hv photonics

IMPACT FACTOR 1.9

CITESCORE 3.5

Article

Dynamic Security-Aware Resource Allocation in Quantum Key Distribution-Enabled Optical Networks

Vimal Bhatia, Adolph Kasegenya and Bowen Chen

Special Issue

Enabling Technologies for Optical Communications and Networking

Edited by

Prof. Dr. Xian Zhou and Prof. Xue Chen

MDPI

https://doi.org/10.3390/photonics12070645

photonics

MDPI

Article

Dynamic Security-Aware Resource Allocation in Quantum Key Distribution-Enabled Optical Networks

Vimal Bhatia [1,2,*], Adolph Kasegenya [2] and Bowen Chen [1,*]

[1] School of Electronic and Information Engineering, Soochow University, Suzhou 215006, China
[2] Department of Electrical Engineering, Indian Institute of Technology (IIT) Indore, Indore 453552, India; phd2301102014@iiti.ac.in
* Correspondence: vbhatia@iiti.ac.in (V.B.); bwchen@suda.edu.cn (B.C.)

Abstract

The demand for secure communication in the age of quantum technologies has driven progress in quantum key distribution (QKD) techniques for optical networks. This research addresses the issues of high blocking probabilities (BPs) and the proper utilization of quantum resources in varying network loads by introducing a novel heuristic approach, termed dynamic security-aware quantum resource allocation (D-SQRA), designed for dynamic resource allocation in QKD-enabled optical networks. We propose two D-SQRA algorithms to employ an adaptive resource assignment (RA) strategy that concurrently addresses routing, wavelength, and time-slot selection while dynamically modifying security levels according to the real-time network load and resource availability. We evaluate the proposed D-SQRA performance against two conventional methods, namely, fixed security quantum resource allocation (F-SQRA) and baseline quantum resource allocation (B-QRA). We discuss the results for NSFNET and UBN24 topologies for network security performance metrics such as network security performance (NSP), BP, quantum key utilization (QKU), and time-slot utilization. The results show that the proposed D-SQRA algorithms provide significant improvement with respect to conventional techniques in addressing proper resource utilization and management by reducing BPs of the new incoming connection requests.

Keywords: QKD; optical networks; resource allocations

Received: 15 April 2025
Revised: 9 June 2025
Accepted: 23 June 2025
Published: 25 June 2025

Citation: Bhatia, V.; Kasegenya, A.; Chen, B. Dynamic Security-Aware Resource Allocation in Quantum Key Distribution-Enabled Optical Networks. *Photonics* **2025**, *12*, 645. https://doi.org/10.3390/photonics12070645

1. Introduction

Quantum key distribution (QKD) is revolutionizing secure communications by using the principles of quantum mechanics to establish cryptographic keys that are essentially secure against both classical and quantum attacks [1]. In contrast to classical cryptographic protocols based on computational hardness, the security of QKD is based on the laws of physics, making it a key technology for future-proofing optical networks [2]. However, real-world implementations of QKD in networks face challenges concerning resource utilization, time-slot assignment, and network scalability [3,4].

For optical networks implementing QKD, the assignment of both wavelengths and time-slots plays a major role in QKD efficiency and reducing the wastage of resource utilization [5]. Thus, routing, wavelength, and time-slot assignment (RWTA) is a crucial problem for resource sharing in QKD-enabled optical networks [6–8]. Existing solutions are not agile enough to adapt to changing security requirements, leading to degraded throughput, increased blocking probability (BP), and inefficient quantum key utilization (QKU) [9].

QKD has physical-layer constraints in establishing point-to-point connectivity, requiring optimal wavelength and time-slot resources to maximize capacity as highlighted in [10–12]. QKD networks can deploy resources across the network via a unified control plane, enhancing operational efficiency. Software-defined networking (SDN) emerges as a solution by abstracting network management into control and data planes, providing flexibility and programmability [13]. SDN facilitates traffic management, separating control, and data functions, and allows coordinated QKD network orchestration, providing secure solutions for SDN-based networks [14,15].

To enhance security, SDN-enabled QKD networks introduce a dedicated secure key management layer within software-defined optical networks (SDONs) [6]. Various assignment strategies improve security for control signals and data services using wavelength division multiplexing (WDM) and optical time division multiplexing (OTDM). However, limited research exists on systematic secret-key distribution with centralized management and coordination of QKD resources [16,17].

To address this, we propose dynamic security-aware quantum resource allocation (D-SQRA) algorithms, a framework for optimizing QKD resource allocation by dynamically adjusting time-slot allocation strategies. The proposed D-SQRA algorithms ensure security-aware decision-making for effective quantum resource allocation while guaranteeing the highest achievable security levels.

In this work, we explore and compare two adaptive security management mechanisms for resource allocation in QKD-enabled optical networks. We propose a security-level (SL) downgrading strategy, where the allocation process starts from the highest security level, and during the allocation, if there are not enough resources (e.g., time-slots or wavelengths), it downgrades to medium or low security. It assumes that service level agreements (SLAs) allow for the downgrades to accept the incoming connection requests (CRs).

Next, we investigate an upgrading strategy at the security level, where the allocation starts at a low security level and is upgraded to a medium or high security level when more resources are available. This technique initially tries to allocate the incoming CRs at a lower security level, and if the resources are available, they will upgrade CRs into higher security levels (middle and higher levels). This comparative study serves to shed light on the optimal balance from the perspectives of resource efficiency and BP under mutually contrasting network conditions and traffic loads, both of which are important considerations for the practical deployment of QKD networks.

The proposed D-SQRA employs the First-Fit (FF) algorithm for resource allocation and Dijkstra's shortest path algorithm for routing, optimizing network security performance (NSP), time-slot utilization, and QKU. Additionally, the assumption of a single optical fiber shared for both classical and QKD channels introduces constraints, making efficient resource management crucial. The proposed D-SQRA algorithm was compared with the two conventional methods below.

2. Background

This background outlines the role of optical networks, the integration of RWTA in QKD networks, and the key challenges in QKD resource allocation.

2.1. Optical Networks and Common Optical Fibers

Optical networks underpin today's high-speed internet infrastructure, facilitating the high-speed transmission of gigabytes of data over long distances with low latency and high reliability [18]. Optical networks are replacing traditional copper communication methods with light signals transmitted on optical fibers to transport information. Optical fibers, which are usually composed of silica, amplify very little signal and provide a large

bandwidth, which supports the perpetual increase in internet traffic and bandwidth-hungry services like video streaming, cloud computing, and secure communications [19].

Through WDM, multiple wavelengths are capable of transmitting data through the same optical fiber on a per-channel basis. This multiplexing greatly increases the network capacity and efficiency [20,21]. As quantum networks begin to deploy QKD-enabled optical networks, these networks will rely on both quantum and classical signals traversing the same fiber infrastructure, necessitating increasingly sophisticated interference, isolation, and integrity mechanisms to maintain the integrity of quantum keys [22].

2.2. RWTA in QKD Networks

The RWTA problem is central to resource allocation in QKD-enabled optical networks. Efficient RWTA optimizes quantum channel allocation while balancing security requirements and BP [7,9,23–27]. The key components of RWTA include the following:

- **Route Assignment**: Identifying the shortest and most optimized paths for transmitting quantum keys.
- **Wavelength Assignment**: Allocating different wavelengths to QKD and classical channels to prevent overlap and interference.
- **Time-slot Allocation**: Assigning time-slots to quantum transmissions based on security requirements and network availability.

2.3. Challenges in QKD Resource Allocation

Before QKD networks can be fully realized, several resource utilization and security performance challenges must be addressed [26] as follows:

- **Scarcity of Wavelengths**: The limited availability of wavelengths necessitates efficient allocation mechanisms.
- **Security Adaptability**: V arying security levels require dynamic time-slot allocation strategies based on incoming connection requests.
- **Reduction in Blocking Probability**: Optimizing allocation mechanisms to minimize the BP.

To tackle these issues, we proposed D-SQRA, a new and flexible framework designed to provide flexible time-slot allocations and security configurations, which adapt to changing circumstances in real time, considering factors such as resource availability and security needs for incoming CRs while also improving resource utilization and overall network security in QKD-enabled optical networks.

3. Related Work

The integration of QKD with optical networks has been extensively investigated, and considerable work has been performed to tackle the challenges associated with resource allocation, RWTA, and security-aware networking. In this section, the relevant literature on these crucial aspects is reviewed.

3.1. Resource Management in Optical Networks with QKD

At the core of QKD-enabled networks is an efficient allocation of classical and quantum channels over a shared optical fiber infrastructure. Other recent works investigated using WDM techniques to guarantee minimum interference of classical with quantum signals [28]. For instance, in [29], the paper suggests different dynamic spectrum allocation strategies to overcome the classical signal cross-talk interference in QKD transmissions. Some authors [9,30] present adaptive assignment of wavelength algorithms to optimize the depth of quantum key collection, thus achieving good usage of quantum keys and formal privacy-preserving completion under strict security constraints.

3.2. RWTA Strategies

Conventional RWTA designs typically assume a static division of resources, which can result in suboptimal routing of quantum channels. In [31,32], the authors further improve performance by utilizing real-time traffic conditions and security level requirements in the dynamic RWTA schemes. In addition, time-slot based RWTA schemes [16,27,33] prescribe flexible time-slot assignment schemes that favor higher security level requests while considering network usage.

3.2.1. Fixed Security Quantum Resource Allocation (F-SQRA)

F-SQRA is a static resource allocation technique in which each CR is given a fixed security level in the entire network. The security level is static and independent of the network load and available resources. Under resource-constrained scenarios, the resource assignment (i.e., the allocation of the routing, wavelength, and time-slot) is strictly carried out according to this fixed security constraint, and typically, this may incur a higher BP. Although it has predictable security performance, it is not flexible, thereby leading to low efficiency in dynamic or heavy traffic [9,26].

3.2.2. Baseline Quantum Resource Allocation (B-QRA)

B-QRA is a simple benchmark model that allocates resources without regard to security levels. All CRs are treated equally, and the algorithm only concentrates on assigning connections based on the availability of resources. It serves as a baseline to assess the advances brought by more advanced approaches such as F-SQRA or D-SQRA [9,26].

3.3. Networking in QKD Systems with Security Awareness

Networking frameworks with security awareness aim to automatically tune security mechanisms in response to the state of the network conditions. Researchers in [9,27] recently analyzed security-level adaptation mechanisms that enable both the downgrade and upgrade of security levels based on resource availability. The above-mentioned mechanisms assist in optimizing the probability of success for a key distribution while reducing the BP. Additionally, integrated security policies for QKD networks have been explored in [23] as a means to manage the efficient and confidential use of resources; however, integrated methods remain an open challenge.

3.4. Coexistence Between Shared Optical Fibers and Multiple Channels

The shared nature of optical fibers and multiple (quantum, classical, and measuring-basis) channels in QKD-enabled optical networks raises concerns about cross-talk, unwanted signal degradation, and quantum key transmission integrity. To support secure multiplexing over a shared physical infrastructure, advanced techniques like channel isolation, guard bands, and time-slot synchronization are used [7,34,35].

4. Proposed Solution

The D-SQRA approach was developed to dynamically modify security settings according to real-time network conditions. By incorporating an adaptive time-slot allocation mechanism, it efficiently manages RWTA to optimize QKU while minimizing the BP. Using the FF algorithm for resource allocation and Dijkstra's algorithm for shortest path selection, D-SQRA ensures that QKD networks achieve optimal security–performance trade-offs in a shared optical fiber environment.

To address the challenges of resource-efficient QKD deployment, we propose D-SQRA algorithms for the downgrading and upgrading of security levels. This approach

dynamically adapts security levels based on network conditions, ensuring efficient RWTA while maintaining optimal security performance.

4.1. System Model

From Figure 1, the proposed system model illustrates an optical network that incorporates QKD alongside classical data transmission, utilizing a shared optical infrastructure. This architecture fundamentally relies on a WDM fiber system, which concurrently transmits three distinct types of optical signals: classical channels for standard data communication, quantum channels for the distribution of quantum keys (QKChs), and measuring-basis channels (MBChs) for the classical post-processing of quantum states. The separation is achieved through a guard band, which serves to shield the delicate quantum signals from the disruptive effects of more robust classical signals. A multiplexer and an Erbium-Doped Fiber Amplifier (EDFA) are employed to combine these wavelength groups and inject them into a single optical fiber, facilitating effective channel coexistence.

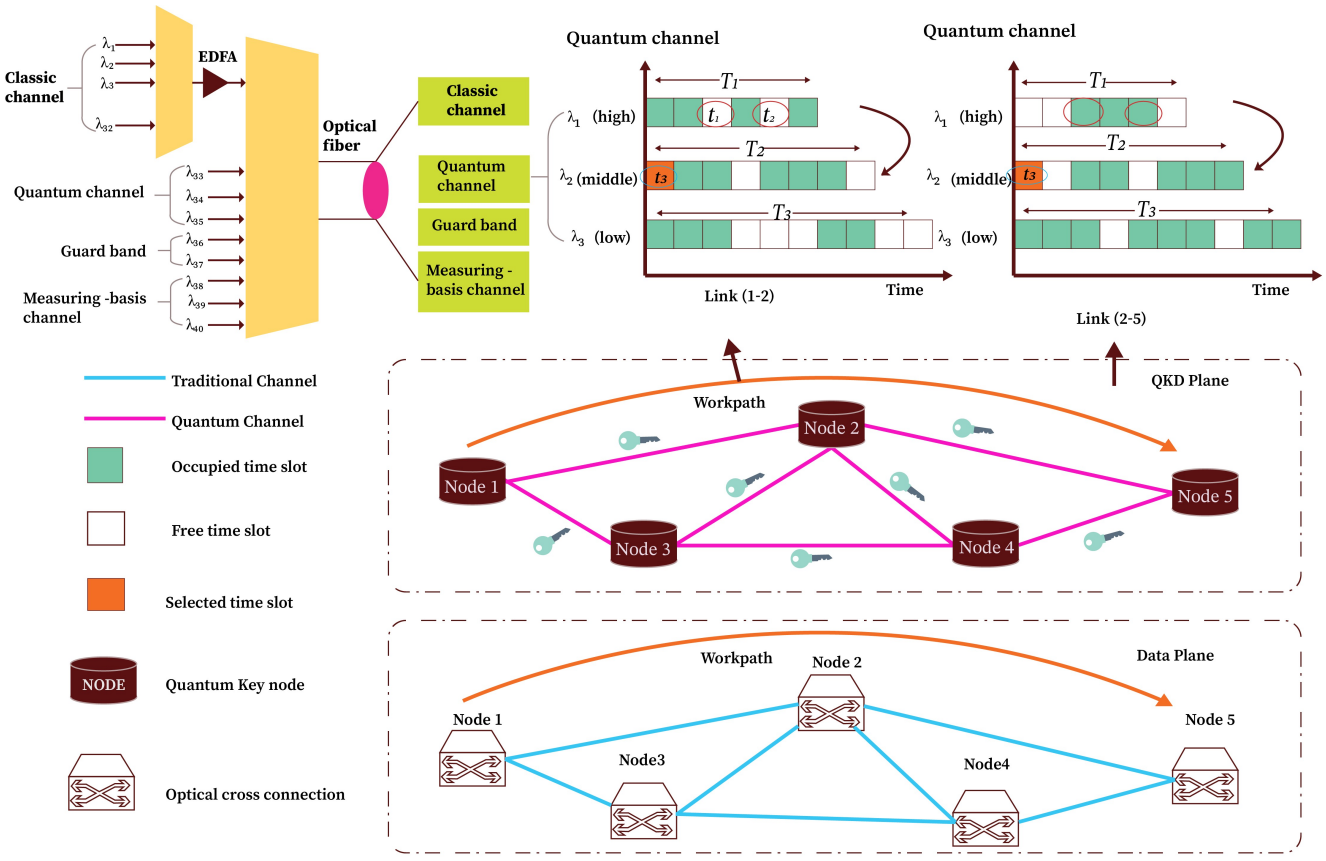


Figure 1. QKD-enabled optical network [26].

The time-slot structure depicted in the figure establishes varying security levels (high, medium, and low), each necessitating distinct amounts of quantum key utilization. Higher security levels, such as SL-1, necessitate more regular key updates, resulting in a tighter arrangement of time-slots (T_1). Conversely, medium SL-2 requires medium time-slots (T_2), and lower security levels, like SL-3, require a reduced number of slots (T_3), thereby preserving key material. Upon receiving a CR, the system evaluates the availability of QKChs and MBChs along the proposed path. In cases where the available resources do not meet the initially specified security level, the system adjusts the request to a lower level. This modification enhances the likelihood of successful allocation while ensuring that a minimum security standard is upheld. On the other hand, when quantum key resources

are plentiful, the system has the potential to elevate the request to a higher security level, thereby enhancing confidentiality.

The architecture delineates two distinct planes: the QKD plane and the data plane. The QKD plane consists of quantum nodes that exchange and retain keys through QKCh and MBCh connections. The keys are subsequently employed to ensure the security of classical communication within the data plane, which consists of optical cross-connects (OXCs) that facilitate the routing of encrypted user data. The whole operation is managed by an SDN controller that observes the real-time status of both quantum and classical resources, determines routing and wavelength choices, and adjusts security levels dynamically. This division of responsibilities enables the network to effectively manage performance and security across different load scenarios, resulting in a system that is both adaptable and attuned to quantum considerations.

4.2. Security Level Downgrade Algorithm

The security level downgrade algorithm (given in Algorithm 1) is designed to allocate network resources for a CR while maintaining the highest possible level of security. It begins by receiving a request defined by a source node (s), a destination node (d), an initial security level, and a set of available resources. The algorithm first determines a set of candidate paths between the source and destination using the K-shortest path algorithm. Next, the algorithm attempts to allocate resources, specifically time-slots, based on the current (initial) security level. If a suitable path is found, the FF algorithm is applied to check for available time-slots on that path. If resources are available, the algorithm allocates them and completes the process. However, if allocation fails at the current security level, the algorithm downgrades to a lower security level (which requires more relaxed resource constraints) and retries the allocation process. This continues until either a successful allocation is made or the lowest security level is reached. If all attempts fail, the request is marked as blocked. This process will repeat itself until all CRs have been served or all resources have been utilized; then the algorithm will end there.

Algorithm 1 Security level downgrade

```
procedure SECURITY_LEVEL_DOWNGRADE(s, d, initial_security_level, K, resourceMatrix)
    currentLevel ← initial_security_level
    candidatePaths ← FINDKSHORTESTPATHS(s, d, K)
    while currentLevel ≥ 1 do
        requiredSlots ← GETTIME-SLOTREQUIREMENT(currentLevel)
        for path ∈ candidatePaths do
            available ← FIRSTFIT(path, requiredSlots, resourceMatrix)
            if available = True then
                ALLOCATERESOURCES(path, requiredSlots)
                return path, currentLevel
            end if
        end for
        currentLevel ← currentLevel − 1
    end while
    return [ ], −1
end procedure
```

4.3. Security Level Upgrade Algorithm

The security level upgrade algorithm (given in Algorithm 2) aims to allocate resources for a connection request starting from the lowest security level, with the goal of gradually upgrading to a higher level when additional resources are available. It begins by accepting

the input parameters, including the source node (s), destination node (d), the highest allowable security level for the request, and the resource availability matrix. The algorithm first identifies K-candidate paths between the source and the destination using the K-shortest path algorithm. It then starts the allocation process at the lowest security level (level 1 and tries to upgrade up to level 3), determining the required number of time-slots for that level. For each candidate path, it uses the FF algorithm to check if the required resources are available. If a successful allocation is made at the current level, the algorithm attempts to upgrade the security level by incrementally checking if additional time-slots are available for the next higher level. If resources for a higher level are available, the allocation is upgraded, and the process repeats until the initial requested security level is reached or no further upgrade is possible. This process will repeat itself until all CRs have been served or all resources have been utilized; then the algorithm will end there. This approach allows the network to flexibly adapt to available resources while prioritizing connection success. If no allocation is possible at any level, the request is considered blocked. Overall, this strategy promotes high acceptance rates and the opportunistic enhancement of security, especially in resource-constrained environments.

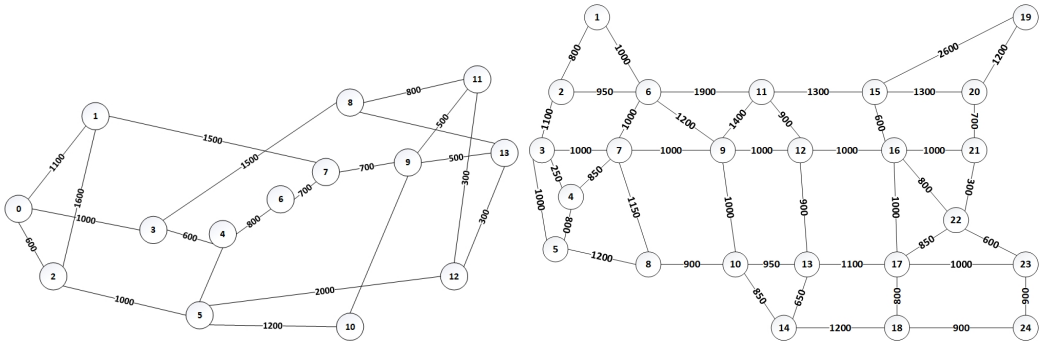
Algorithm 2 Security level upgrade

```
procedure SECURITY_LEVEL_UPGRADE(s, d, initial_security_level, K, resourceMatrix)
    currentLevel ← 1
    candidatePaths ← FINDKSHORTESTPATHS(s, d, K)
    while currentLevel ≤ initial_security_level do
        requiredSlots ← GETTIME-SLOTREQUIREMENT(currentLevel)
        for path ∈ candidatePaths do
            available ← FIRSTFIT(path, requiredSlots, resourceMatrix)
            if available = True then
                ALLOCATERESOURCES(path, requiredSlots)
                while currentLevel < initial_security_level do
                    nextLevel ← currentLevel + 1
                    extraSlots ← GETTIME-SLOTREQUIREMENT(nextLevel)
                    if FIRSTFIT(path, extraSlots, resourceMatrix) = True then
                        UPGRADEALLOCATION(path, extraSlots)
                        currentLevel ← nextLevel
                    else
                        break
                    end if
                end while
                return path, currentLevel
            end if
        end for
        currentLevel ← currentLevel + 1
    end while
    return [ ], −1
end procedure
```

5. Simulation Setup

To assess the effectiveness of the proposed D-SQRA algorithms, comprehensive simulations were performed on two research topologies: NSFNET (14 nodes, 21 bidirectional links) and UBN24 (24 nodes, 43 bidirectional links), as shown in Figure 2. Both topologies assume a shared optical fiber infrastructure where quantum and classical channels coexist, reflecting practical future deployment scenarios for QKD networks. The optical spectrum was divided into 40 wavelengths, with 3 wavelengths reserved for QKCh transmissions, 3 wavelengths for MBCh synchronization purposes, and 2 wavelengths serving as a guard

band for channel isolation. The remaining wavelengths were assigned to a traditional data channel (TDCh). Simulations were performed with varying network loads of 100, 200, 300, 400, and 500 CRs [9,26]. The security levels were allocated with a total of 6, 12, and 18 time-slots for high, medium, and low security levels, respectively, to allow security level downgrading or upgrading.



(**a**) NSFNET topology (**b**) UBN24 topology

Figure 2. Network simulation topology.

5.1. Performance Metrics

The proposed and conventional algorithms are evaluated on the following performance metrics:

- **Network Security Performance**: This indicates the weight score by the number of security levels that were successfully assigned to the CR (high = 100; mid = 80; low = 60), normalized according to all the accepted CRs. NSP measures the global security posture of the network. In QKD optical networks, where it is particularly important to have more connections established at a higher security level, higher NSP values are preferable [26,36].
  Let R be the set of all accepted CRs, and $|R|$ be the total number of accepted CRs. For each $r \in R$, let the assigned security level weight w_r be

$$w_r = \begin{cases} 100 & \text{if security level is high} \\ 80 & \text{if security level is mid} \\ 60 & \text{if security level is low} \end{cases}.$$

  Then, the NSP is defined as

$$\text{NSP} = \frac{1}{|R|} \sum_{r \in R} w_r.$$

- **Blocking Probability**: This indicates the percentage of CRs that are rejected because not enough resources (wavelengths, time-slots, or whatever resources modeled) are available. The BP is essential to indicate both network scalability and service quality. A decreased BP means that the network can accommodate more CRs even when the network is heavily loaded, thus delivering better reliability for secure quantum communication [36].
  Let R_{total} be the total number of CRs, and let R_{blocked} be the number of CRs that are rejected due to insufficient resources (e.g., wavelengths or time-slots).
  The **BP** is defined as

$$\text{BP} = \frac{R_{\text{blocked}}}{R_{\text{total}}} \times 100\%.$$

- **Quantum Key Utilization**: It demonstrates the ratio of successfully allocated quantum key resources (time-slots/wavelengths) to the overall available quantum resources. QKU captures the efficiencies in quantum resource utilization in QKChs and MBChs. This is important because quantum resources are limited and expensive, and having a high QKU means that your network is employing quantum resources to (ideally) their utmost value while mandating the least amount of wastage [36].
  Let Q_{used} be the number of successfully allocated quantum key resources (e.g., time-slots or wavelengths), and let Q_{total} be the total number of available quantum key resources.
  The **QKU** is defined as

$$\text{QKU} = \frac{Q_{\text{used}}}{Q_{\text{total}}} \times 100\%.$$

- **Time-Slot Utilization**: This is the ratio of time-slots used for quantum key transmission with respect to the total available time-slots at quantum-related wavelengths. It is a metric of temporal efficiency in the network. Higher utilization means quantum transmissions are better scheduled and synchronized, which has a direct effect on network throughput and latency [36].
  Let T_{used} be the number of time-slots used for quantum key transmission, and let T_{total} be the total number of available time-slots at quantum-related wavelengths.
  The **Time-Slot Utilization** is defined as

$$\text{TSU} = \frac{T_{\text{used}}}{T_{\text{total}}} \times 100\%.$$

5.2. Comparative Analysis

The simulation results show that the proposed D-SQRA significantly outperforms both conventional techniques. The same is described in detail below:

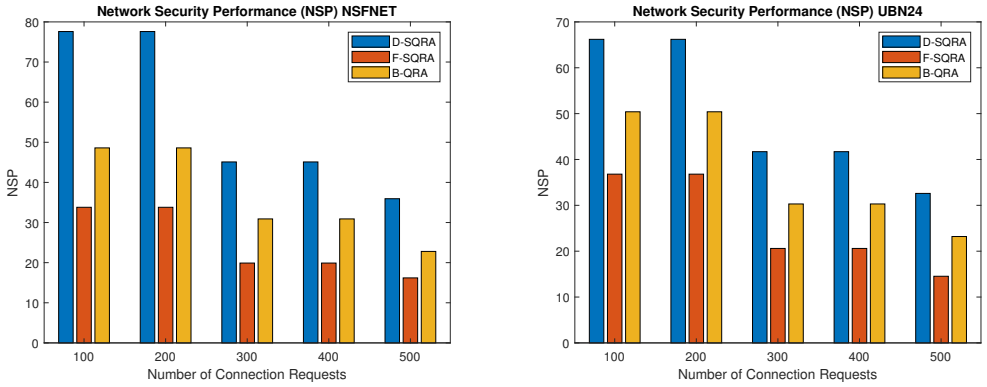
5.2.1. NSP During Security Level Downgrading

The NSP results shown in Figure 3a,b highlight the effectiveness of the D-SQRA protocol in balancing security and connectivity under constrained conditions. D-SQRA consistently outperforms both F-SQRA and B-QRA across varying connection loads, achieving notably higher NSP values. For instance, on the NSFNET topology, D-SQRA maintains an NSP of over 75% at low request volumes (100–200), while F-SQRA and B-QRA remain under 50% due to their inability to adapt to QKD resource shortages.

The strength of D-SQRA lies in its ability to dynamically downgrade the security level when the desired QKD resources are insufficient. This flexibility allows the system to admit more connections at slightly lower security constraints, maintaining the overall quantum protection level while improving request fulfillment. In contrast, F-SQRA strictly enforces security level requirements, leading to higher blocking and a sharp drop in NSP as the load increases. B-QRA, while classical and resource-efficient in general networks, lacks any quantum awareness and thus exhibits inferior NSP in QKD-enabled contexts.

Similar trends are observed in the UBN24 topology. Although the absolute NSP values are lower due to increased topological complexity and traffic competition, D-SQRA still secures the highest performance under all conditions. These findings support the conclusion that security level downgrading is not only a practical adaptation strategy

under limited quantum key availability but is also crucial for preserving network-wide secure communication.



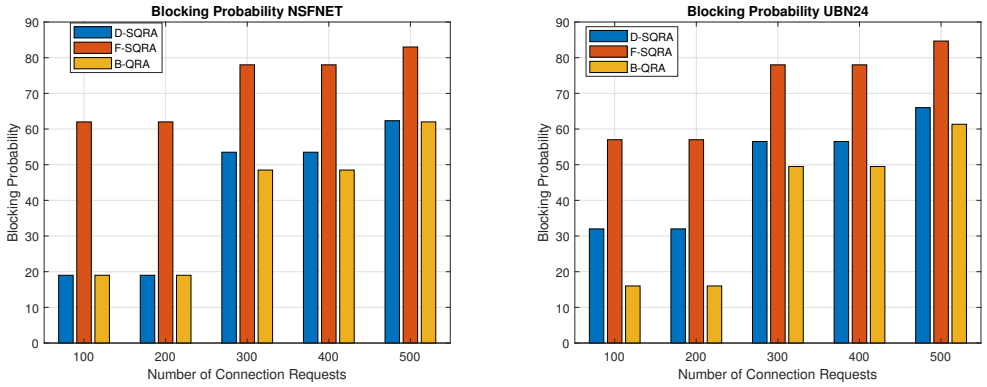
(**a**) NSP on NSFNET topology (**b**) NSP on UBN24 topology

Figure 3. NSP while downgrading security levels.

In comparison to earlier studies such as [9,26], which focused on static key allocations or rigid security assignments, our approach introduces a novel dynamic mechanism that enhances both resource utilization and security effectiveness. Thus, D-SQRA contributes to the development of resilient, scalable QKD-enabled optical networks that maintain high security standards even under high-load and resource-scarce conditions.

5.2.2. BP for Security Level Downgrading

The results presented in Figure 4a,b clearly demonstrate the performance differences among the proposed D-SQRA and the comparison protocols F-SQRA and B-QRA, particularly in terms of BP. Across both the NSFNET and UBN24 topologies, D-SQRA consistently achieves a significantly lower BP than F-SQRA, and in many cases outperforms the classical B-QRA despite its quantum constraints.



(**a**) BP on NSFNET topology (**b**) BP on UBN24 topology

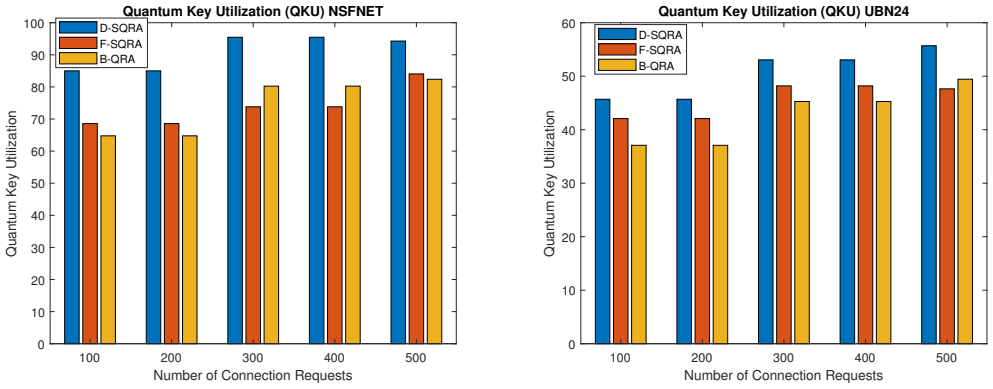
Figure 4. BP while downgrading security levels.

This is particularly notable in high-load scenarios. For instance, at 500 connection requests on NSFNET, D-SQRA maintains a BP of around 62% while F-SQRA reaches approximately 84%. This reduction of more than 20% highlights the effectiveness of dynamic security level adaptation in alleviating resource contention, especially under constrained quantum key conditions. The improvement is even more pronounced on UBN24, where D-SQRA exhibits better scalability and adaptability due to its larger and more meshed structure.

Compared to previous studies such as [9,26], which used fixed security assumptions and static QKD scheduling policies, our approach introduces a flexible adaptation mechanism that balances security requirements with resource availability. The downgrade and upgrade mechanisms enable D-SQRA to intelligently trade-off between stringent key renewal rates and successful admission, which has not been fully explored in earlier resource allocation studies. These results demonstrate that D-SQRA's quantum awareness provides a tangible advantage over both static QKD-secured strategies and purely classical methods.

5.2.3. QKU for Security Level Downgrading

Figure 5a,b present the QKU under varying connection loads on NSFNET and UBN24 topologies, specifically reflecting the impact of the security level downgrading mechanisms implemented in D-SQRA. In both topologies, D-SQRA consistently achieves the highest QKU compared to F-SQRA and B-QRA. This is primarily due to D-SQRA's ability to adaptively downgrade the security level when higher-level key resources are exhausted, thereby avoiding request blocking and ensuring continued utilization of available quantum keys. The policy of adapting the security level allows D-SQRA to maintain quantum key consumption efficiency even as the network load increases.



(**a**) QKU on NSFNET topology (**b**) QKU on UBN24 topology

Figure 5. QKU while downgrading security levels.

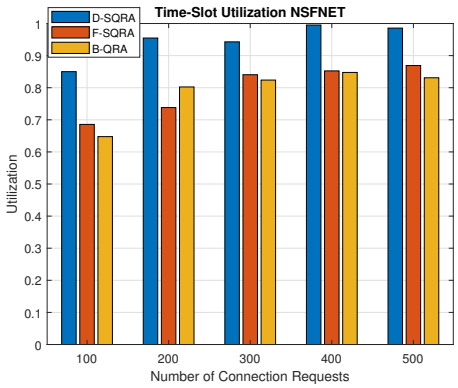
For example, in the NSFNET scenario, D-SQRA maintains the QKU above 90% at all traffic levels, reaching the peak at around 97%, while F-SQRA—restricted by fixed security policies—demonstrates significantly lower utilization (ranging from 70% to 80%). B-QRA shows even lower QKU due to its lack of quantum-aware mechanisms and key scheduling strategies. A similar trend is observed in the UBN24 topology, although utilization values are relatively lower due to the network's larger size and denser traffic matrix.

These results affirm that the security level downgrading mechanism in D-SQRA not only contributes to lowering the BP but also enhances quantum resource efficiency. In contrast, F-SQRA's static allocation strategy leads to the underutilization of available key material. This highlights the practical benefit of dynamic security adaptation in resource-constrained QKD-enabled optical networks, supporting observations from prior studies such as [9,26].

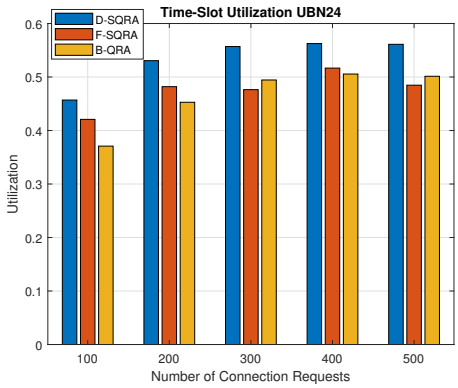
5.2.4. Time-Slot Utilization During Security Level Downgrading

Figure 6a shows that in the NSFNET topology, D-SQRA consistently achieves the highest time-slot utilization, reaching near-optimal levels (above 0.95) as traffic load increases. This demonstrates its ability to flexibly allocate available time-slots by dynamically downgrading security levels under constrained conditions, ensuring fewer resources are wasted and more requests are admitted. F-SQRA and B-QRA lag behind, especially at low

request volumes, due to their rigid or classical security constraints, which restrict time-slot reallocation efficiency.



(**a**) Time-slot utilization on NSFNET topology



(**b**) Time-slot utilization on UBN24 topology

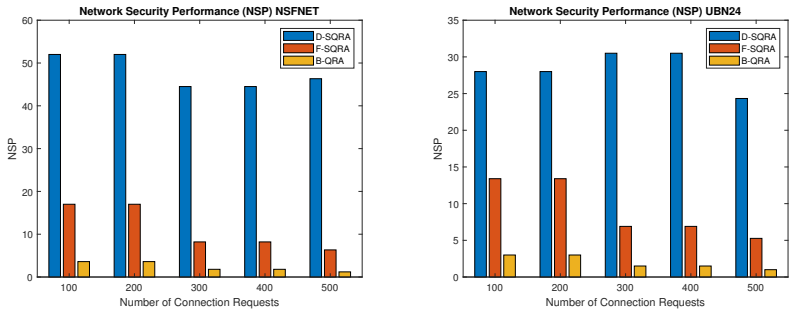
Figure 6. Time-slot utilization while downgrading security levels.

On UBN24, shown in Figure 6b, a more complex topology, the overall time-slot utilization values are lower across all protocols due to increased path lengths and contention. However, D-SQRA still maintains a clear advantage, showing over 55% utilization at high request loads. This reinforces the value of adaptive security strategies in dense quantum-enabled optical networks.

5.2.5. NSP During Security Level Upgrading

Network Security Performance Under Security Level Upgrading

Figure 7a,b illustrate the NSP for the D-SQRA, F-SQRA, and B-QRA protocols under security level upgrading in both the NSFNET and UBN24 topologies. D-SQRA consistently outperforms the other two protocols by maintaining significantly higher NSP values across all traffic loads. Specifically, in the NSFNET topology, D-SQRA sustains NSP values above 45, while F-SQRA falls below 18 and B-QRA drops below 5. A similar trend is seen in the UBN24 topology, where D-SQRA achieves an NSP of around 30 at peak load, in contrast to under 15 for F-SQRA and below 4 for B-QRA. This performance advantage stems from D-SQRA's adaptive upgrade mechanism, which allows it to opportunistically elevate requests to higher security levels when excess quantum key material is available, thus enhancing the cryptographic strength of admitted flows without increasing the BP. F-SQRA's rigid policy precludes such upgrades, and B-QRA lacks quantum security capabilities altogether. These results confirm that D-SQRA not only optimizes resource utilization but also enhances security outcomes dynamically, positioning it as a scalable and forward-looking solution for QKD-integrated optical networks. This observation aligns with recent findings in Chen et al. [9], reinforcing the value of security-aware adaptive control in optical data center networks.

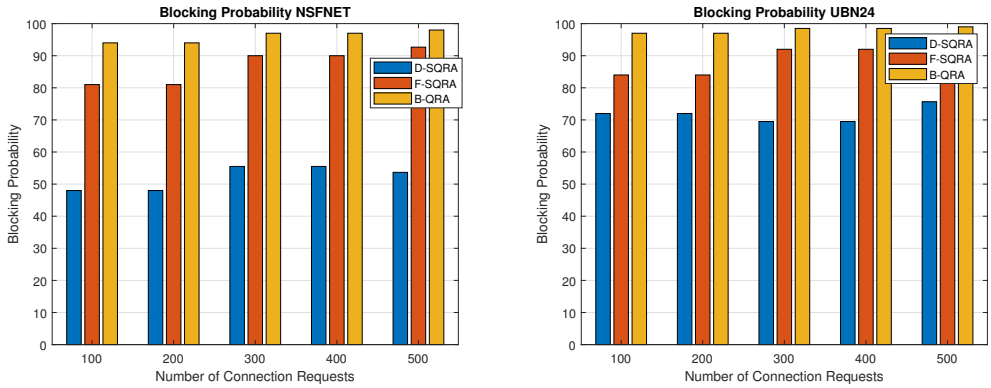


(**a**) (**b**)

Figure 7. NSP while upgrading security levels. (**a**) NSFNET topology. (**b**) UBN24 topology.

5.2.6. BP During Security Level Upgrading

Figure 8a,b above illustrate the BP trends under security level upgrading for the three strategies, D-SQRA, F-SQRA, and B-QRA, across two topologies—NSFNET and UBN24. Across both topologies, we observe that D-SQRA consistently maintains a lower BP compared to F-SQRA and B-QRA, even in scenarios where requests are upgraded to higher security levels. This is a crucial outcome, as it shows that D-SQRA is not only efficient at serving requests under constrained resources (as shown in the downgrade-based BP results) but also adaptively utilizes surplus quantum key resources to upgrade security levels without significantly compromising admission rates.



(**a**) BP on NSFNET topology (**b**) BP on UBN24 topology

Figure 8. BP while upgrading security levels.

In NSFNET, D-SQRA maintains a BP around 50%, while F-SQRA and B-QRA exhibit much higher rates (above 80%) across varying request volumes. This difference becomes even more noticeable in the UBN24 topology, where network complexity and path diversity increase. Here, D-SQRA achieves significantly better request accommodation despite actively upgrading the security level when resources permit. This validates the advantage of our dynamic approach: instead of strictly following a fixed security model (F-SQRA) or relying on classical routing without quantum awareness (B-QRA), D-SQRA intelligently balances between enhancing security and minimizing request rejections.

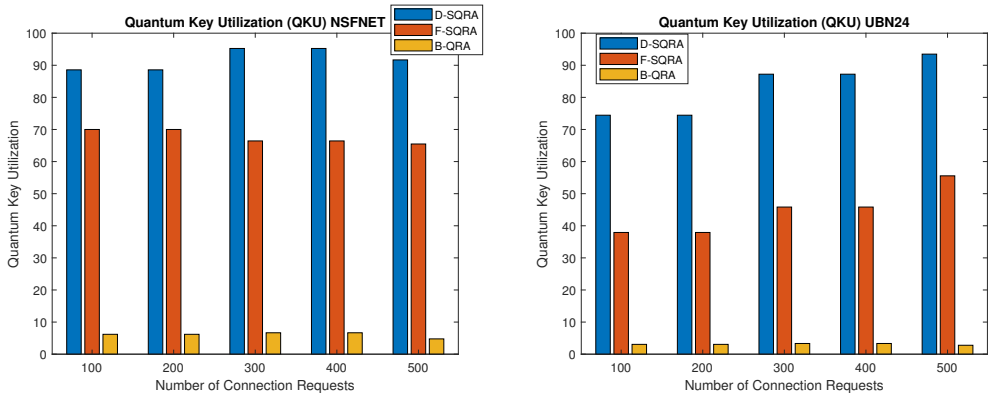
From a broader perspective and in line with recent studies such as [9], the proposed model distinguishes itself by actively reacting to real-time key availability, outperforming traditional approaches in adaptability and network utility. The improvement is particularly meaningful under high-load conditions where key buffer optimization and security trade-offs become critical. These findings underline the practical value of D-SQRA in supporting scalable and resilient QKD-enabled networks, offering a groundbreaking shift from static or classical methods toward dynamic, quantum-capable security management.

5.2.7. QKU During Security Level Upgrading

From Figure 9a,b, the D-SQRA approach demonstrates consistently high QKU, exceeding 90% in the NSFNET topology and reaching up to 95% in UBN24 as the number of connection requests increases. This significant utilization level reflects D-SQRA's ability to dynamically adapt and elevate security levels (from SL-1 and SL-2) when surplus quantum key resources are available. Such proactive upgrades increase QKCh and MBCh consumption, indicating that the system not only accepts more connections but also strengthens its security guarantees by maximizing the use of quantum key buffers.

In contrast, the F-SQRA protocol, which fixes security levels, shows moderate utilization (below 70% in NSFNET and rising to approximately 55% in UBN24), suggesting it cannot exploit additional key material even when available. B-QRA's utilization remains the lowest across all request loads, as it does not leverage QKD resources at all.

These findings reinforce that D-SQRA introduces a quantum-aware upgrade mechanism absent in the alternative schemes, effectively optimizing secure resource consumption and pushing the practical boundaries of quantum-assisted communication. Thus, the results not only outperform existing benchmarks but also offer novel value in resource-constrained QKD deployments.



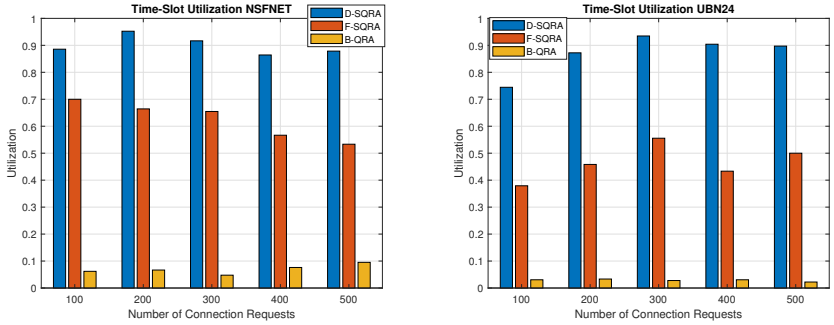
(**a**) QKU on NSFNET topology (**b**) QKU on UBN24 topology

Figure 9. QKU while upgrading security levels.

5.2.8. Time-Slot Utilization During Security Level Upgrading

Figure 10a,b illustrate the time-slot utilization under security level upgrading in both the NSFNET and UBN24 topologies for the D-SQRA, F-SQRA, and B-QRA schemes. In both topologies, D-SQRA consistently outperforms the other two schemes in terms of time-slot utilization. This improvement is attributed to its adaptive upgrade mechanism, which intelligently exploits available quantum and classical channel resources to elevate connection requests to higher security levels whenever the system detects spare key capacity. As a result, more secure keys are actively utilized, leading to denser and more efficient time-slot allocations.

In contrast, F-SQRA, which operates under fixed security constraints, demonstrates relatively stable but lower utilization levels due to its rigid allocation policy. It neither downgrades nor upgrades requests, which limits its adaptability in dynamic traffic environments. B-QRA, being a classical routing approach, exhibits very low time-slot utilization since it does not actively engage with QKD resource scheduling and only marginally consumes quantum-related slots.



(**a**) Time-slot utilization on NSFNET topology (**b**) Time-slot utilization on UBN24 topology

Figure 10. Time-slot utilization while upgrading security levels.

Overall, these results highlight that D-SQRA achieves superior time-slot efficiency by dynamically upgrading requests based on real-time resource conditions, which aligns with its goal of maximizing the utilization of the secure channel. This is particularly critical for future QKD-enabled networks, where efficient and adaptive resource management will be key to ensuring both scalability and security-aware performance [9].

5.3. Results Discussion

The proposed D-SQRA algorithm demonstrates significant performance advantages over both F-SQRA and B-QRA on a comprehensive set of evaluation metrics, including BP, NSP, QKU, and time-slot utilization. By dynamically adjusting security levels, downgrading under resource constraints, and upgrading when surplus quantum key resources are available, D-SQRA achieves an effective balance between resource efficiency and security assurance.

Compared to the fixed-policy F-SQRA and the classical, non-quantum-aware B-QRA, D-SQRA reduces the BP by more than 20% in high load scenarios, particularly in complex and meshed topologies such as UBN24. In terms of NSP, D-SQRA consistently maintains the highest security coverage by opportunistically elevating the security level of admitted requests based on real-time QKD buffer conditions. Moreover, it maintains QKU above 90% and demonstrates near-optimal time-slot utilization, reflecting robust and intelligent management of quantum resources. These results reinforce the protocol's quantum awareness and adaptive decision-making capabilities, aligning with and extending beyond previous studies by [9,26], which relied on static security-level assumptions or baseline quantum routing heuristics.

In the broader context of QKD network deployment, [37] emphasized the limitations of static quantum key allocation schemes in meeting the scalability and performance demands of future networks. The proposed D-SQRA framework addresses these limitations directly through security-level reconfigurations based on the current state of the network, enabling more effective mitigation of quantum key exhaustion while ensuring end-to-end confidentiality.

Furthermore, as discussed by [38], traditional QKD systems often operate under fixed session structures and idealized key consumption assumptions, which can lead to underperformance under real-world conditions. In contrast, D-SQRA introduces operational flexibility by dynamically adapting key usage according to network dynamics, thereby improving the practicality and deployability of QKD in optical backbone networks.

Overall, D-SQRA represents a significant advance in the allocation of QKD-enabled resources. Its integration of SDN control with adaptive quantum resource logic enables it to outperform existing protocols under both performance and security objectives with a minimal increase in computational complexity. These results validate the scalability of the

protocol and make it a strong candidate for practical implementation in next-generation quantum secure communication infrastructures.

5.3.1. Overhead Introduced by D-SQRA

The proposed D-SQRA protocol introduces measurable overhead due to its adaptive security-level mechanism. This overhead is observed in the control and management operations required to reconfigure requests when resource contention or key scarcity occurs. Specifically, D-SQRA induces the following:

- **Security Downgrades:** Requests that cannot be served at their initial security level are reassigned to a lower level, leading to an increase in downgrade operations. This enables higher request acceptance at the cost of minimal security relaxation.
- **Control Plane Signaling:** Each downgrade or upgrade triggers updates to the key managers and MBCh handlers, requiring additional signaling across the SDN controller and QKD plane.
- **Key Buffer Updates and Reallocations:** Dynamic reassignment of QKCh and MBCh time-slots leads to multiple key buffer updates and reallocation attempts, increasing computational and synchronization overhead.

Figure 11 above shows the control plane and operational overhead introduced by the D-SQRA protocol under increasing request loads. The x-axis shows the number of connection requests (100 to 500), while the y-axis indicates the count of overhead events observed during the simulation. This means that as the number of CRs increases, the number of overhead operations, such as security downgrades/upgrades, reallocation calls, control plane messages, and key buffer updates, scales accordingly.

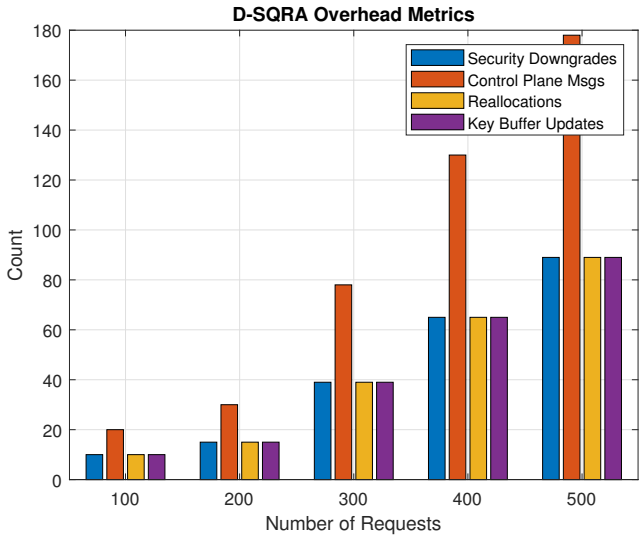


Figure 11. D-SQRA overhead metrics under increasing traffic load.

5.3.2. Computational Complexity Analysis of D-SQRA

The D-SQRA protocol shares a similar worst-case asymptotic complexity with F-SQRA and B-QRA, expressed as

$$\mathcal{O}(R \cdot K \cdot l \cdot W \cdot T),$$

where R is the number of connection requests, K is the number of candidate paths per request, l is the average path length, W is the number of wavelengths, and T is the number of time-slots per channel. This reflects the nested loop structure of the protocol, in which each request examines multiple candidate paths and iteratively scans wavelengths and time-slots for availability [9,24,39].

However, D-SQRA incurs higher *practical runtime complexity* than its counterparts. This is due to the following reasons:

- **Security-Level Adaptation Logic:** For each request, D-SQRA attempts allocation across multiple security levels, restarting the allocation process upon each downgrade. This leads to repeated invocations of the wavelength and time-slot check logic.
- **Reallocation Attempts:** Additional cycles are consumed for each reallocation trial after a downgrade or upgrade, further increasing the time-slot checking operations.
- **SDN Interaction Overhead:** D-SQRA's decisions involve updates across the SDN control plane, which introduces delays in message synchronization and state updates.

From Figure 12 above it shows that the number of path evaluations scales similarly across D-SQRA, F-SQRA, and B-QRA protocols as the number of connection requests increases.

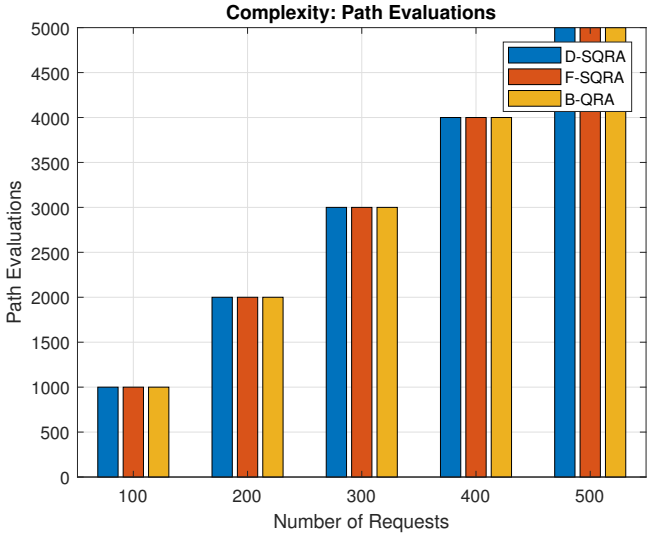


Figure 12. Comparison of path evaluations across D-SQRA, F-SQRA, and B-QRA protocols.

As shown in Figure 13, D-SQRA results in the highest runtime per request due to its adaptive mechanism involving repeated fallback attempts, time-slot scanning, path reevaluation, and control plane synchronization. F-SQRA, enforcing fixed security constraints without fallback, achieves a lower runtime than D-SQRA by avoiding repeated checks. Notably, B-QRA has the lowest runtime since it bypasses QKD processes entirely and does not manage quantum key resources or related signaling overhead. These results indicate that while all protocols share the same asymptotic complexity, practical runtime is strongly influenced by protocol behavior and quantum-layer operations, especially in adaptive QKD-aware schemes like D-SQRA.

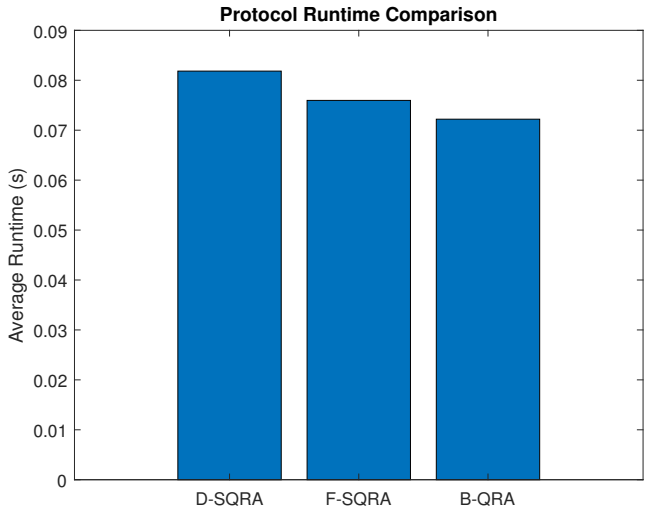


Figure 13. Average protocol runtime per request across D-SQRA, F-SQRA, and B-QRA strategies.

6. Conclusions

In this paper, we proposed the D-SQRA algorithm, which aims to maximize resource utilization of QKD-enabled optical networks at dynamic security levels. The simulation results of the NSFNET and UBN24 topologies clearly indicated that D-SQRA can outperform F-SQRA and B-QRA under various performance metrics, which are NSP, BP, QKU, and time-slot utilization. With its ability to handle not only downgrades but also upgrades of security levels in real time, D-SQRA enables better resource utilization, assisting in meeting security needs appropriately. This adaptive capability allows performance optimization without sacrificing communication channel security, as network resource demand varies over time. In addition, the proposed D-SQRA across different topologies shows its applicability in a variety of network configurations. The proposed D-SQRA proves itself to be a powerful solution that guarantees significant security while using fewer computing resources, which is more important than ever in the face of increasing demand for secure communication in the wake of new security threats.

Future work will include analytical modeling of BPs using probabilistic traffic arrival processes, such as Poisson or semi-static models, and the derivation of worst-case or average-case bounds on NSP based on resource availability and the statistical distribution of request security levels. Additionally, we plan to conduct a complexity analysis and evaluate the approximation performance of the proposed allocation strategies. The flexibility of the D-SQRA framework makes it a promising candidate for practical deployment in operational networks and integration with next-generation infrastructures. We believe that D-SQRA can serve as a foundation for further research aimed at enhancing security-aware resource allocation in quantum communication networks, a field that continues to evolve rapidly.

Author Contributions: Conceptualization, A.K.; Methodology, A.K. and B.C.; Software, A.K.; Validation, A.K. and V.B.; Formal analysis, A.K.; Investigation, A.K.; Resources, A.K. and V.B.; Data curation, A.K.; Writing—original draft, A.K.; Writing—review & editing, V.B. and B.C.; Visualization, A.K.; Supervision, V.B. and B.C.; Project administration, V.B. All authors have read and agreed to the published version of the manuscript.

Funding: The financial support from ICCR, MeitY, and Chair Professorship from Soochow University for this work is rightly acknowledged.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: We acknowledge the financial support from the ICCR, MeitY, and Soochow University for this work.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shandilya, S.K.; Datta, A.; Kartik, Y.; Nagar, A. Thriving in the Quantum Era. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 401–458.
2. Sergienko, A.V. *Quantum Communications and Cryptography*; CRC Press: Boca Raton, FL, USA, 2018.
3. Neway, A.S. *Beyond the Bit: A Guide to Quantum Computing and Its Impact*; Amazon Kindle Direct Publishing Edition: Seattle, WA, USA, 2024.
4. Amanzholova, S.; Priyanka, A.C. Exploring advancements, applications, and challenges in the realm of quantum cryptography. *Next Gener. Mech. Data Encryption* **2025**, *2025*, 116.
5. Yu, X.; Ning, X.; Zhu, Q.; Lv, J.; Zhao, Y.; Zhang, H.; Zhang, J. Multi-Dimensional Routing, Wavelength, and Timeslot Allocation (RWTA) in Quantum Key Distribution Optical Networks (QKD-ON). *Appl. Sci.* **2020**, *11*, 348. [CrossRef]
6. Zhao, Y.; Cao, Y.; Yu, X.; Zhang, J.; Morozov, O. Quantum Key Distribution (QKD) over Software-Defined Optical Networks. *Quantum Cryptogr. Adv. Networks* **2019**, *1*, 13.
7. Sharma, P.; Agrawal, A.; Bhatia, V.; Prakash, S.; Mishra, A.K. Quantum key distribution secured optical networks: A survey. *IEEE Open J. Commun. Soc.* **2021**, *2*, 2049–2083. [CrossRef]
8. Zhang, Q.; Ayoub, O.; Gatto, A.; Wu, J.; Musumeci, F.; Tornatore, M. Routing, channel, key-rate, and time-slot assignment for QKD in optical networks. *IEEE Trans. Netw. Serv. Manag.* **2023**, *21*, 148–160. [CrossRef]
9. Chen, B.; Ma, W.; He, B.; Chen, H.; Jiang, M.; Shao, W.; Gao, M.; Peng, L.; Ho, P.H.; Jue, J.P. Resource Allocation in Quantum-Key-Distribution Optical Data Center Networks. *J. Light. Technol.* **2025**, *43*, 5086–5099. [CrossRef]
10. Xiao, Q.; Zhao, J.; Feng, S.; Li, G.; Hu, A. Securing NextG networks with physical-layer key generation: A survey. *Secur. Saf.* **2024**, *3*, 2023021. [CrossRef]
11. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 839–894. [CrossRef]
12. Li, Y.; Zhang, H.; Zhang, C.; Huang, T.; Yu, F.R. A Survey of Quantum Internet Protocols From a Layered Perspective. *IEEE Commun. Surv. Tutorials* **2024**, *26*, 1606–1634. [CrossRef]
13. Masoudi, R.; Ghaffari, A. Software defined networks: A survey. *J. Netw. Comput. Appl.* **2016**, *67*, 1–25. [CrossRef]
14. Mendez, R.B.; Buruaga, J.S.; Vicente, R.J.; Mengual, L.; Pastor, A.; Muñiz, A.; Morales, J.; Canto, R.; Folgueira, J.; Lopez, D.R.; et al. SDN-Based Hybrid Quantum-Safe Domain Intercommunication Within MadQCI. In Proceedings of the 2024 International Conference on Quantum Communications, Networking, and Computing (QCNC), Kanazawa, Japan, 1–3 July 2024; pp. 168–175.
15. Aguado, A.; Hugues-Salas, E.; Haigh, P.A.; Marhuenda, J.; Price, A.B.; Sibson, P.; Kennard, J.E.; Erven, C.; Rarity, J.G.; Thompson, M.G.; et al. Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared QKD Resources. *J. Light. Technol.* **2017**, *35*, 1357–1362. [CrossRef]
16. Cao, Y.; Zhao, Y.; Wu, Y.; Yu, X.; Zhang, J. Time-scheduled quantum key distribution (QKD) over WDM networks. *J. Light. Technol.* **2018**, *36*, 3382–3395. [CrossRef]
17. Yu, Y.; Zhang, J.; Zhao, Y.; Cao, X.; Lin, X.; Gu, W. The first single-link exact model for performance analysis of flexible Grid WDM networks. In Proceedings of the 2013 Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), Anaheim, CA, USA, 17–21 March 2013; p. JW2A-68.
18. Aziz, M.B. High-Speed Optical Interconnects in Harsh Environments. Master's Thesis, Chalmers Tekniska Hogskola, Göteborg, Sweden, 2024.
19. Sharma, A.; Chaudhary, S.; Parnianifard, A. Introduction to Advances in Optical and Wireless Communication. In *Optical and Wireless Communications: Applications of Machine Learning and Artificial Intelligence*; CRC Press: New Delhi, India, 2025; pp. 1–38.
20. Saridis, G.M.; Alexandropoulos, D.; Zervas, G.; Simeonidou, D. Survey and Evaluation of Space Division Multiplexing: From Technologies to Optical Networks. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2136–2156. [CrossRef]
21. Richardson, D. New optical fibres for high-capacity optical communications. *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2016**, *374*, 20140441. [CrossRef]
22. Mehic, M.; Niemiec, M.; Rass, S.; Ma, J.; Peev, M.; Aguado, A.; Martin, V.; Schauer, S.; Poppe, A.; Pacher, C.; et al. Quantum key distribution: A networking perspective. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–41. [CrossRef]
23. Cao, Y.; Zhao, Y.; Yu, X.; Wu, Y. Resource Assignment Strategy in Optical Networks Integrated With Quantum Key Distribution. *J. Opt. Commun. Netw.* **2017**, *9*, 995–1004. [CrossRef]

24. He, B.; Zheng, N.; Lu, Y.; Chen, H.; Gao, M.; Shao, W.; Peng, L.; Ho, P.H.; Chen, B. Quantum Key Service Provisioning in QKD-Enabled Optical Networks. In Proceedings of the GLOBECOM 2024—2024 IEEE Global Communications Conference, Cape Town, South Africa, 8–12 December 2024; pp. 4406–4411. [CrossRef]
25. Ruiz, L.; Garcia-Escartin, J.C. Routing and wavelength assignment in hybrid networks with classical and quantum signals. *IEEE J. Sel. Areas Commun.* **2025**, *43*, 412–421. [CrossRef]
26. Ma, W.; Liu, L.; Chen, B.; Gao, M.; Chen, H.; Wu, J. Routing, Wavelength and Time-Slot Assignment Approaches with Security Level in QKD-Enabled Optical Networks. In Proceedings of the 2020 Asia Communications and Photonics Conference (ACP) and International Conference on Information Photonics and Optical Communications (IPOC), Beijing, China, 24–27 October 2020; pp. 1–3.
27. Ma, W.; Chen, B.; Liu, L.; Chen, H.; Shao, W.; Gao, M.; Wu, J.; Ho, P.H. Equilibrium Allocation Approaches of Quantum Key Resources With Security Levels in QKD-Enabled Optical Data Center Networks. *IEEE Internet Things J.* **2022**, *9*, 25660–25672. [CrossRef]
28. Kong, W.; Sun, Y.; Tang, J.; Gao, Y.; Dou, T.; Li, Z.; Xie, Y.; Zhao, Q.; Chen, N. Resource Allocation in Twin-Field QKD Coexisting With Classical Communication Over Multicore Fiber. *J. Light. Technol.* **2024**, *43*, 1032–1042. [CrossRef]
29. Calvo-Salcedo, A.F.; González, N.G.; Jaramillo-Villegas, J.A. Dynamic Spectrum Assignment in Passive Optical Networks Based on Optical Integrated Microring Resonators Using Machine Learning and a Routing, Modulation Level, and Spectrum Assignment Method. *Appl. Sci.* **2023**, *13*, 13294. [CrossRef]
30. Zhao, T.; Fan, X.; Dong, B.; Niu, Q.; Guo, B. A Resource-Adaptive Routing Scheme with Wavelength Conflicts in Quantum Key Distribution Optical Networks. *Entropy* **2023**, *25*, 732. [CrossRef]
31. Ruan, L.; Luo, H.; Liu, C. A dynamic routing algorithm with load balancing heuristics for restorable connections in WDM networks. *IEEE J. Sel. Areas Commun.* **2004**, *22*, 1823–1829. [CrossRef]
32. Randhawa, R.; Sohal, J. Static and dynamic routing and wavelength assignment algorithms for future transport networks. *Optik* **2010**, *121*, 702–710. [CrossRef]
33. Wang, F.; Yan, F.; Xue, X.; Liu, B.; Zhang, L.; Zhang, Q.; Xin, X.; Calabretta, N. Traffic Load Balancing based on Probabilistic Routing in Data Center Networks. In Proceedings of the 2020 International Conference on Optical Network Design and Modeling (ONDM), Barcelona, Spain, 18–21 May 2020; pp. 1–3.
34. Thomas, J.M.; Kanter, G.S.; Kumar, P. Designing noise-robust quantum networks coexisting in the classical fiber infrastructure. *Opt. Express* **2023**, *31*, 43035–43047. [CrossRef] [PubMed]
35. Alia, O.; Tessinari, R.S.; Bahrani, S.; Bradley, T.D.; Sakr, H.; Harrington, K.; Hayes, J.; Chen, Y.; Petropoulos, P.; Richardson, D.; et al. DV-QKD Coexistence With 1.6 Tbps Classical Channels Over Hollow Core Fibre. *J. Light. Technol.* **2022**, *40*, 5522–5529. [CrossRef]
36. Bi, L.; Miao, M.; Di, X. A dynamic-routing algorithm based on a virtual quantum key distribution network. *Appl. Sci.* **2023**, *13*, 8690. [CrossRef]
37. Lella, E.; Schmid, G. On the security of quantum key distribution networks. *Cryptography* **2023**, *7*, 53. [CrossRef]
38. Yuen, H.P. Security of Quantum Key Distribution. *IEEE Access* **2016**, *4*, 724–749. [CrossRef]
39. McCool, M.; Robison, A.D.; Reinders, J. *Structured Parallel Programming: Patterns for Efficient Computation*; Morgan Kaufmann: Burlington, MA, USA, 2012.