IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 27 January 2026, accepted 7 February 2026, date of publication 12 February 2026, date of current version 19 February 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3664094

RESEARCH ARTICLE

Quantum Key Distribution Network Simulator With Hyperparameter Tuning for Realistic Performance Analysis

JU-BONG KIM[1], HYUN-KYO LIM[1], (Member, IEEE), WONHYUK LEE[1], DAHYUN YUM[2], AND CHANKYUN LEE[1], (Member, IEEE)

[1]Korea Institute of Science and Technology Information (KISTI), Yuseong, Daejeon 34141, South Korea
[2]ID Quantique Ltd., Bundang-gu, Gyeonggi-do 13595, South Korea

Corresponding author: Chankyun Lee (chankyunlee@kisti.re.kr)

This work was supported in part by Korea Institute of Science and Technology Information (KISTI) under Grant K26L1M3C5, and in part by the Institute of Information and Communications Technology Planning and Evaluation (IITP) funded by Korean Government (MSIT) under Grant RS-2025-02263666.

ABSTRACT Realistic simulation of quantum key distribution (QKD) networks requires a combination of precise models of quantum channels and network functions. Unfortunately, existing QKD network simulators lack either rigorous quantum physics modeling or network key-management and routing protocols, which limit their practical applicability. To address this limitation, we propose a QKD network simulator with hyperparameter tuning (QKDSim-HT), a NetSquid-based simulator specialized for polarization-based discrete-variable QKD networks. Specifically, QKDSim-HT models properties in quantum physics (photon loss, polarization-dependent depolarization, detector inefficiencies, dark counts, and dead times) as well as advanced functionalities in networking algorithms (multi-hop key relay and adaptive routing). Extensive simulations over diverse topologies reveal that the networking performance varied with respect to the fundamental properties of quantum physics, such as depolarization, fiber length, and channel attenuation. As a representative use case of QKDSim-HT, simulation results from QKDSim-HT over simple examples clearly manifest that a design of QKD networks highly affects performance of the networks. Accordingly, QKDSim-HT can serve as a practical platform for performance evaluation and optimization of quantum secured network.

INDEX TERMS Quantum key distribution (QKD), QKD networks, quantum key relay, QKD network simulator.

I. INTRODUCTION

Quantum key distribution (QKD) enables information-theoretically secure communication by leveraging fundamental principles of quantum mechanics to detect eavesdropping on transmitted quantum states. Although early experimental QKD networks (QKDNs), such as DARPA [1] and SECOQC [2], confirmed the feasibility of secure quantum communications, they also revealed practical limitations. Recently deployed advanced QKDNs, including MadQCI [3] and the coherent quantum network in Germany [4], have sought to overcome these limitations by integrating more scalable and practical architectures. The primary challenges identified include expensive quantum optical equipment, substantial photon losses, polarization-dependent depolarization, and noise that critically degrade key quality, particularly over long-distance optical fiber links [5]. Consequently, accurate and comprehensive simulation tools have become indispensable for researchers and network designers to rigorously analyze, evaluate, and optimize quantum network architectures prior to costly physical deployments [6].

The associate editor coordinating the review of this manuscript and approving it for publication was Kashif Sharif.

Existing simulation approaches for QKDNs can be broadly categorized into two classes. The first category encompasses simulators with a strong emphasis on detailed quantum-layer modeling, notably NetSquid [7], which accurately represents critical quantum-layer effects such as photon loss, depolarization, dephasing errors, and realistic detector behaviors. A BB84 implementation study [8] based on Qiskit [9], a general-purpose quantum computing framework, focuses on protocol-level simulation and does not provide comprehensive network-oriented functionalities. Consequently, it does not address essential features such as multi-hop key relay mechanisms [10], detailed key-management operations, or realistic network-level implementations necessary for practical QKDN evaluation. In contrast, the second category consists of network-oriented simulators built upon classical network simulation frameworks, such as QKDN simulator (QKDNetSim) [11] and QKDNetSim+ [13], which offer robust key-management schemes, multi-hop key relay mechanisms, and classical network integration. However, these simulators frequently abstract essential quantum-layer effects, resulting in overly simplified and unrealistic estimations of critical performance metrics, including quantum bit error rate (QBER) and secure key rates. Therefore, there is a clear need for an integrated simulation platform that combines high-fidelity quantum-layer modeling with comprehensive network-level functionalities to support realistic evaluation and design of QKDN architectures.

In this paper, we propose a QKDN simulator with hyperparameter tuning (QKDSim-HT), a novel NetSquid-based simulator specifically designed for QKDNs implementing polarization-based discrete-variable (DV)-QKD protocols, particularly the widely used BB84, E91 [14], and decoy-state schemes. In this work, the term hyperparameter tuning denotes configurable adjustment of quantum-layer and device-dependent parameters to ensure that the simulator reflects realistic QKD system conditions. We focus on polarization-based DV-QKD protocols because they are commercially deployed and provide well-specified device parameters (e.g., IDQ systems [31]), which allows the simulator to be validated under practical operating conditions. Continuous-variable (CV)-QKD and measurement-device-independent (MDI)-QKD require physical models that differ fundamentally from polarization-based DV schemes, and thus remain beyond the present scope of the simulator. The modular design of QKDSim-HT permits these protocols to be added as separate modules when their inclusion becomes appropriate.

Our simulator uniquely integrates detailed quantum-layer modeling, including channel loss, polarization depolarization, dephasing, and realistic detector imperfections, with advanced network functionalities such as multi-hop quantum key relay and comprehensive protocol implementations. This integration provides trustworthy simulation environment to the QKDN community to test and optimize QKDN under various realistic operational conditions. Specifically, the key contributions of our work are threefold:

- We provide rigorous quantum-layer models specifically tailored for realistic QKDN conditions, such as distance-dependent photon loss, polarization depolarization, dephasing errors, finite detector efficiency, dark counts, and detector dead times. These models leverage the quantum optical modules available in NetSquid. Compared to existing QKDN simulators which rely on simplified abstractions of quantum-layer, proposed QKDSim-HT provides precise quantum-layer models and thus improves the validity of performance evaluations for QKDN.
- In order to support advanced network algorithms in QKDN, QKDSim-HT further addresses the limitations of existing QKD simulators that typically employ simplified networking models. Based on the NetSquid simulator, QKDSim-HT integrates comprehensive network-oriented functionalities such as multi-hop key relay, adaptive routing, and advanced key-management.
- Extensive simulations on benchmark topologies quantify how critical quantum-layer parameters, such as depolarization rate, link length, and fiber attenuation, affect performance of QKDN. The simulation results clearly identify the importance of an effective QKDN design to achieve an acceptable QKDN network performance. In addition, systematic hyperparameter tuning provides empirical guidelines for rigorous performance analysis of realistic QKDN scenarios.

Through these advancements, QKDSim-HT substantially enhances the accuracy and effectiveness of QKDN simulations and bridges the critical gap between detailed quantum-layer models and comprehensive network-level functionality. Consequently, QKDSim-HT offers insights into how quantum-layer imperfections and network topology shape the performance and reliability of QKDNs, supporting the effective design of practical quantum-secure communication infrastructures. It serves as a tool for evaluating the end-to-end impact of quantum-layer properties and network architectures in realistic deployment scenarios.

The remainder of this paper is organized as follows. Section II reviews existing QKDN simulators and analyzes their strengths and limitations to clearly demonstrate the necessity for the proposed simulator. Section III presents the simulation structure of the proposed QKDSim-HT, including its quantum processors, quantum state encoding, detection models, and quantum and classical channel implementations. Section IV describes our simulation methodology, which includes quantum state preparation, basis reconciliation, error-correction, secure key generation, and key relay operations. Section V provides extensive simulation results that evaluate how quantum-layer parameters affect QKD performance metrics and analyze the influence of network topology. Finally, Section VI summarizes our key findings

TABLE 1. Technical comparison of existing QKDN Simulators and the proposed QKDSim-HT.

Simulator	Quantum-layer modeling	Quantum source & detector modeling	Key-management	Multi-hop key relay	Adaptive routing support
Parallel discrete-event simulation [15]	Simplified abstraction	Minimal	Basic	No	No
QKDNetSim [11]	Simplified abstraction	Minimal	Basic	No	No
Large-scale QKDNetSim [16]	Simplified abstraction	Minimal	**Advanced**	**Yes**	**Yes**
QKDNetSim+ [13]	Simplified abstraction	Minimal	**Advanced**	**Yes**	No
QSCN simulation [17]	**Detailed** (GLLP-based)	**Realistic**	Basic	No	No
Dissipative dynamics in QKD [18]	**Detailed** (Jaynes–Cummings-based)	**Realistic**	Basic	No	No
QKDSim-HT (proposed)	**Detailed** (NetSquid-based)	**Realistic**	**Advanced**	**Yes**	**Yes**

and discusses the implications of QKDSim-HT for practical QKDN design and optimization.

II. RELATED WORKS

QKDNs leverage fundamental quantum principles to achieve information-theoretically secure communication by enabling the detection of eavesdropping [19]. Due to the considerable costs, technical complexity, and practical limitations involved in deploying real-world QKDNs, simulation tools have become essential for designing, testing, and optimizing these networks before costly physical implementations [16]. To comprehensively evaluate and enhance QKDN architectures, accurate and robust simulation tools are necessary, which can realistically model quantum-layer effects, quantum hardware components, and critical network functionalities such as key-management and multi-hop routing [20].

This section presents a comparative analysis of six representative QKDN simulators. Each simulator focuses on different aspects of network modeling and contributes distinct capabilities. We identify their strengths and limitations to highlight the need for the proposed simulator QKDSim-HT.

A. DETAILED REVIEW OF EXISTING QKDN SIMULATORS

1) PARALLEL DISCRETE-EVENT SIMULATION [15]

This simulation emphasizes scalability using parallel discrete-event simulation, with the aim of efficiently handling large-scale QKDNs. While highly effective for simulating extensive network configurations, its approach abstracts key quantum-layer effects. Crucial quantum-layer effects such as photon depolarization, detector imperfections, and dephasing are simplified, which limits the accuracy and predictive reliability of its simulations.

2) QKDNetSim [11]

Built on the network simulator 3 (NS-3) classical framework [12], the QKDNetSim provides basic functionalities for key synchronization and static routing protocols. However, it simplifies the quantum-layer modeling, neglecting critical quantum effects such as detailed depolarization and detector errors. Consequently, it struggles to deliver realistic estimates of critical performance indicators, particularly the QBER, which reduces its usefulness for precise performance evaluations.

3) LARGE-SCALE QKDNetSim [16]

This simulator extends QKDNetSim with improved key-management and adaptive routing strategies. It effectively handles larger and more complex networks through advanced key synchronization mechanisms. Nevertheless, it does not model detailed quantum-layer effects. This limitation reduces the fidelity of the simulation and weakens its ability to produce practical performance predictions.

4) QKDNetSim+ [13]

An enhanced version of the NS-3-based simulator, QKDNetSim+ introduces improvements in key-management, including dual-buffer structures and indexed databases that facilitate efficient synchronization across nodes. Despite these enhancements, the simulator uses a highly simplified quantum-layer model and does not include quantum device representations. These limitations reduce its ability to deliver detailed performance insights in real-world scenarios.

5) QUANTUM SECURE COMMUNICATION NETWORK (QSCN) SIMULATION [17]

The QSCN simulation provides a realistic representation of quantum-layer effects based on the GLLP security model [21]. Despite these realistic features, it does not support multi-hop key relay functions and does not provide sufficient configurability for quantum hardware and protocol parameters. These limitations reduce its usefulness in multi-hop QKDN evaluations.

6) DISSIPATIVE DYNAMICS IN QKD [18]

This simulation uses the Jaynes–Cummings model [22] to accurately depict realistic quantum-layer effects. It provides detailed insights into how these factors affect the QBER with respect to transmission distance. This capability is useful for analyzing realistic operational constraints. However, it lacks support for complex network-level functions such as multi-hop key relay and adaptive routing. As a result, it is less effective in scenarios that require large-scale network evaluations.

B. COMPARATIVE ANALYSIS WITH QKDN SIMULATORS

To clearly illustrate differences among existing QKDN simulators and to emphasize the advantages of the proposed QKDSim-HT, Table 1 presents a comprehensive technical

TABLE 2. Computational performance comparison of existing QKDN simulators and the proposed QKDSim-HT.

Simulator	Topology (number of nodes)	Simulation runtime	Memory usage	CPU/GPU utilization	Time complexity
Parallel discrete-event simulation [15]	Ring (128)	18.5 s	336 KB	Multicore CPU	$O(1)$ (ladder queue)
QKDNetSim [11]	Chain (2)	NR	NR	CPU (NS-3)	$O(\log n_{\text{evt}}^{\text{NS3}})$
Large-scale QKDNetSim [16]	Padua QKD network [33] (6)	NR	NR	CPU (NS-3)	$O(\log n_{\text{evt}}^{\text{NS3}})$
QKDNetSim+ [13]	Chain (2)	NR	NR	CPU (NS-3)	$O(\log n_{\text{evt}}^{\text{NS3}})$
QSCN simulation [17]	QSCN (6)	NR	NR	CPU	NR
Dissipative dynamics in QKD [18]	Chain (2)	NR	NR	CPU/GPU	NR
QKDSim-HT (proposed)	Chain (2), Ring (5), Butterfly (6), Grid (9), NSFNET (14)	23.0 s, 87.4 s, 108.7 s, 176.4 s, 289.8 s	140.4 MB, 156.8 MB, 167.4 MB, 174.0 MB 192.3 MB	Multicore CPU	$O(\log n_{\text{evt}}^{\text{NSQ}})$ (event scheduling) $O(n_{\text{key}} \log n_{\text{key}})$ (BB84 post-processing) $O(E \log N)$ (routing)

comparison. The comparison criteria include quantum-layer modeling, quantum source & detector modeling, key-management, multi-hop key relay, and adaptive routing support. Each criterion and its respective categories are clearly defined below.

The quantum-layer modeling criterion evaluates how accurately simulators represent quantum channel effects. ''Simplified abstraction'' indicates a basic representation of channel characteristics without capturing detailed quantum-layer effects. In contrast, ''Detailed'' represents realistic modeling of quantum-layer effects.

Quantum source & detector modeling indicates the detail level in modeling quantum source and detector devices. ''Minimal'' is used to denote fundamental representations of quantum sources and detectors with limited device-specific characteristics. In contrast, ''Realistic'' represents a comprehensive modeling of quantum-layer effects.

Key-management measures the level of sophistication of the mechanisms that manage, synchronize, and distribute keys throughout the network. ''Basic'' represents elementary synchronization and minimal key distribution capabilities. ''Advanced'' represents sophisticated mechanisms that involve dual-buffer structures, indexing databases, and network-wide synchronization features for effective key-management.

Multi-hop key relay distinguishes whether simulators support secure key distribution through multiple intermediate relay nodes. ''No'' indicates that multi-hop relay is not supported, while ''Yes'' indicates robust capabilities that enable secure and reliable multi-hop key relay operations.

Adaptive routing support assesses whether simulators dynamically adapt routing paths based on changes in network conditions and key availability. ''No'' indicates that the simulator supports only static routing. ''Yes'' indicates that the simulator includes dynamic routing mechanisms, adapting paths according to real-time network conditions.

As illustrated in Table 1, a comparative analysis reveals notable distinctions among the aforementioned simulators. Most existing simulators are inclined either toward simplified quantum-layer models for scalability or toward detailed quantum-layer modeling, but lack sufficient support for network-level functionalities. The proposed QKDSim-HT addresses these critical limitations by combining detailed quantum-layer modeling based on NetSquid, realistic quantum source and detector modeling, advanced key-management mechanisms, robust multi-hop key relay, and adaptive routing strategies. These integrated capabilities render QKDSim-HT uniquely suited to realistic QKDN evaluations, providing greater predictive accuracy and practical applicability for quantum secured network design and optimization.

Table 2 reports simulation runtime, memory usage, CPU/GPU utilization, and time complexity for representative QKDN simulators. The notation NR (not reported) indicates that the original publication did not provide the corresponding metric. For QKDSim-HT, results are presented across five topologies (Chain, Ring, Butterfly, Grid, NSFNET [34]), as illustrated in Fig. 3.

Most prior works focus on point-to-point evaluations over small Chain topologies and do not include scaling experiments on larger or more diverse network topologies. Direct benchmarking under identical scenarios is therefore infeasible, because many simulators lack either advanced networking functions or accurate quantum-layer modeling. The parallel discrete-event simulator reports shorter runtimes on larger topologies, but its omission of these two capabilities reduces reliability and applicability. In contrast, QKDSim-HT provides both capabilities and thus represents a more suitable framework for scenarios requiring detailed physical modeling and network-level operations.

The time complexity reflects the costs of the underlying kernels. The parallel discrete-event simulator adopts a ladder-queue scheduler with $O(1)$ operations. QKDNetSim, Large-scale QKDNetSim, and QKDNetSim+ are all built upon the QKDNetSim and implemented on top of the NS-3 simulation kernel. As a result, these simulators inherit NS-3's discrete-event scheduling mechanism with a time complexity of $O(\log n_{\text{evt}}^{\text{NS3}})$, where $n_{\text{evt}}^{\text{NS3}}$ denotes the number of pending events. On the other hand, QKDSim-HT follows NetSquid's discrete-event scheduler. Quantum transmission events, such as qubit propagation and detection, are processed with a time complexity of $O(\log n_{\text{evt}}^{\text{NSQ}})$, where $n_{\text{evt}}^{\text{NSQ}}$ denotes the number of pending events managed by the NetSquid kernel. Since the definition and scale of event queues differ across simulation

kernels, these complexity expressions should be interpreted as kernel-specific scheduling costs rather than as absolute cross-simulator comparisons. After the transmission phase, BB84 post-processing is executed. Basis sifting requires $O(n_{\text{key}})$, and Cascade [30] error-correction dominates with $O(n_{\text{key}} \log n_{\text{key}})$ complexity, where n_{key} denotes the sifted key length. For end-to-end key delivery across the network, the simulator applies a shortest path routing algorithm with $O(E \log N)$ complexity [36], where N denotes the number of nodes and E denotes the number of links in the topology. In sparse networks, this complexity reduces to $O(N \log N)$.

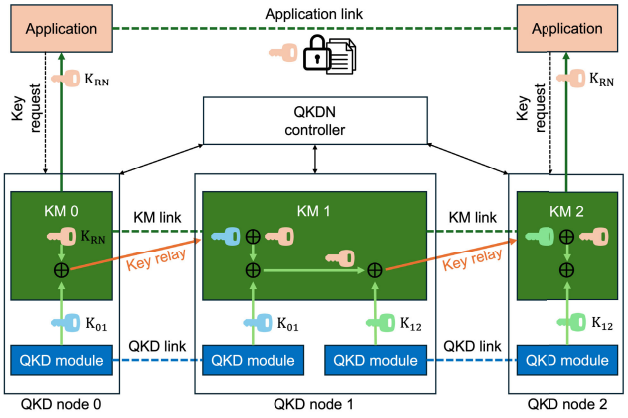

FIGURE 1. Conceptual architecture of a QKDN as modeled by QKDSim-HT, depicting QKD modules, key-management, classical control flows, and key relay, in accordance with ITU-T recommendations.

III. SIMULATION STRUCTURE OF QKDN IN QKDSim-HT

QKDSim-HT adopts a conceptual structure based on ITU-T recommendations Y.3800 [23] and Y.3803 [25], highlighting a realistic QKDN setup that the simulator aims to represent. Figure 1 provides an abstract overview of key distribution mechanisms and relay operations within a QKDN framework, as described in these recommendations. The figure reflects the intended operational principles of QKDSim-HT. The specific implementation within QKDSim-HT builds on the NetSquid framework, incorporating detailed quantum-layer modeling and essential network functionalities such as multi-hop key relay, adaptive routing, and key-management. In addition, the QKDN controller periodically monitors the network state, and adaptive rerouting is triggered upon node or link failures to ensure resilient key delivery. While Fig. 1 focuses on functional entities and control flows, Fig. 2 summarizes the internal simulation stack that realizes these functions in QKDSim-HT.

As illustrated in Fig. 2, the implementation of QKDSim-HT is organized into three layers on top of the NetSquid primitives. The bottom QKD layer aggregates the physical and protocol models that constitute a realistic QKD stack, including the error-correction module and detector-inefficiency and depolarization models described in Sections III and IV. These components directly expose device- and channel-dependent hyperparameters such as detection efficiency, dark count rate, fiber attenuation, and depolarization rate. The KM layer implements key-management functionality, including the trusted-relay module, key-pool manager, and key-consumption tracker that realize the ITU-T Y.3803 key-management procedures [25] on top of link-level QKD keys. The service layer hosts network modules for key provisioning, traffic generation, and topology scaling, which generate end-to-end key requests and shape multi-user service workloads. In this work, the term provisioning refers to the process of serving end-to-end key requests using the available link-level keys maintained in the key-pools.

The vertical parameter tuning block in Fig. 2 represents the hyperparameter tuning interface of QKDSim-HT. By varying physical-layer and traffic parameters through this interface, the simulator produces quantitative performance metrics such as key rate, QBER, delay, and throughput, which are collected in the performance-analysis module at the top of the stack. This layered structure explicitly connects the configurable hyperparameters to the network-level metrics reported in Section V, and thus supports reproducible and realistic performance analysis of QKDNs.

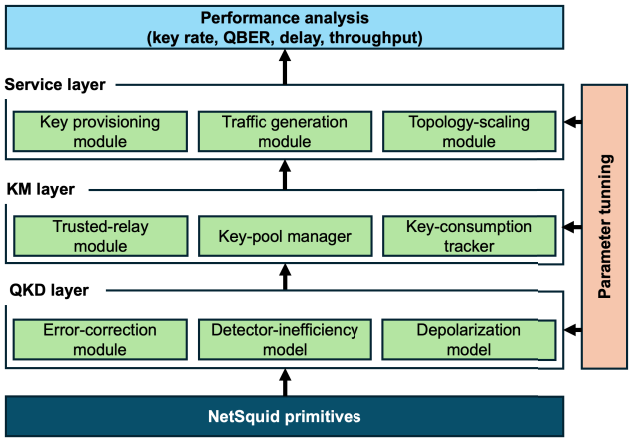

FIGURE 2. Layered simulation structure of QKDSim-HT. NetSquid primitives provide quantum optical components and event scheduling, on top of which a realistic QKD layer, a key-management (KM) layer, and a service layer for network modules are composed. Physical and traffic parameters are configured through the parameter-tuning interface, and the performance-analysis module collects quantitative metrics such as key rate, QBER, delay, and throughput.

A. QUANTUM STATE PREPARATION AND PHOTON SOURCES

QKDSim-HT uses NetSquid's quantum processor, gate, and photon-source modules [7] to implement polarization-based DV-QKD. Pauli-X and Hadamard operations define and rotate the rectilinear ($|H\rangle, |V\rangle$) and diagonal ($|+45°\rangle$, $|-45°\rangle$) bases. Qubits represent single-photon polarization and provide faithful models of state preparation, transmission, and measurement.

The photon sources emit single photons according to configurable probability distributions and source rates, which

reflect realistic emission statistics and device-level imperfections. The event-driven scheduler coordinates gate durations, source timing, and operation order to match propagation delays and detector timing across the network. Imperfections in state preparation and subsequent gate operations are modeled through the modular components of the NetSquid quantum layer (e.g., depolarization, dephasing, and gate duration constraints). This design establishes the foundation for the state-preparation of subsequent channels and detection models.

B. QUANTUM DETECTION MODELS

The photon detectors in QKDSim-HT consider three critical physical parameters: detection efficiency, dark count rate, and detector dead time. Detection efficiency represents the probability that an arriving photon is successfully detected and influences the achievable secure key rates [27]. The dark count rate quantifies false detection events resulting from intrinsic noise in photon detectors [28]. When the photon arrival rate is low, dark counts contribute more significantly to the total detections, increasing the QBER [29].

The detector dead time refers to the required recovery interval following a photon detection event. This interval is fundamental to reset the detector to a stable state and to prevent afterpulsing and false detections. Consequently, dead time imposes limitations on the maximum attainable detection throughput, thereby affecting the overall performance of the QKD system.

C. QUANTUM CHANNEL MODELS

QKDSim-HT applies three physical models provided by NetSquid to accurately represent photon propagation and imperfections within optical fiber channels used in QKDNs.

Photon propagation delay t_{delay} is defined as:

$$t_{\text{delay}} = \frac{L}{c_{\text{fiber}}} \times 10^9 \text{ [ns]}, \tag{1}$$

where L is the fiber link length (km) and c_{fiber} is the photon propagation speed in the fiber (approximately 2×10^5 km/s). This delay ensures realistic timing synchronization in simulations.

Photon loss within optical fibers is represented by an exponential loss model:

$$P_{\text{loss}} = 1 - (1 - P_{\text{init}}) \times 10^{-\frac{\alpha_{\text{loss}} L}{10}}, \tag{2}$$

where P_{init} denotes the initial insertion loss, and α_{loss} represents the fiber attenuation coefficient (dB/km). This parameter directly affects achievable communication distances and secure key rates.

Depolarization noise, which describes random polarization changes due to channel imperfections, is expressed as:

$$P_{\text{depolar}} = 1 - \exp\left(-\lambda_{\text{depolar}}\, t_{\text{delay}}\right), \tag{3}$$

where λ_{depolar} denotes the depolarization rate (Hz), and t_{delay} is the photon propagation delay expressed in seconds, obtained by converting the delay defined in Eq. (1). Depolarization critically affects QBER and consequently influences the overall performance of QKD systems.

D. CLASSICAL COMMUNICATION CHANNELS

Classical channels in QKDSim-HT handle essential tasks such as basis reconciliation, error-correction and synchronization. Classical channels connect the QKD nodes for exchanging control messages that support QKD operations. These channels are modeled with configurable latency and realistic propagation delays, ensuring accurate timing and synchronization of control signals across the QKDN. In particular, classical messages exchanged include basis matching information, key reconciliation data and error-correction information. These interactions are essential to establish and manage the quantum keys throughout the network.

E. KEY RELAY AND MANAGEMENT

Key relay and management in QKDSim-HT follow ITU-T Y.3803 recommendation. This allows secure key distribution between two distant nodes through intermediate relay nodes. Consider two distinct QKD nodes i and j (i, j $\in \{0, 1, \ldots, N-1\}$, i $\neq$ j), where N is the total number of nodes in a network topology.

At the source node, a random key K_{RN}, where RN denotes a random number, is locally generated. This key is XOR-encrypted using a local QKD-generated key K_{ij}, and the resulting ciphertext is transmitted to the next relay node. Each intermediate node decrypts the incoming ciphertext using the shared QKD key with the previous node, and then re-encrypts the recovered key data with a new QKD key shared with the next node. This relay process continues until the final destination node, where the initially generated K_{RN} is decrypted using the QKD key shared between the destination node and the preceding relay node.

The relay operation between adjacent nodes i and j is computed as:

$$\text{K}_{\text{relay}} = \text{K}_{\text{ij}} \oplus \text{K}_{\text{RN}}, \tag{4}$$

where K_{ij} denotes the QKD-generated key shared between nodes i and j. This design ensures that no relay node simultaneously possesses both the encrypted relay key and the corresponding QKD key, which improves the security of the relay process.

F. HYPERPARAMETER TUNING AND SIMULATION WORKFLOW

QKDSim-HT supports hyperparameter tuning to closely simulate experimental conditions and operational scenarios. Configurable parameters include detector efficiency, dark count rate, fiber attenuation (α_{loss}), depolarization rate (λ_{depolar}) and photon emission rate. These parameters can be configured to reflect realistic device performance and channel conditions, which enables accurate simulation of QKD system behavior under practical operating scenarios.

The simulation workflow in QKDSim-HT consists of sequential steps that include quantum state preparation, photon transmission, quantum channel propagation losses, depolarization effects and timing delays. Subsequent steps cover photon detection events that account for detector efficiency, dark counts and dead times. Then, Cascade [30] based basis reconciliation and error-correction are performed to derive identical sifted keys between communicating parties. Subsequently, multi-hop relay operations are performed in the order of requests generated by the applications. NetSquid's event-driven scheduler ensures accurate timing and synchronization throughout these steps. This stepwise simulation flow, combined with NetSquid's event-driven execution, enables QKDSim-HT to reproduce system-level behavior accurately and support detailed evaluation of QKDN performance across various scenarios.

IV. SIMULATION METHODOLOGY

This section describes the simulation methodology used in QKDSim-HT and explains the sequence of procedures used to model detailed QKD processes.

A. QUANTUM STATE PREPARATION AND TRANSMISSION

Photons are represented as qubits in the simulation, and are encoded into quantum states according to the QKD protocol. Quantum gates such as Pauli-X and Hadamard are applied to these qubits to prepare polarization states essential for QKD operations. The encoded qubits then propagate through simulated quantum channels that incorporate realistic physical effects, including fiber loss, depolarization, and detector imperfections.

The simulation utilizes the concept of batches and runs for robust statistical analysis. A batch consists of multiple photon transmissions intended to generate sufficient data for reliable error-correction. Using multiple batches simultaneously reduces statistical fluctuations during error-correction, enhancing overall accuracy. A run comprises multiple batches, providing a sufficiently large key sample for meaningful statistical evaluation. This approach ensures accurate estimation of critical performance metrics such as the QBER and secure key rate.

B. MEASUREMENT AND BASIS RECONCILIATION

At the receiver, incoming photons are measured using randomly selected polarization bases. After photon transmission, the sender and receiver publicly announce their selected bases via a classical channel. Only the measurement results corresponding to matching bases are retained to form the sifted key, while the rest are discarded. To estimate the quantum bit error rate (QBER), a randomly chosen subset of the sifted key is publicly compared. The QBER is defined as:

$$\text{QBER} = \frac{\text{Number of mismatched bits}}{\text{Number of total compared bits}}. \tag{5}$$

The QBER reflects the noise level and potential disturbances in the quantum channel. It is used to assess link reliability and to identify issues such as eavesdropping attempts, channel misalignment, or device instability that may compromise secure key generation.

C. CASCADE ERROR-CORRECTION

Based on the calculated QBER, the Cascade protocol corrects errors in the sifted key through iterative parity checks and binary search within blocks. Each message exchange involved in the Cascade protocol is explicitly modeled in the simulation. The time delays associated with these classical communications are taken into account as they can influence the overall latency of secure key generation.

D. SECURE KEY GENERATION AND RATE CALCULATION

In this study, a secure key refers to the portion of the sifted key that remains after successful error-correction, where both parties have verified bitwise agreement. Its length reflects the combined effects of quantum channel imperfections and the efficiency of the error-correction process.

After completing photon transmissions for a defined batch size, the Cascade error-correction protocol is executed. Quantum transmission occurs over the quantum channel and error-correction is performed through classical computation on local devices. The repeated execution of the protocol enables the two processes in a pipelined manner [15] and overlap in time at the system level. Therefore, either the quantum transmission duration or the error-correction duration becomes the dominant factor. The secure key generation rate is then calculated based on the longer duration between these two processes:

$$\text{Key rate} = \frac{\text{Secure key length}}{\max(T_{\text{tran}}, T_{\text{ec}})}, \tag{6}$$

where T_{tran} represents the quantum transmission time and T_{ec} denotes the error-correction time. This formula reflects realistic throughput limitations in practical QKDNs.

E. KEY RELAY OPERATION

Secure keys are distributed via a trusted-relay method. Intermediate nodes relay keys between two distant nodes using XOR operations. Consider adjacent QKD nodes i and j. The relay key is computed as defined in Eq. (4).

The XOR-based relay mechanism transmits the encrypted relay key across intermediate nodes, while ensuring that no relay node simultaneously holds both the encrypted relay key and the corresponding QKD key. To support secure and efficient key delivery, the QKDN controller dynamically selects routing paths based on the real-time availability of QKD keys.

F. PERFORMANCE METRICS AND EVALUATION

QKDSim-HT provides several performance metrics for evaluating QKDNs. The key performance metrics include the QBER, secure key rate, resource utilization, and blocking statistics for end-to-end key requests. QBER directly indicates quantum state integrity. The secure key rate measures

the efficiency of key generation. Resource utilization and blocking statistics reflect how effectively quantum resources are allocated across the network and how reliably end-to-end key requests are fulfilled. These performance metrics offer essential insights for practical QKDN deployment and optimization.

G. HYPERPARAMETERS

Simulations use realistic hyperparameters summarized in Table 3. Parameters such as depolarization rate, dark count rate, and detector efficiency are based on standard experimental conditions to reflect practical QKD system. Detector settings were selected based on the manufacturer-provided specifications of the ID 230 single-photon detector [31] to reflect experimentally feasible conditions. QKD node manages key-pools, which are 256 kbit (1,024 entries of AES 256 key) in size. The DV-QKD quantum channel operates at 1550 nm.

In practical QKDN deployments, the dominant component of end-to-end latency is the hop-by-hop trusted-relay processing delay. According to ITU-T Y.3801 [24] and ETSI GS QKD-004 [26], key delivery latency increases linearly with the hop count N_h because each trusted node performs verification and forwarding before the key progresses to the next hop. The experimental study in [37] reports a per-hop trusted-relay node (TRN) processing delay of approximately 20 ms. Based on this observation, we adopt a per-hop TRN delay of 20 ms in our simulation model. Consequently, the end-to-end relay delay is modeled as $20 \times N_h$ ms, which captures the dominant contribution to QKDN delay.

TABLE 3. Common hyperparameters used in all simulations.

Hyperparameter	Value
QKD protocol	BB84
Number of runs	32
Key size (bits)	256
Session batch size	256
Detection efficiency	25 %
Detector dead time	2000 ns
Dark count rate (counts per second)	50 cps
Base link length	50 km
fiber loss coefficient	0.2 dB/km
Depolarization rate	50 Hz
Dephasing rate	50 Hz
Quantum gate duration	10 ns
Source frequency	1 GHz
Application type	multi-all
Reconciliation	Cascade error-correction
QKD key size for relay	256 bits
TRN processing delay	20 ms

V. SIMULATION RESULTS

We evaluate the performance of QKDSim-HT across five network topologies: Chain, Ring, Butterfly, Grid, and NSFNET [34] as shown in Fig. 3. NSFNET serves as a practical testbed topology and provides a realistic baseline for cross-topology comparisons. NSFNET assumes that

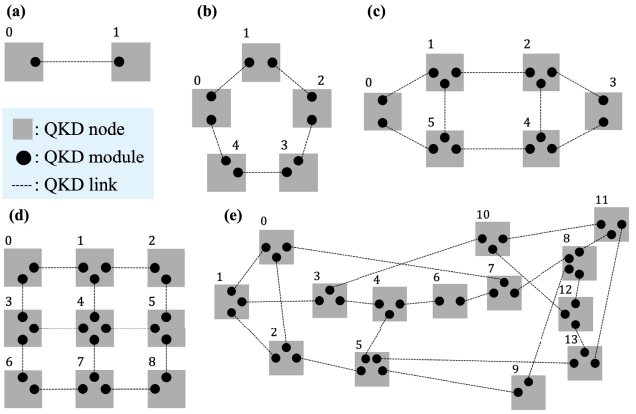

FIGURE 3. Five network topologies analyzed: (a) Chain, (b) Ring, (c) Butterfly, (d) Grid, and (e) NSFNET [34]. Each node represents a QKD node containing one or more QKD modules; dashed lines represent quantum links.

intermediate relay nodes are included so that the distance between adjacent relays does not exceed the base link length. Each link in these topologies has an identical length to ensure a controlled environment. This setup isolates how physical parameters such as depolarization rate, link length, and fiber attenuation affect QKDN performance.

A. ANALYSIS OF PHYSICAL PARAMETERS ON QKD PERFORMANCE

We analyzed the butterfly topology to assess how depolarization rate, link length, and fiber attenuation affect QKD performance, as illustrated in Fig. 4. To evaluate the impact of these error-related parameters, we performed a grid search over the hyperparameters, and the representative results are summarized. Throughout this paper, error bars represent 95% confidence intervals computed using a Student's t-distribution from ten repeated simulations with different random seeds. As the depolarization rate increases, the QBER rises accordingly, while the BB84 protocol continues to produce stable key generation rates at moderate depolarization levels. These trends confirm the protocol's robustness under realistic optical-channel conditions.

The link length analysis reveals a exponential decrease in the secure key rate with longer distances. This decline aligns with known photon losses in optical fiber channels. Additionally, QBER increases at longer link lengths due to reduced photon arrival rates. Lower photon arrival rates increase the relative effect of detector dark counts, leading to higher bit error rates. Key rates become impractical to use over relatively long link distances. This distance thus indicates the practical limit of direct fiber-based QKDNs under current physical constraints and detector technologies.

Although the fiber loss model in Eq. (2) defines photon attenuation as an exponential function of link length and loss coefficient, the observed reduction in key rate does not strictly follow this trend. This discrepancy results from detector dead time, which limits the effective detection rate

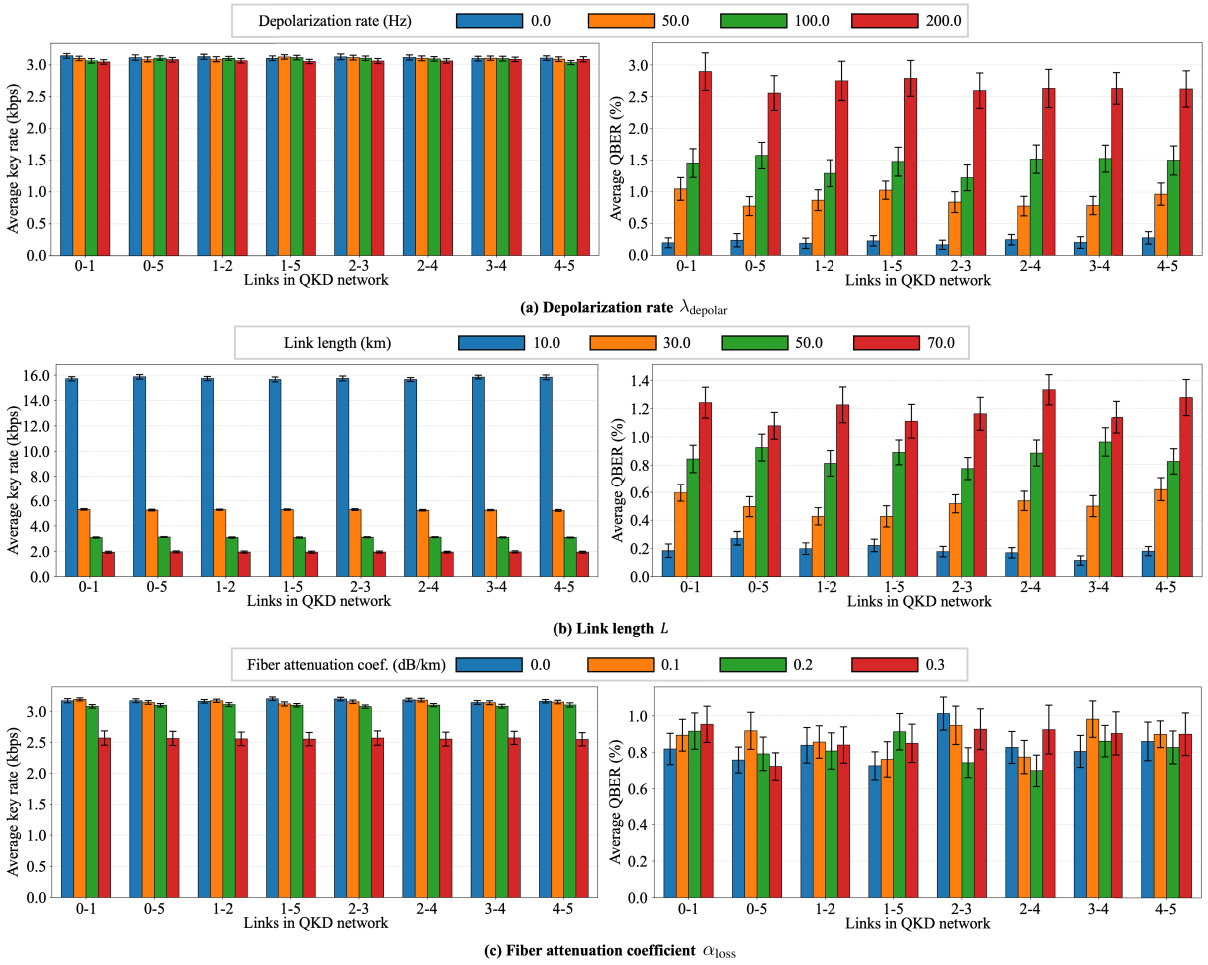

FIGURE 4. QKD performance in a butterfly topology under varying physical-layer parameters: (a) depolarization rate λ_{depolar}, (b) link length L, and (c) fiber attenuation coefficient α_{loss}. For each subfigure, the left panel shows the average key rate and the right panel shows the average QBER across network links.

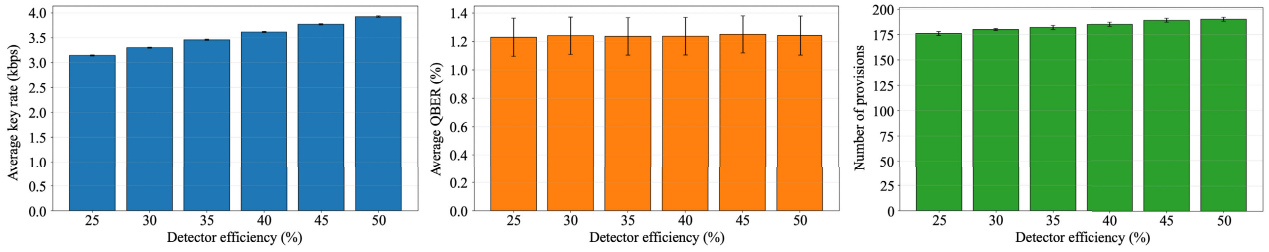

FIGURE 5. Impact of detector efficiency on BB84 performance in QKDSim-HT on the NSFNET topology. From left to right: average key rate, average QBER, and number of provisions as a function of detector efficiency.

and conceals how photon loss degrades the key generation performance under high-attenuation conditions. While the QBER remains largely unaffected across varying attenuation levels, the reduction in detected photon counts directly lowers the achievable key rate. These results highlight the importance of accurately modeling fiber attenuation when evaluating the feasibility and performance limits of QKD systems.

Figure 5 presents the impact of detector efficiency while all other hyperparameters in Table 3 remain fixed. The experiments use the NSFNET topology, and each simulation generates end-to-end key requests according to a Poisson traffic model with an average of 200 requests per simulation. When the efficiency increases from 25% to 50%, the average key rate increases in a near-linear manner. The number of provisions also increases because a larger portion

TABLE 4. Performance metrics comparison across different network topologies under varying depolarization rates, link lengths, and fiber loss coefficients.

Topology	Metrics	Depolarization rate (Hz)				Link length (km)				Attenuation coef. (dB/km)			
		0.0	50.0	100.0	200.0	10.0	30.0	50.0	70.0	0.0	0.1	0.2	0.3
Chain	Key rate (kbps)	3.1	3.0	3.1	3.0	15.8	5.2	3.1	1.6	3.2	3.2	3.0	2.0
	T_{tran} (ms)	64.0	65.1	64.0	64.2	12.9	39.0	64.7	91.1	64.9	64.5	64.2	64.4
	T_{ec} (ms)	2.2	5.6	7.3	14.3	0.5	2.5	6.1	5.9	5.2	5.9	6.3	4.5
	QBER (%)	0.1	0.7	1.2	2.8	0.1	0.5	0.8	1.4	0.7	0.7	0.8	1.1
Ring	Key rate (kbps)	3.1	3.0	3.1	3.1	15.8	5.2	3.0	1.6	3.1	3.2	3.1	2.0
	T_{tran} (ms)	64.3	64.7	64.3	64.6	13.0	38.9	64.8	90.4	64.9	64.5	64.3	64.8
	T_{ec} (ms)	3.8	8.9	12.5	19.5	0.7	3.9	9.4	11.7	9.4	8.6	9.1	5.7
	QBER (%)	0.2	0.7	1.4	2.6	0.1	0.5	0.8	1.1	0.8	0.7	0.8	0.8
Butterfly	Key rate (kbps)	3.0	3.0	3.0	3.0	15.8	5.3	3.0	1.6	3.2	3.2	3.0	2.0
	T_{tran} (ms)	64.6	64.7	64.5	64.6	13.0	38.8	64.6	90.4	64.7	64.6	64.5	64.7
	T_{ec} (ms)	4.0	9.6	13.4	19.7	0.8	4.3	9.1	12.4	9.6	10.1	9.5	6.4
	QBER (%)	0.1	0.8	1.3	2.6	0.1	0.5	0.8	1.1	0.7	0.8	0.7	0.7
Grid	Key rate (kbps)	3.1	3.0	3.0	3.0	15.7	5.3	3.0	1.6	3.2	3.2	3.1	2.0
	T_{tran} (ms)	64.7	64.8	64.7	64.4	13.0	38.8	64.7	90.2	64.0	64.7	64.5	64.6
	T_{ec} (ms)	4.5	10.6	14.0	20.4	0.9	4.7	10.3	13.8	10.7	10.3	9.9	7.3
	QBER (%)	0.1	0.8	1.4	2.6	0.1	0.5	0.8	1.1	0.7	0.8	0.7	0.9
NSFNET	Key rate (kbps)	3.1	3.1	3.0	3.0	15.8	5.3	3.0	1.6	3.2	3.2	3.0	2.0
	T_{tran} (ms)	64.6	64.7	64.8	64.7	13.0	38.8	64.7	90.2	64.5	64.7	64.6	64.6
	T_{ec} (ms)	4.6	10.3	14.1	20.5	0.9	4.9	10.5	14.1	10.5	10.3	10.1	7.8
	QBER (%)	0.1	0.8	1.4	2.6	0.1	0.5	0.8	1.1	0.7	0.8	0.8	0.8

of transmitted photons is detected and contributes to the accumulation of secure keys in the key-pools. The average QBER stays close to 1.2% across all settings, which indicates that the dominant error sources in this regime originate from the quantum channel and are not affected by detector efficiency. These results confirm that higher detector efficiency improves key throughput and service capacity. They also show that QKDSim-HT can evaluate device-dependent trade-offs between detector specifications and practical QKDN performance.

B. COMPARATIVE NETWORK TOPOLOGY ANALYSIS

We evaluated how network topology affects QKD performance by simulating five representative configurations: Chain, Ring, Butterfly, Grid, and NSFNET. The results summarized in Table 4 demonstrate how topology influences key rate, transmission time T_{tran}, error-correction time T_{ec} and QBER. The simulation results indicate that key performance indicators, such as the secure key rate and QBER, exhibit consistent trends across different topologies when the parameters of the quantum layer remain fixed.

For example, when the depolarization rate increases from 0 to 200 Hz, all topologies show a similar increase in QBER from approximately 0.1% to 2.8%. Although higher QBER values extend the duration of error-correction T_{ec}, this increase remains small compared with T_{tran}. Under the pipelined process model [15], where quantum transmission and error-correction proceed concurrently, this difference does not substantially affect the final key rate.

Link length L increments from 10 to 70 km reduce the key rate and increase the measured QBER across all network topology types. According to the fiber loss model in Eq. (2), longer links increase photon attenuation, which lowers detection counts and leads to a reduction in the key rate. In the depolarization model of Eq. (3), where L is proportional to t_{delay}, longer links result in greater depolarization and consequently higher QBER. For the attenuation coefficient α_{loss}, the same loss model applies, but α_{loss} is not a parameter in Eq. (3), and QBER shows no significant variation over the range from 0.0 to 0.3 dB/km. When $\alpha_{\text{loss}} \leq 0.2$ dB/km, the detector dead time limits detection throughput at a fixed link length, which prevents substantial variation in the key rate. At $\alpha_{\text{loss}} = 0.3$ dB/km, the photon loss surpasses this limit and the key rate decreases.

These patterns suggest that the primary factors affecting link-level QKD performance are physical in nature, including photon loss, depolarization, and detector imperfections. When physical conditions are kept constant, variations in the per-link key rate or QBER are not attributable to the network topology. This observation is consistent with the characteristics of DV-QKD protocols, where channel-level loss and noise dominate performance outcomes. Furthermore, these experimental results on topological scalability, together with Table 2, demonstrate that simulation runtime and memory usage remain within acceptable limits even as the network scale increases.

By comparing the field-test results reported in [35], we validate the physical-layer modeling of our simulator. The key-rate trends produced by QKDSim-HT also agree with commercially deployed BB84 systems, such as ThinkQuantum's QUKY platform [38], consistent with the attenuation-dependent results reported in Table 4, which further supports the accuracy of our quantum-layer models. Moreover,

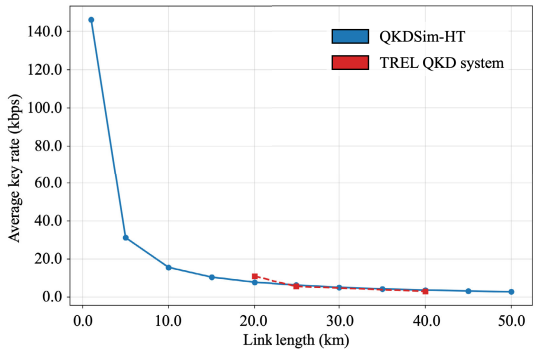

FIGURE 6. Comparison of QKDSim-HT with the TREL decoy-state BB84 field-test results.

we reproduced the decoy-state BB84 field-test configuration of the Toshiba Research Europe Ltd. (TREL) system [2], and the key-rate trend shown in Fig. 6 closely matches the measured performance. For the reported link losses at 20, 25, and 40 km, the TREL system achieved key rates of 11, 5.7, and 3.1 kbps, respectively, whereas our reproduced results deviated by 3.1 kbps at 20 km and remained within 0.5 kbps at 25 and 40 km. These consistent results across experimental and commercial systems demonstrate that the physical-layer models in QKDSim-HT reliably capture practical channel behavior.

C. KEY DISTRIBUTION AND RELAY ANALYSIS

This subsection analyzes how different QKD topologies affect network performance and shows that QKDSim-HT provides practical insights for the design and optimization of QKDNs from a networking perspective. The design task considers a 6-node network with 7 bidirectional links and has the objective of maximizing the number of successfully served end-to-end key relay requests. Each solution has the same number of nodes and links and therefore incurs the same implementation cost, but the link arrangement is different and this results in different patterns of key usage. In the simulation, each round processes all possible directional source-destination pairs, resulting in $N(N-1) = 30$ requests for $N = 6$ nodes.

Figure 7 shows the normalized remaining key distribution over successive request rounds for two selected solutions to this task. In each round, R denotes the cumulative number of processed end-to-end requests, and "**Blocked**" denotes the cumulative number of requests that could not be served due to insufficient keys on the selected paths. Each matrix element represents the remaining key quantity on a given link, normalized to the maximum number of keys initially generated by the BB84 protocol under identical configuration.

The key relay paths in the simulations were determined using a weighted shortest path algorithm based on the following metric from DARPA's QKDN study [32]:

$$m = \begin{cases} 100 + \dfrac{1000}{q - t}, & q > t, \\ \infty, & q \le t, \end{cases} \tag{7}$$

where m represents the link cost metric used to compute the shortest path, q indicates the available key quantity on the link, and t is a predefined threshold set to 5, as recommended by DARPA's study. The metric increases sharply as the available key quantity approaches the threshold value, which effectively penalizes links close to key depletion. This ensures that selected paths consistently maintain sufficient quantum keys for secure relay operations.

In the solution 1, keys on the central link are quickly depleted because multiple shortest relay paths converge there, which causes traffic concentration. After the third round, the number of blocked requests increases sharply and reaches 36 by the fourth round. The lack of path redundancy concentrates traffic on critical links, which causes rapid key exhaustion and consequently blocks subsequent requests that depend on these links.

In contrast, the solution 2 distributes the relay traffic across multiple paths. The additional links, including horizontal and diagonal connections, create alternative routes that reduce the load on the central link. This structure mitigates key depletion and limits request blocking. Out of 120 total end-to-end requests, the solution 2 records only 2 blocked requests by the fourth round, whereas the solution 1 records 36 under the same traffic conditions.

These results emphasize the need to evaluate QKDN architectures through simulation before physical deployment. Even when two topologies have the same number of nodes and links, their structural differences can lead to substantial variations in performance under realistic traffic. In particular, topology-dependent key depletion patterns highlight the necessity of adaptive routing and dynamic key-management that respond to real-time quantum key availability and network conditions. QKDSim-HT provides detailed insights by integrating accurate quantum-layer models with network-level protocols such as key relay and management. This capability allows researchers and system designers to identify critical bottlenecks, assess key usage efficiency, and make informed architectural decisions without relying on real-world testing.

To assess the influence of key-management hyperparameters on relay performance, we evaluated how the QKD key size for relay affects the average relay delay and the number of provisions, as shown in Fig. 8. As in Fig. 5, these experiments were also conducted on the NSFNET topology. Each end-to-end request consumes a single 256-bit key. A larger QKD key size for relay allows one relay operation to supply several 256-bit keys stored in the key-pools. When the QKD key size for relay increases from 256 to 2048 bits, the average relay delay decreases because the number of relay operations per request falls and the trusted-relay nodes are

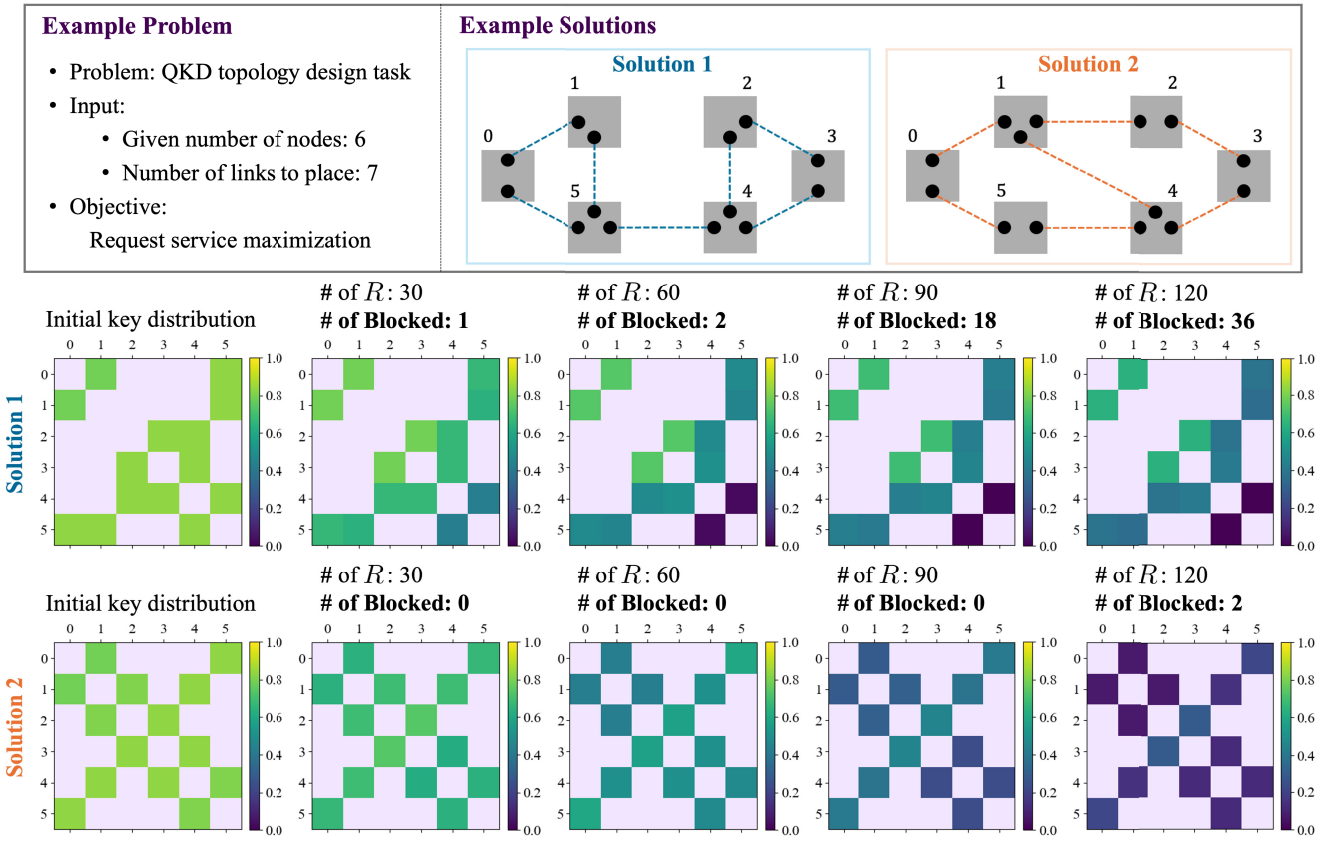

FIGURE 7. Example of a QKD topology design task, in which the objective is to maximize request service under a given number of nodes and links.

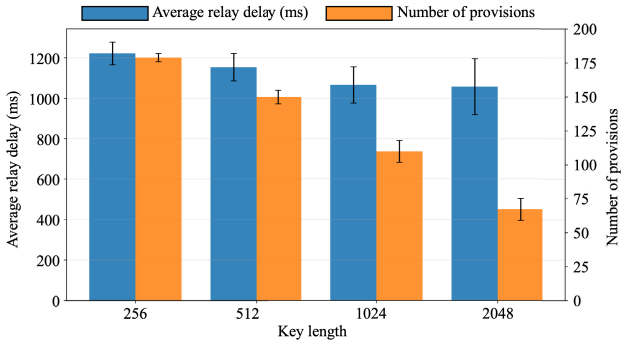

FIGURE 8. Average relay delay and number of provisions for different QKD key sizes for relay in QKDSim-HT on the NSFNET topology.

activated less often. The total number of provisions decreases, however, because partially used relay keys leave more unused 256-bit segments when the simulation ends or when routing paths change. This effect reduces the effective utilization of the generated keys. This trade-off shows that QKDSim-HT can tune the QKD key size for relay for the intended application and adjust the balance between lower relay delay, higher key utilization, and service capacity in realistic QKDN deployments.

VI. CONCLUSION

This paper introduced QKDSim-HT, a comprehensive NetSquid-based QKDN simulator designed polarization-based DV-QKD protocols. QKDSim-HT integrates rigorous quantum-layer models of quantum optical components, including realistic quantum-layer effects such as photon loss, polarization depolarization, dephasing errors, finite detector efficiency, dark counts, and detector dead times, with advanced network-level functionalities such as multi-hop key relay and adaptive routing.

A comparative study of existing QKD simulators highlighted the capabilities of QKDSim-HT, which integrates detailed quantum-layer effects with complete network-level operations. The simulation results across link-level and topology-level settings indicate that physical parameters such as depolarization, link length, attenuation, and detector efficiency exert a direct influence on QKDN performance. The evaluation of relay-key size further shows its role as a key-management parameter that determines both relay delay and the number of provisions, and it identifies a measurable trade-off between reduced relay activation frequency and lower key-utilization efficiency. The analysis of key availability demonstrates that limited path redundancy can induce biased key usage and depletion, while topologies with alternative routing paths significantly reduce blocking,

with reductions of approximately 94% in our experiments. Taken together, these findings show that QKDSim-HT provides a coherent and reliable simulation framework that quantifies the interaction between physical-layer properties, topology structure, and key-management parameters in practical QKDN operation.

Consequently, QKDSim-HT advances QKDN simulations, providing accurate and practical insights into quantum-layer imperfections and network topology affects. These contributions support the effective design, analysis, and optimization of robust and secure QKD communication infrastructures. In future work, we plan to extend QKDSim-HT with additional QKD protocols and error-correction schemes, and we also intend to apply it to larger-scale, heterogeneous topologies, including real-world testbed deployments. In addition, we plan to investigate algorithmic contributions, including routing and resource-management algorithms, using QKDSim-HT as the simulation platform. QKDSim-HT is available upon non-profit request, with plans to extend API access and provide GUI support in future releases.

REFERENCES

[1] C. Elliott and H. Yeh, "DARPA quantum network testbed," BBN Technol., Cambridge, MA, USA, Tech. Rep. AFRL-IF-RS-TR-2007-180, 2007.

[2] M. Peev et al., "The secoqc quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, Jul. 2009, Art. no. 075001.

[3] V. Martin et al., "MadQCI: A heterogeneous and scalable SDN-QKD network deployed in production facilities," *npj Quantum Inf.*, vol. 10, no. 1, p. 80, Sep. 2024.

[4] M. Pittaluga, Y. S. Lo, A. Brzosko, R. I. Woodward, D. Scalcon, M. S. Winnel, T. Roger, J. F. Dynes, K. A. Owen, S. Juárez, P. Rydlichowski, D. Vicinanza, G. Roberts, and A. J. Shields, "Long-distance coherent quantum communications in deployed telecom networks," *Nature*, vol. 640, no. 8060, pp. 911–917, Apr. 2025.

[5] C. Huang, Y. Chen, L. Jin, M. Geng, J. Wang, Z. Zhang, and K. Wei, "Experimental secure quantum key distribution in the presence of polarization-dependent loss," *Phys. Rev. A, Gen. Phys.*, vol. 105, no. 1, Jan. 2022, Art. no. 012421.

[6] D. E. Jones, D. L. P. Vitullo, T. Cook, L. M. Scott, A. Toth, and B. T. Kirby, "Simulation of quantum key distribution using entangled photon pairs over free-space channels," in *Proc. IEEE Photon. Conf. (IPC)*, Nov. 2022, pp. 1–2.

[7] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. de Oliveira Filho, M. Papendrecht, J. Rabbie, F. Rozpędek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. Torres-Knoop, D. Elkouss, and S. Wehner, "NetSquid, a network simulator for quantum information using discrete events," *Commun. Phys.*, vol. 4, no. 1, p. 164, Jul. 2021.

[8] M. H. Saeed, H. Sattar, M. H. Durad, and Z. Haider, "Implementation of QKD BB84 protocol in qiskit," in *Proc. 19th Int. Bhurban Conf. Appl. Sci. Technol. (IBCAST)*, Aug. 2022, pp. 689–695.

[9] A. Javadi-Abhari, M. Treinish, K. Krsulich, C. J. Wood, J. Lishman, J. Gacon, S. Martiel, P. D. Nation, L. S. Bishop, A. W. Cross, B. R. Johnson, and J. M. Gambetta, "Quantum computing with qiskit," 2024, *arXiv:2405.08810*.

[10] C. Lee, Y. Kim, K. Shim, and W. Lee, "Key-count differential-based proactive key relay algorithm for scalable quantum-secured networking," *J. Opt. Commun. Netw.*, vol. 15, no. 5, pp. 282–293, May 2023.

[11] S. P. Kumar, T. Jaya, and P. Rajalingam, "Implementation of quantum key distribution network simulation in quantum channel," *J. Phys., Conf. Ser.*, vol. 2335, no. 1, Sep. 2022, Art. no. 012056.

[12] T. R. Henderson and G. F. Riley, "Network simulations with the NS-3 simulator," *SIGCOMM Demonstration*, vol. 14, no. 14, p. 527, 2006.

[13] D. Soler, I. Cillero, C. Dafonte, M. Fernández-Veiga, A. F. Vilas, and F. J. Nóvoa, "QKDNetSim+: Improvement of the quantum network simulator for NS-3," *SoftwareX*, vol. 26, May 2024, Art. no. 101685.

[14] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[15] X. Wu, B. Zhang, G. Chen, and D. Jin, "A scalable quantum key distribution network testbed using parallel discrete-event simulation," *ACM Trans. Model. Comput. Simul.*, vol. 32, no. 2, pp. 1–22, Apr. 2022.

[16] E. Dervisevic, M. Voznak, and M. Mehic, "Large-scale quantum key distribution network simulator," *J. Opt. Commun. Netw.*, vol. 16, no. 4, pp. 449–462, 2024.

[17] Y. Wang, Q. Li, Q. Han, and Y. Wang, "Modeling and simulation of practical quantum secure communication network," *Quantum Inf. Process.*, vol. 18, no. 9, pp. 1–18, Sep. 2019.

[18] L. Salatino, L. Mariani, C. Attanasio, S. Pagano, and R. Citro, "Dissipative dynamics in quantum key distribution," *Eur. Phys. J. Plus*, vol. 138, no. 6, p. 517, Jun. 2023.

[19] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130502.

[20] X. Wu, A. Kolar, J. Chung, D. Jin, T. Zhong, R. Kettimuthu, and M. Suchara, "SeQUeNCe: A customizable discrete-event simulator of quantum networks," *Quantum Sci. Technol.*, vol. 6, no. 4, Oct. 2021, Art. no. 045027.

[21] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inf. Comput.*, vol. 4, no. 5, pp. 325–360, Sep. 2004.

[22] E. T. Jaynes and F. W. Cummings, "Comparison of quantum and semiclassical radiation theories with application to the beam maser," *Proc. IEEE*, vol. 51, no. 1, pp. 89–109, 1963.

[23] International Telecommunication Union (ITU-T). (2019). *ITU-T Recommendation Y.3800: Overview on Networks Supporting Quantum Key Distribution*. [Online]. Available: https://handle.itu.int/11.1002/1000/13990

[24] International Telecommunication Union (ITU-T). (2020). *ITU-T Recommendation Y.3801: Functional Requirements for Quantum Key Distribution Networks*. [Online]. Available:https://handle.itu.int/11.1002/1000/14258

[25] International Telecommunication Union (ITU-T). (2020). *ITU-T Recommendation Y.3803: Quantum Key Distribution Networks—Key Management*. [Online]. Available: https://handle.itu.int/11.1002/1000/14408

[26] ETSI Group Specification. (2020). *Quantum Key Distribution (QKD); Application Interface*. [Online]. Available: https://www.etsi.org/deliver/etsi/QKD/001099/004/02.01.0160/gs.pdf

[27] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, "Security proof of practical quantum key distribution with detection-efficiency mismatch," *Phys. Rev. Res.*, vol. 3, May 2021, Art. no. 013076.

[28] H. Shibata, T. Honjo, and K. Shimizu, "Quantum key distribution over a 72 dB channel loss using ultralow dark count superconducting single-photon detectors," *Opt. Lett.*, vol. 39, no. 17, pp. 5078–5081, 2014.

[29] Muskan, R. Meena, and S. Banerjee, "Analysing QBER and secure key rate under various losses for satellite based free space QKD," 2023, *arXiv:2308.01036*.

[30] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, 2007, pp. 410–423.

[31] ID Quantique. (2019). *ID230 Infrared Single-Photon Detector Datasheet*. [Online]. Available: https://www.idquantique.com/quantum-detection-systems/products/id230/

[32] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, C. Pacher, and M. Voznak, "Quantum key distribution: A networking perspective," *ACM Comput. Surv.*, vol. 53, no. 5, pp. 1–41, 2020.

[33] M. Avesani, G. Foletto, M. Padovan, L. Calderaro, C. Agnesi, E. Bazzani, F. Berra, T. Bertapelle, F. Picciariello, F. B. L. Santagiustina, D. Scalcon, A. Scriminich, A. Stanco, F. Vedovato, G. Vallone, and P. Villoresi, "A quantum key distribution network in the metropolitan area of padova," *Proc. SPIE*, vol. 12446, pp. 112–117, Jul. 2023.

[34] L. Gong, X. Zhou, X. Liu, W. Zhao, W. Lu, and Z. Zhu, "Efficient resource allocation for all-optical multicasting over spectrum-sliced elastic optical networks," *J. Opt. Commun. Netw.*, vol. 5, no. 8, pp. 836–847, Aug. 2013.

[35] P. Horoschenkoff et al., "DemoQuanDT: A carrier-grade QKD network," *J. Opt. Commun. Netw.*, vol. 17, no. 9, pp. 743–756, 2025.

[36] B. V. Cherkassky, A. V. Goldberg, and T. Radzik, "Shortest paths algorithms: Theory and experimental evaluation," *Math. Program.*, vol. 73, no. 2, pp. 129–174, May 1996.
[37] C. Stan, D. Verchere, J. J. V. Olmos, I. T. Monroy, and S. Rommel, "Dynamic-threshold-based pre-relaying for enhanced key allocation in quantum-secured networks," *J. Opt. Commun. Netw.*, vol. 17, no. 3, pp. 233–248, 2025.
[38] ThinkQuantum Srl. *QUKY: Quantum Key Distribution Platform—Detailed Brochure*. Accessed: Dec. 2025. [Online]. Available: https://www.thinkquantum.com/wp-content/uploads/files/Brochuredetailed.pdf

JU-BONG KIM received the B.S. and M.S. degrees in computer science engineering from Korea University of Technology and Education, South Korea, in 2017 and 2019, respectively, and the joint Ph.D. degree from the Department of Computer Engineering and the Department of Future Convergence Engineering, Korea University of Technology and Education, in 2023.

He is currently a Postdoctoral Researcher with the Quantum Network Research Center, Korea Institute of Science and Technology Information (KISTI), Daejeon, South Korea. His current research interests include quantum key distribution networks, reinforcement learning-based quantum key distribution optimization, multi-agent reinforcement learning, and exploration in reinforcement learning.

HYUN-KYO LIM (Member, IEEE) received the B.S. and M.S. degrees in computer science engineering from Korea University of Technology and Education, South Korea, in 2015 and 2017, respectively, and the Ph.D. degree from the Department of Interdisciplinary Program in Creative Engineering, Korea University of Technology and Education, in 2022.

He is currently a Postdoctoral Researcher with the Quantum Network Research Center, Korea Institute of Science and Technology Information (KISTI), Daejeon, South Korea. His research interests include reinforcement learning, network optimization, and quantum key distribution networks.

WONHYUK LEE received the B.S., M.S., and Ph.D. degrees from the School of Electrical, Electronic and Computer Engineering, Sungkyunkwan University, South Korea, in 2001, 2003, and 2010, respectively.

He is currently a Principal Researcher with the Quantum Network Research Center, Korea Institute of Science and Technology Information (KISTI), South Korea. His research interests include quantum network management, network performance enhancement, and QKDNs.

DAHYUN YUM received the B.S., M.S., and Ph.D. degrees in physics from Seoul National University, South Korea, in 2002, 2004, and 2012, respectively.

He is currently a Principal Scientist with ID Quantique. Previously, he was a Research Professor with Ewha Womans University and a Research Follow with the National University of Singapore and Tsinghua University, China. His research interests include quantum key distribution, quantum networks, quantum computing, and single-photon detectors.

CHANKYUN LEE (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical engineering from Korea Advanced Institute of Science and Technology (KAIST), South Korea, in 2009, 2011, and 2016, respectively.

He is currently a Principal Researcher with the Quantum Network Research Center, Korea Institute of Science and Technology Information (KISTI), South Korea. Prior to joining KISTI, he held a senior research position with the Next Generation Business Team, from 2016 to 2018, and Network Business Team, from 2018 to 2019, Samsung Electronics. His current research interests include quantum key distribution networks, networking algorithms, and optical networking.