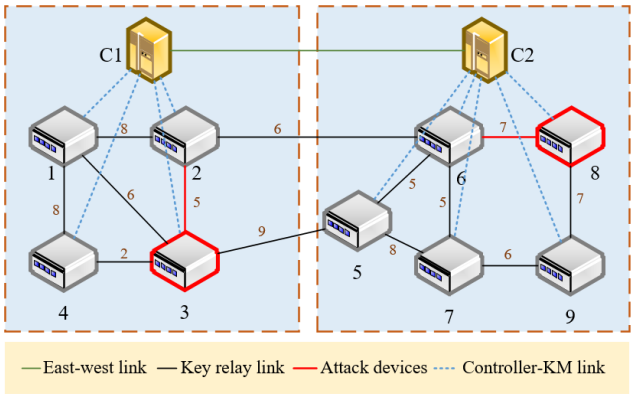
The pseudo code of *RKA-aEav* is illustrated in table I. *Key+key'* represents the sum of encryption keys and redundant keys. If *key+key'* is larger than split *thresh*, the key request will need to be divided into *n* sub-requests and should find *n* sub-routes to relay keys. The number of keys relaying on each sub-route is 1/n of *key+key'*. If *key+key'* cannot be divisible by *n*, the remainder will be randomly allocated to one of the sub-requests. Then the source controller calculates *n* routes only containing GWNs, because it is unable to get other domains' specific topology information and it just has topology structures of local domain and global GWNs. For each route in *n* routes, the source controller further notifies other controllers to calculate *k* paths with minimum hops between GWNs they manage. If *key+key'* is smaller than split *thresh*, source controller only needs to calculate one GWN route from source node to destination node. For each path in *k* paths with minimum hops, the controller checks key resources in every quantum key pool (QKP). If all QKPs related to the current path do not have enough key resources to provide, the current key request will be blocked. Conversely, the controller obtains the amount of available key resources on the current path and compares it to the maximum key resources ever recorded. If the amount of available key resources is larger than the value ever recorded, the controller will update the number of the max key resources and record the current path. The step of key redundancy aggravates the imbalance of key resources in QKPs, so the controller selects the path with the most abundant key resources as the relay route to balance key consumption. After routing and key resource allocation, each controller will update related information and network status, and shares messages that are not the privacy of its own domain.

TABLE I. Pseudo Code Of RKA-aEav

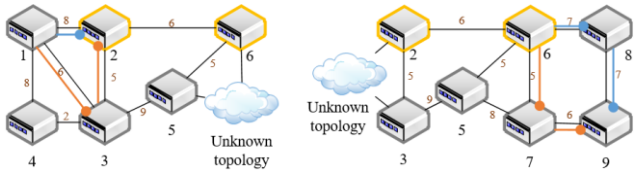
	Algorithm—*RKA-aEav*
	Input: *G (V, E, P, C), R(s, d, p, key, key')*
	Output: *RKA for R*
1	**for** each *R (s, d, p, key, key')*
2	**if** p_s *!=*p_d **then**
3	**if** *key+key'>thresh* **then**
4	*R(s, d, p, newKey)←newKey=(key+key')/n;*
5	**for** each *path i in n*
6	**for** each *2 adjacent GWNs*
7	*sp={sp1, sp2, sp3, …, spk};*
8	**end for**
9	**end for**
10	**else**
11	*R(s, d, p, newKey)←newKey=key+key';*
11	**for** each *2 adjacent GWNs*
12	*sp'={sp1', sp2', sp3', …, spk'};*
13	**end for**
14	**for** each *sp(sp') in each C*
15	*maxKey=0;*
16	**if** *keys in QKP of each sp(sp') link > newKey* **then**
17	*availKey=max(key_sp1,key_sp2,…,key_spk);*
18	**if** *availKey>maxKey* **then**
19	*maxKey=availKey;*
20	*route=spi/spi'←maxKey;*
21	**end if**
22	**else** *fail;*
23	**end for**
24	**end for**

An illustrate example is used to describe *RKA-aEav* in Fig. 2. A topology with 2-domain, 9-nodes and 13-relay link is applied. The amount of keys contained in QKP of each adjacent node has been marked next to every relay link. The consulted redundancy key addition rate is 25%, the key split *thresh* is set as 10, *n* and *k* are both equal to 2. The attacker eavesdrops on two links: 2-3 and 6-8, and key data in relay node 3 and relay node 8 are leaked, which means that the attacker can steal secret keys that are relayed through these two links. Key request *R (1, 9, 2, 8, null)* needs to be serviced. Node 1 sends information of *R* to controller C_1, C_1 communicates with C_2 through east-west link C_1- C_2. *Key+key'* is 8+8*25%=10, and 10 is larger than split *thresh* 8, so

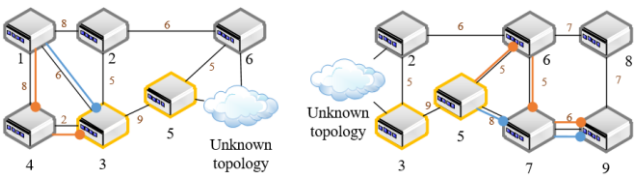
the key request is divided into two sub-requests: $R_1(1, 9, 2, 5)$, $R_2(1, 9, 2, 5)$. Then C_1 calculates 2 GWN routes 2-6 and 3-5. For the first GWN path 2-6, there is just one node (node 2) belonging to domain 1, so 2 minimum-hop paths in domain 1 are 1-2 and 1-3-2 calculated by C_1. In 1-2, the amount of available key resources is 8 while the amount of available key resources in 1-3-2 is 5, so 1-2 is selected as the first part of the first sub-path. Node 6 belongs to domain 2 and is managed by C_2, 2 candidate paths in domain 2 are 6-8-9 and 6-7-9. In 6-8-9, the amount of available key resources is 7 while the amount of available key resources in 6-7-9 is 5, so 6-8-9 is selected as the second part of the first sub-path. Therefore, the first complete sub-path of R_1 is 1-2-6-8-9. Similarly, the second complete sub-path of R_1 is 1-3-5-7-9. Two controllers send routing information to key relays respectively and key relays provide keys to the user in destination. When keys of all sub-routes reach the destination node, C_2 processes these keys and restores them to the keys used to encrypt information according to the rules agreed with C_1. In this process, although the attacker eavesdrops on link 2-3 and link 6-8, and some key relays are not safe, link 2-3 is not involved in the routing result in this example. Only part of secret keys is transmitted on 6-8, the attacker cannot obtain the entire real keys used encrypting. Thus, for this request, *RKA-aEav* successfully resists the eavesdropping attack.



(a)



(b) (c)



(d) (e)

Fig. 2 Illustration example of *RKA-aEav:*

(a) topology of the example; (b) view of C_1 and routing in domain 1 (GWN-path 1); (c) view of C_2 and routing in domain 2 (GWN-path 1); (d) view of C_1 and routing in domain 1(GWN-path 2); (e) view of C_2 and routing in domain 2(GWN-path 2).

IV. Simulation Results and Analysis

24-node and *43*-link *USNET* (Fig. 3) is applied in the simulation. It is divided into three QKD domains, domain 1 contains nodes *{1, 2, 3, 4, 5, 6, 7, 8}*, domain 2 contains nodes *{9, 11, 12, 15, 16, 19, 21, 22}*, domain 3 contains nodes *{10, 13, 14, 17, 18, 22, 23, 24}*, and GWNs belonging to different domains are highlighted with different colors. Every two adjacent nodes jointly maintain a set of quantum key pools (QKP), and each set of QKPs' capacity is $4500t$ (t is the key unit, which is set to 1 in this simulation). Totally 10^5 Poisson distribution key requests are generated, and their source nodes and destination nodes are randomly selected from IDNs. New quantum key generation rate v is $50t$/s, and the number of requested keys is selected randomly from the set $\{4t, 8t, 12t\}$. In this paper, there are two parameters are used to test the performance of *RKA-aEav* and the baseline algorithm: eavesdropping ratio and network blocking ratio. Eavesdropping ratio is the rate of the number of eavesdropped key requests to the number of successfully served key requests, while network blocking ratio is the rate of the number of requests which blocked due to lack of resources to the number of all requests reaching the network. The baseline does not have any methods of defense against attacks and it just provides keys from source to destination domain-by-domain. The number of paths with minimum hops can be changed in the baseline.

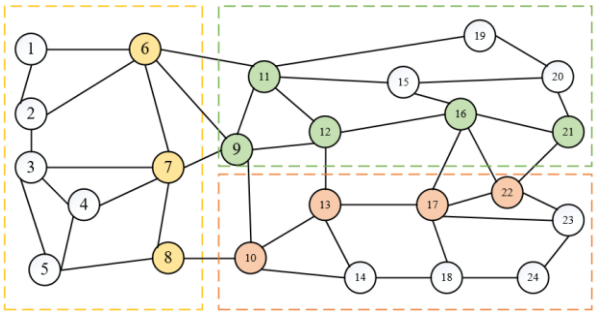


Fig. 3 3-domain *USNET* topological structure.

Figs. 4-6 are results of the simulation results. Fig. 4 is about the eavesdropping ratio versus the number of eavesdropped links when $k=3$, $thresh=12$, $redundancy\ rate=25\%$, and (1) baseline, (2) $n=1$, (3) $n=2$, (4) $n=3$. It can be found that compared with *RKA-aEav*, the baseline cannot resist eavesdropping attacks, so it has the highest eavesdropping ratio. And when n increases, the eavesdropping ratio decreases. It means that higher security can be achieved with more sub-routes, because the more the keys with redundant bits are split, the more difficult it is for the attacker to obtain the real secret keys. And the eavesdropping ratio with $n=4$ is more than 50% smaller than baseline. In Fig. 5, the variable is the value of key split *thresh*, and $k=3$, $n=4$. It shows that the split *thresh* also affects the eavesdropping ratio. The lower the threshold, the easier it is for the keys with redundant bits to be divided into multiple sub-keys and transmitted along multiple sub-paths. Compared with the complete keys, the probability of sub-keys being successfully eavesdropped is lower. In this simulation, the maximum sum of encryption keys and redundant keys is 16, so when *thresh* is equal to16, it is not divided into several paths actually. However, its eavesdropping ratio is still lower than the baseline. It is because that even though the attacker obtains the complete keys, these keys contains redundancy bit so that the attacker cannot correctly select encryption keys from the

mixed keys. Fig. 6 is the relationship between the blocking ratio and traffic load when *k=3*, *thresh=8*, (1) *n=1*, (2) *n=2*, (3) *n=3*, and (4) baseline. This figure reflects the cost of high security. It can be seen that the proposed algorithm has higher blocking ratio than the baseline, it is because that the redundant keys occupy a part of keys encrypted for the services, which accelerates the consumption of key resources. However, the increase of *n* can decrease the blocking ratio, because key requirement on each sub-path is less than on one path.

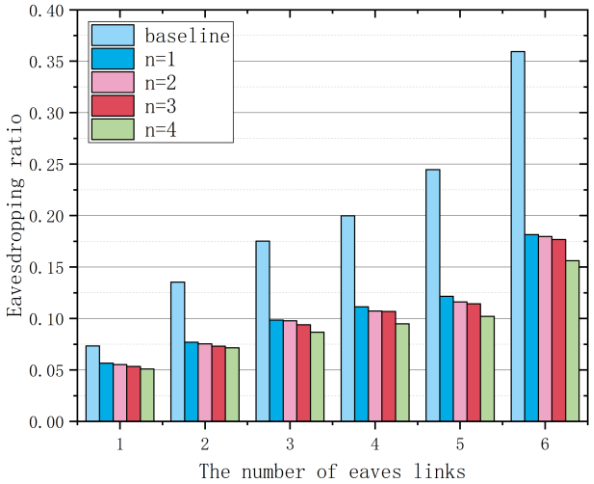


Fig. 4 Eavesdropping ratio VS the number of eavesdropped links under: (1) baseline, (2) n=1, (3) n=2, (4) n=3.

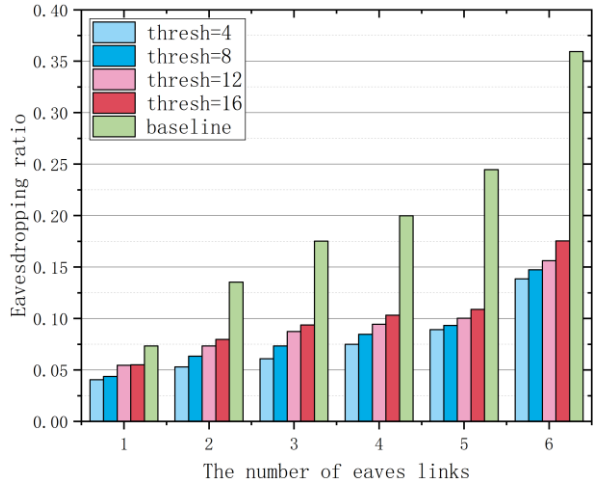


Fig. 5 Eavesdropping ratio VS the number of eavesdropped links under: (1) thresh=4, (2) thresh=8, (3) thresh=12, (4) thresh=16, (5) baseline.

V. Conclusions

This paper proposes a routing and key resource allocation method against eavesdropping attack *(RKA-aEav)* in Multi-Domain Quantum-Key-Distribution Networks (MD-QKDN). Simulation results show that the proposed method has lower eavesdropping ratio, so that it can resist eavesdropping attack better than the baseline algorithm which has no redundant bits and sub-routes. *RKA-aEav* also alleviates the problem of uneven consumption of key resources to a certain extent by adjusting internal parameters, and effectively reduces the network blocking ratio.

Acknowledgment

This work is supported by Science and Technology Innovation 2030- Major Project (2021ZD0300704), NSFC project (61971068, 62150032, U22B2026), National Key Research and Development Program of China (2020YFE0200600), Fund of State Key Laboratory of Information Photonics and Optical Communications, BUPT (IPOC2020ZT04).

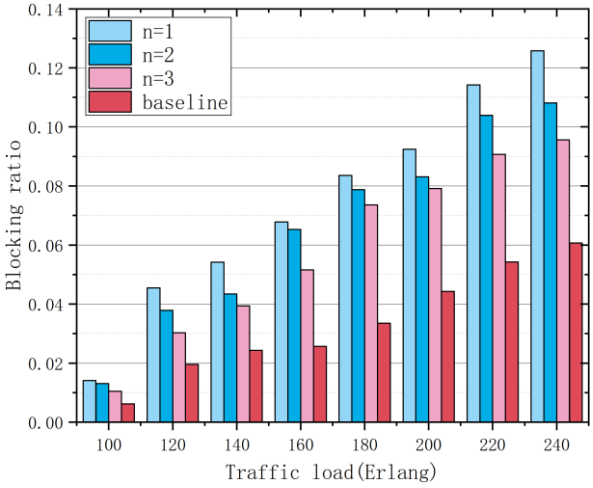


Fig. 6 Blocking ratio VS traffic load under: (1) n=1, (2) n=2, (3) n=3, (4) baseline.

References

[1] J. Zou et al., "Topological Mapping Based Failure Recovery in Multi-domain Quantum Key Distribution Networks", 2021 Opto-Electronics and Communications Conference (OECC), Hong Kong, Hong Kong, pp. 1-3, 2021.

[2] J. Lv, X. Yu, Y. Zhao, A. Nag and J. Zhang, "Recovery Scheme with Resource Abstraction in Multi-Domain Quantum-Key-Distribution Networks", 2022 27th OptoElectronics and Communications Conference (OECC) and 2022 International Conference on Photonics in Switching and Computing (PSC), Toyama, Japan, pp. 1-3, 2022.

[3] Q. Wang, X. Yu, Q. Zhu, Y. Zhao, and J. Zhang, "Quantum key pool construction and key distribution scheme in multi-domain QKD optical networks (QKD-ON)", Proc. SPIE 11781, 4th Optics Young Scientist Summit (OYSS 2020), Feb 2021.

[4] M. Mehic et al., "A Novel Approach to Quality-of-Service Provisioning in Trusted Relay Quantum Key Distribution Networks", in IEEE/ACM Transactions on Networking, vol. 28, no. 1, pp. 168-181, Feb. 2020.

[5] C. Yang, H. Zhang and J. Su, "Quantum key distribution network: Optimal secret-key-aware routing method for trust relaying", in China Communications, vol. 15, no. 2, pp. 33-45, Feb. 2018.

[6] X. Yu, X. Liu, Y. Liu, A. Nag, X. Zou, Y. Zhao, and J. Zhang, "Multi-path-based quasi-real-time key provisioning in quantum-key-distribution enabled optical networks (QKD-ON)," Opt. Express 29, 21225-21239, 2021.

[7] O. Shirko and S. Askar, "A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking", in IEEE Access, vol. 11, pp. 21641-21654, 2023.

[8] X. Yu et al., "Secret-Key Provisioning With Collaborative Routing in Partially-Trusted-Relay-based Quantum-Key-Distribution-Secured Optical Networks", in Journal of Lightwave Technology, vol. 40, no. 12, pp. 3530-3545, June 15, 2022.

[9] X. Xu, H. Hu, Y. Liu, "Moving target defense of routing randomization with deep reinforcement learning against eavesdropping attack", Digital Communications and Networks, vol. 8, pp. 373-387, June 2022.

[10] W. Bai et al., "Eavesdropping-aware routing and spectrum allocation based on multi-flow virtual concatenation for confidential information service in elastic optical networks", Optical Fiber Technology, vol. 40, pp. 18-27, January 2018.