EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Quantum Communication Technology for Optimizing 3D Cost Estimation and Secure Data Transmission in Substation Engineering

Junchao Li[1,*], Fei You[1] and Dan Chen[1]

[1]Economic and Technical Research Institute, State Grid Ningxia Electric Power Co., Ltd., Yinchuan 750000, China

Abstract

INTRODUCTION: The highly sensitive 3D cost estimation data in substation projects faces significant security challenges during distributed transmission, as conventional encryption approaches prove inadequate against quantum computing threats for large-scale engineering data protection. OBJECTIVES: This study aims to develop a quantum communication-based secure transmission framework for substation 3D cost estimation data, employing a three-tier quantum architecture to achieve information-theoretic security levels with robust defense against network attacks. METHODS: The proposed solution employs a three-tier quantum architecture encompassing physical, network, and application layers, with optimized quantum channels for engineering data flow. The framework utilizes the BB84 protocol with the decoy state method, implementing quantum key distribution and classical encryption integration to maintain data integrity through a distributed optimization strategy. RESULTS: Simulation validation across 10-50 node networks demonstrates quantum key generation rates of 8-40 kbps and 23% improvement in network throughput compared to star topology over traditional methods. The system achieves 99.99% reduction in key usage compared to pure quantum approaches while maintaining information-theoretic security levels. CONCLUSION: This research establishes fundamental principles and implementation pathways for quantum communication applications in engineering domains, offering significant advancement in secure data transmission for sensitive industrial applications and providing a reliable solution for protecting critical infrastructure engineering data.

Keywords: Quantum communication; Secure data transmission; Substation engineering; 3D cost estimation; Distributed systems

Received on 15 September 2025, accepted on 17 October 2025, published on 16 March 2026

doi: 10.4108/eetsis.12021

1. Introduction and Related Work

Coupled with the increasingly prominent role of digital transformation, the 3D cost estimation data for substation engineering is facing prominent security risks. The 3D cost estimation data is both a type of commercial secret, including devices and costs, and a type related to geography and scale, as a smart grid cybersecurity study contends that the threats to smart grids are increasingly complicated [1], as typical defenses will be inadequate against serious cyberattacks [2, 3].

In distributed collaborative environments, design institutes, construction units, supervision agencies, and other parties need to frequently share and update data, while traditional encryption schemes face fundamental threats in the post-quantum era. Research on cybersecurity protection for power grid control infrastructure emphasizes that critical infrastructure requires higher levels of security protection capabilities [4]. Simulation of cyberattack consequences in critical business scenarios of smart grids demonstrates [5] that data security incidents may produce chain reactions affecting power system operations with impacts far exceeding

*Corresponding author. Email: wfswxhll@163.com

expectations. More seriously, engineering archives need to remain confidential for 30-50 years, and the current "harvest-then-decrypt" attack model makes it difficult for traditional encryption schemes to provide long-term security guarantees. Traditional cryptographic schemes face fundamental limitations in protecting engineering data. Symmetric algorithms, while efficient, suffer from key distribution challenges in multi-party scenarios, while public key systems are vulnerable to quantum computing threats. Research indicates that combining classical, post-quantum, and quantum technologies is necessary [6], yet post-quantum approaches remain based on computational assumptions rather than providing information-theoretic security.

Quantum key distribution technology provides a fundamental solution to these challenges. Theoretical research on secure quantum key distribution shows [7] that quantum communication can provide information-theoretic security guarantees that do not depend on computational complexity assumptions. Comprehensive research on quantum key distribution protocols demonstrates [8] that modern QKD protocols can already provide reliable security guarantees in practical environments. A survey of quantum cryptography and quantum key distribution protocols indicates [9] that classical protocols such as BB84 achieve theoretically perfect security through four-state polarization encoding, with any eavesdropping behavior detectable by quantum state collapse mechanisms.

In recent years, quantum key distribution technology has made important progress in network scaling. Research on quantum key distribution in large-scale networks [10] provides a technical foundation for multi-user key distribution, making it possible for quantum communication to extend from point-to-point to networked applications. Research on the evolution of quantum key distribution networks shows [11] that the quantum internet is gradually moving from concept to reality, laying the foundations for constructing global quantum secure communication networks. However, applications of quantum machine learning in quantum key distribution optimization remain in exploratory stages [12], particularly with relatively lagging application research in the engineering field.

Research in smart grid security provides an important reference for applications of quantum communication technology in power systems. A review of quantum key distribution protocols from the perspective of smart grid communication security [13] indicates that quantum communication technology can effectively address threats faced by traditional schemes, particularly suitable for protecting high-value power grid control data. However, existing research mainly focuses on protecting real-time control data, such as SCADA systems, with insufficient attention to security requirements for data in the engineering construction phase.

Engineering data security research has explored various approaches, including attribute-based encryption for BIM systems [14] and blockchain integration [15,16], while IoT-based collaborative design reveals cross-domain sharing limitations [17]. However, these solutions primarily rely on traditional cryptographic schemes with insufficient quantum threat consideration.

Current research has obvious gaps: a lack of quantum transmission protocol design for multi-dimensional characteristics of engineering data, a lack of quantum key management systems supporting complex multi-party collaboration, and a lack of integration solutions between quantum communication technology and existing engineering systems. Engineering data has characteristics such as multi-dimensional structure, dynamic updates, and version management, which differ significantly from traditional data types. The evolution of access patterns and permissions related to various project phases demands the necessity for flexible approaches to key management. Simulation studies on smart grid cyberattacks' implications [5] further extend evidence related to critical engineering data security protection requirements.

The research focuses on the secure transmission problem of substation 3D cost estimation data, and a systemic solution scheme is presented by utilizing quantum communication technology. Based on the designing scheme of a three-layer structure model involving quantum communication, the development of hybrid transmission schemes between the classical and quantum world, and hierarchical key management, a critical breakthrough is achieved among others from the computational security domain to the information theoretic security domain, a crucial void so far remaining in the usage of quantum communication technology among other areas related to engineering.

2. System Architecture and Protocol Design

2.1 Design Principles and Requirements

The secure transmission system design for the 3D cost estimation data of substation 3D has to offer information-theoretic security while taking into account both efficiency and usability requirements in engineering applications. Based on the requirements, secure transmission should offer information-theoretic security guarantees, which are assured by the laws of quantum mechanics, so that decrypted data will be impossible even if unlimited computational resources are exerted by the attacker. Eavesdropping detection availability checks QBER values in real time, with alarm signals given if QBER values are over 5% and transmission is stopped if values are over 11%. Forward security will guarantee that past data will remain secure even if future keys are exposed, as engineering confidentiality requirements are 30-50 years.

The functional requirements are: multi-party collaboration support involving 5-20 roles with role-based access control, verification of data integrity, and auditability. The performance requirements are: data transmission at a scale consistent with the GB level (throughput of 100Mbps or better, and latency of less than 100ms), a node number between 10 and 50,

The requirements related to practicality focus on the implications of integration and ease of deployment. The proposed solution should have the capacity to interface well with the presently developed BIM/CAD systems and should be compatible with leading engineering software like Revit and Navisworks. The deployability requirement addresses phased deployment, ultimately lowering the upfront capital expenditure involved due to this component.

2.2 System Overall Architecture

Towards addressing the requirements involved in the transmission of substation engineering data, this proposed thesis puts forward a three-layer structure model for quantum communication, including the system functions decomposed into the physical layer of quantum communication, the security network layer, and the service layer. Such a structure model adopts optimization ideas related to routing and load balancing principles designed by software-defined networks [18].

Figure 1 depicts the application service layer handling 3D cost information and BIM integration as per open BIM principles [19]. The service layer uses a quantum key-based AES 256-bit GCM encryption algorithm with role/phase-based security access controls.

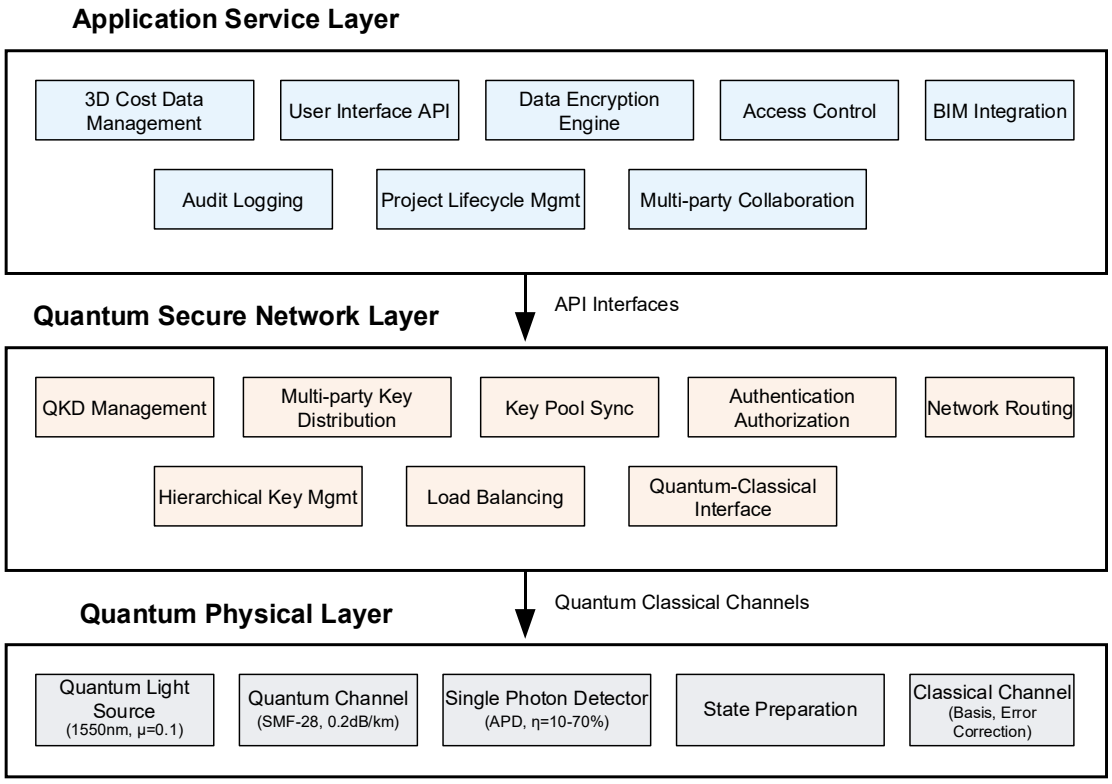

Figure 1. Three-layer Quantum Communication Architecture for Substation Engineering Data Transmission

The quantum security network layer is the central part of this system, as it performs critical tasks including quantum key distribution, multi-party cooperation management, and network route optimization. The structure of this layer takes into account the dynamic optimization strategies proposed by software-defined networks [20]. The multi-party quantum key distribution management supports star, mesh, and hybrid network topologies, which can be dynamically adjusted according to actual demands. The hierarchical key management mechanism can build a comprehensive key hierarchy system, including organizational-level master keys, session keys, and other related levels, so as to realize secure isolation between data of different levels.

The physical layer involves the execution of all the basic functions that make up a quantum communication system, including the preparation, transmission, measurement, and classical processing of the quantum states. The network uses a weak coherent pulse laser, whose photon number is fixed at 0.1, which optimizes the channel transmission, as well as network security. The SMF-28 attenuation value is 0.2 dB per kilometer, which facilitates point-to-point relay-free communication over 100-150km. The interaction between various layers is done by making use of API interfaces, whereby the application layer makes a key request for allocation at the network layer, which, in turn, instructs the physical layer to prepare a quantum state.

2.3 Quantum Physical Layer Design

The quantum physical layer realizes the physical functions for quantum communication, including the crucial building blocks: quantum light sources, quantum channels, single-photon detection, and quantum state preparation and measurement. The quantum light source uses an attenuated laser mode with an operational wavelength of 1550nm, corresponding to the low-loss region suitable for fiber communication. The average photon number is designed as μ = 0.1, reaching a condition suitable for around 9% probability of a single-photon pulse and 0.45% two-photon pulse, and the pulse rate is fixed at 1GHz, providing a high key rate. The light source is kept stable through temperature regulation and feedback adjustment, providing reliability and longevity as well as resistance to environmental disturbances.

The quantum channel operates with standard SMF-28 single-mode fiber, which has a loss of around 0.2 dB/km at a wavelength of 1550 nm. The fiber channels are advantageous due to their mature installation base and resistance to environmental noise, although they are limited by photon attenuation, making their operation over 100km require 1% efficient detectors to achieve the desired key rates. The detectors' polarization stability is dynamically varied by polarization controllers to allow for the birefringence effect-induced polarizations. The detectors are avalanche photodiodes operating in gated detection mode with 10-70% detection efficiency, a dark rate of less than 10^{-6}, and a temperature of -70°C.

The state preparation in the quantum system relies on a polarization encoding scheme involving four polarization states $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ to perform the BB84 scheme. The Z basis is represented by horizontal polarization state $|0\rangle$ and vertical polarization state $|1\rangle$, while the X basis involves +45° polarization state $|+\rangle$ and -45° polarization state $|-\rangle$. The electro-optical modulators and polarization controllers are involved in the process, with the accuracy impacting the bit error rate in the system. The measurement part involves polarization beam splitters and a single-photon detector array to realize measurements of all four states simultaneously.

The classical channel deals with the post-processing tasks involving synchronization, basis comparison, error correction, and privacy amplification, which require nanosecond precision and authenticity.

2.4 Quantum Key Distribution Protocol

The foundation of the overall system is the quantum key distribution. The scheme used by this research involves the integration of the BB84 algorithm and decoy state technology. The trends seen for communication algorithms in the future era of quantum technology show that quantum key distribution will play a central role in establishing "unbreakable communication systems" [21]. The BB84 algorithm makes use of the uncertainty principle of quantum mechanics to generate secure keys via a random process involving four states.

Figure 2 illustrates how the process involved in the BB84 protocol has both a classical post-processing stage and a quantum transmission stage. During the quantum transmission stage, while Alice randomly chooses polarized pulses with bits, as well as bases, Bob adopts independently selected bases to measure, resulting in perfect correlation achieved if both bases are the same.

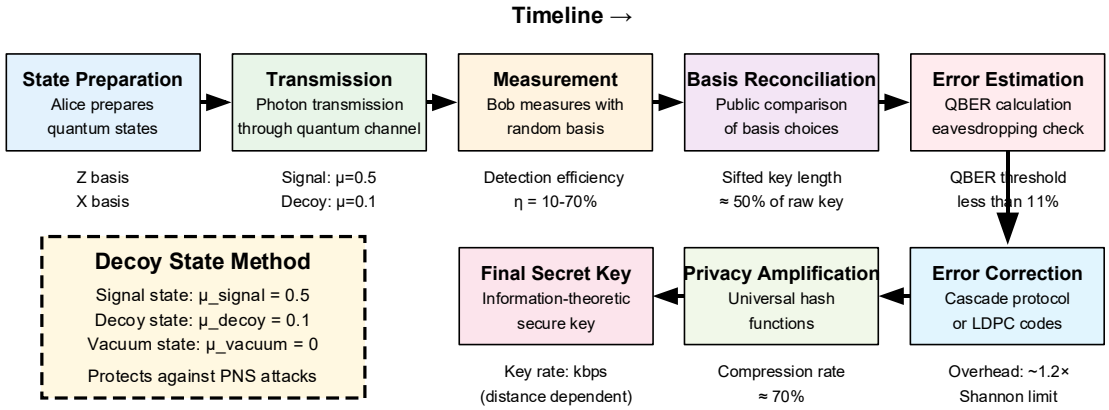

Figure 2. BB84 Protocol Implementation Flow with Decoy State Method

The classical post-processing stage performs tasks like basis reconciliation, bit error rate estimation, error correction, and privacy amplification via public channels. During the basis reconciliation procedure, both Alice and Bob make public their basis choice strings, but not the actual bit values, and keep measurement outcomes with matched bases to obtain the sifted key, around 50% of the original key size. The bit error rate estimation procedure involves a random sampling of 10-20% of the sifted key, with a continuation of the communication process if the QBER is lower than the specified 11% threshold value related to security.

The decoy state approach can resist photon number splitting attacks by transmitting signal pulses, decoy pulses, and vacuum pulses with parameters μ=0.5, μ=0.1, and μ=0, respectively.

The error correction involves the usage of the Cascade protocol or Low-Density Parity-Check (LDPC) codes, eliminating any possible mistakes in both Alice's and Bob's keys via two-way communication. The Cascade protocol relies on block-wise binary search, with theoretical results

showing a proximity to the Shannon limit and an actual cost factor of 1.2 times. The privacy amplification step involves the usage of universal hash functions, which removes any information that may have been gathered by Eve, finally constructing secure keys usable by the application domain.

2.5 Quantum-Classical Hybrid Transmission Protocol

Taking into account the large-scale features of the engineering data in substations, key consumption will be a problem if pure quantum key distribution schemes are applied alone. Based on the large key consumption demands of pure quantum key distribution schemes for GB-level data, the systematic research about the quantum cryptographic technology suggests that hybrid encryption schemes are the best approach to achieve a good balance between high security and high efficiency [22]. The hybrid scheme between the quantum and classical world proposed by this research will make use of the keys produced by the QKD to drive the AES-256-GCM algorithm operation.

As presented in Table 1, the technical requirements addressed by the system include the critical parameters related to the quantum layer, network layer, and application layer. The data encapsulation protocol applies a layered structure design, which breaks down large 3D model files into 10MB data pieces suitable for independent encryption. The data pieces are composed of three components: metadata header, encrypted payload, and authenticated tag. Taking a standard 200MB engineering data file, the traditional one-way pad approach demands 1.6×109 bits of quantum keys, whereas this hybrid approach breaks the data into 20 pieces, each requiring 256 bits of QKD keys, resulting in cumulative key demands totaling 5120 bits, an improvement by over 99.9%, with key generation times reduced to 0.17 seconds, down from 15 hours.

Table 1. Quantum-Classical Hybrid Transmission Protocol Specifications

Parameter	Specification	Security Level
Quantum Layer		
Wavelength	1550 nm	Telecom standard
Pulse Rate	1 GHz	High-speed operation
Mean Photon Number	$\mu = 0.1$ (signal), 0.05 (decoy)	Security optimized
Detector Efficiency	10-70% @ 1550nm	Temperature dependent
QBER Threshold	< 11% (abort), < 5% (continue)	Security monitoring
Network Layer		
Key Pool Size	1000-10000 keys	Dynamic buffer
Key Length	256 bits (AES-256)	Post-quantum secure
Network Topology	Star, Mesh, Hybrid	Scalable architecture
Max Nodes	10-50 nodes	Project scalability
Application Layer		
Data Block Size	10 MB	Optimized for QKD
Encryption Algorithm	AES-256-GCM	NIST approved
Compression Ratio	50-70% (3D models), 80-90% (tables)	Efficiency optimization
System Availability	≥ 99.9%	High reliability

The crucial usage strategy includes a principle of one-use, whereby each data block relies on a unique QKD key, which is destroyed afterwards. The key pool ensures a fixed minimum buffer pool (100-1000 keys). When the number of remaining keys goes below this, the QKD system automatically produces new keys. The integrity verification service relies on a dual-protection scheme, comprising both block-level integrity checks and file-level integrity checks. The block-level integrity checking makes use of the intrinsic Auth Tag of the AES-GCM mode, and the file-level integrity checking makes use of the calculation of the SHA-256 hash value of the file, which is protected by a distinct QKD key.

2.6 Application Layer Design

The application layer relies on the API gateway patterns for transparent BIM integration with Revit and Navisworks. The hierarchical permissions are established through a combination of role-based access control that involves project phase permissions, including full permissions exercised by the owner, management of day-by-day control by the manager, and dynamically changing role-based access rights given to engineers.

The data management functions are capable of version control, incremental updates, and collaborative editing for 3D cost estimation data. The version control system adopts a distributed version management approach, with new versions and their respective times produced every time the data is updated. The incremental updates are applying data differencing algorithms, hence reducing the volume of transmitted data, as they are just updated data blocks.

The audit system is capable of recording all cases involving access to data, modifications to permissions, and critical usage scenarios, thus creating an end-to-end operation log chain. Every audit entry will entail logging information,

logon identifier, type of operation, identifier representing the data, as well as the status of the result, all of which are capable of being queried from any number of dimensions, including timestamp, logon identifier, type, among others.

3. Key Management and Network Optimization

3.1 Multi-Party Quantum Key Distribution Network

Substation engineering projects are characterized by an involvement among various organizations, which demands the creation of a network of quantum communication, capable of a multi-party key distribution process. The topology of the network directly influences any network, either by making the network efficient or costly. A hybrid topology offers the best solution by providing all the nodes with a star connection, solving both the point and economic problems, as faced by star topologies present today. Research on quality-of-service-aware load balancing [23] supports dynamic optimization strategies for quantum network performance enhancement.

As shown in Table 2, different network topologies exhibit significant differences in latency, throughput, and deployment costs. Although star topology has the lowest cost, its average hop count is 2, with all communications requiring passage through the central node, easily creating performance bottlenecks. Hybrid topology controls the number of links within a reasonable range through hierarchical design, requiring only 147 links for a 50-node network with a cost index of 16.3, saving 88% of costs compared to full mesh topology while maintaining good performance.

Table 2. Network Topology Performance Comparison Results

Topology	Nodes	Avg Hops	Latency (ms)	Throughput (Mbps)	Links	Cost Index
Star	10	2.0	85	120	9	1.0
Star	20	2.0	92	115	19	2.1
Star	50	2.0	105	108	49	5.4
Mesh	10	1.5	60	180	45	5.0
Mesh	20	1.7	75	165	190	21.1
Mesh	50	1.9	95	145	1225	136.1
Hybrid	10	1.7	70	150	22	2.4
Hybrid	20	1.8	82	142	58	6.4
Hybrid	50	2.0	98	130	147	16.3

Multi-user quantum key distribution protocols need to solve key routing and synchronization problems. Key distribution between directly connected nodes is relatively simple, generating shared keys directly through point-to-point QKD. Non-directly connected nodes require key forwarding through intermediate nodes, which can adopt either hop-by-hop re-encryption or end-to-end key establishment schemes. A comprehensive study on the approaches involved in load balancing [24] shows that dynamic topology adjustment could react well to network dynamics, including network loading and faults, which offers valuable insights into how a scalable and fault-tolerant system should be designed.

3.2 Hierarchical Key Management System

The hierarchical key management system adjusts to substation engineering project structures by utilizing four tiers: organizational master keys, which have a 5-10 year lifespan, project keys, which are produced through HKDF and have a 2-5 year lifespan, phase keys, which are designed per stage of the project and have a 3-12 months lifespan, and session keys, which are produced immediately, utilizing one-time pad principles. Research on temporal optimization of deep learning in software-defined network load balancing [25] has inspired intelligent management strategies for key pools, enabling advanced preparation of sufficient key reserves by predicting key usage patterns and load changes.

Key pool management is an important component of the hierarchical key system. Session key pools need to maintain buffers of 1000-10000 keys to handle sudden transmission demands, automatically triggering the QKD system to generate new keys when remaining key quantities fall below thresholds. Key synchronization mechanisms are based on logical clocks and version numbers, ensuring all relevant nodes in the network use consistent keys for communication. Research on adaptive clustering methods for data center load balancing [26] provides a reference for the distributed deployment of key management systems, reducing the complexity of cross-domain key synchronization by clustering and managing nodes with close collaborative relationships.

3.3 Access Control Based on Roles and Project Phases

Access control considers user roles (owners, managers, engineers, auditors) and project phases, with hierarchical permissions from full owner access to specialized engineer roles with specific data restrictions.

Dynamic permission management based on project phases is an important feature of the system. During the design phase,

design teams have read-write permissions for design data, while construction teams cannot access incomplete design data. During the construction phase, design data becomes read-only to prevent arbitrary modifications, while construction teams gain viewing permissions for design data and read-write permissions for construction data. Once entering the acceptance stage, all data will remain read-only, and all audit teams will be allowed full view permissions. Some studies involving the optimization of load balancing and incremental updates related to SDN updates over ISP networks [27] show relevant data or ideas involving the optimization of permissions, including the adjustment of permissions through slower approaches to prevent interfering with other processes, focusing on a medium point between the continuity of a business and security aspects.

The rapid permissions by way of emergency schemes handle the demands regarding accessing the data under sudden conditions, which require permissions from two persons, and the period their permissions are valid should be 24-72 hours. The technology used in the process involved in managing access by applying technological approaches via attribute encryption and role-based mapping, assigning members their electronic identities that include attributes like roles, projects, and phases.

3.4 Dynamic Key Update and Revocation

The main revocation processes are involved in handling key revocations related to security emergencies. The revocation process is done under two categories: immediate revocation and planned revocation. The former is applicable when an emergency occurs, and the corresponding keys are immediately invalidated as soon as the threat to security is recognized, which may create a potential service interruption, but ensures security is paramount. The other involves predictable situations, with notifications given to all parties involved, including revocation timed to avoid any effects related to their activities. The process is involved in threat identification, evaluation, implementation, and follow-ups.

The key recovery procedures utilize secret-sharing technology, whereby important upper-level keys are broken down into several shares, each held at a secure, different location. The purpose of having sufficient shares is to reconstruct the important upper-level key, and key recovery procedures require multi-person authorization as well as verification of the persons' identities. Key recovery is facilitated, meaning a point of failure is avoided through making the keys recoverable.

3.5 Network Optimization Strategy

The optimization process regarding the performance related to node key generation rates, topologies, loading, and fault recovery is a complex process involving several parameters. The optimization related to topologies uses genetic algorithms that solve the optimal connection strategy methods, which rely on dynamic weighting schemes as functions related to node conditions, which include the current loading, pool of available keys, link quality, and reliability values. The calculation of the weights relies on weighted averaging, characterized by a dynamic adjustment scheme, which involves an increase related to the load factor weight values and key availability factor weight values, as indicated already.

The fault detection and recovery approaches utilize distributed collaboration algorithms, whereby each node will transmit heartbeat packets to other nodes, a node being suspicious if the timer times out with none received. The approaches utilised to achieve node fault recovery are, indeed, hot standby switching, path recalculation, and load transfer. Hot standby switching performs well if additional nodes are involved, as switching takes a mere 10 seconds. Path recalculation algorithms utilise Dijkstra algorithms, suitable if a node has a number of routes but does not have a standby node.

A network optimization procedure should, apart from performance indicators, take into account other abilities related to security protection as well. Redundancy designs for multi-path, intruder detection schemes, and security isolation schemes shield the network from downtimes resulting from communication link failures, intruder behavioral patterns, and spreading attacks, respectively. The network optimization strategy minimizes the impacts exerted by defects in equipment through the employment of designs and diversity principles, whereby the devices are purchased from different suppliers to eliminate shared defects, as well as periodic updates of device firmware to eliminate security vulnerabilities.

Performance monitoring systems obtain network operation data, such as the rates related to critical key generation, transmission delay, and error rates, as well as equipment status, through real-time monitoring. The information gained through monitoring is used for analysis, prediction, and optimization. The system provides comprehensive performance baselines, which automatically generate alarms and optimization controls once the monitoring indicators move out of the baselines. The system applies machine learning algorithms, which examine past network operation trends to make predictions and prevent maintenance, maintaining the system's long-term stability.

4. Security and Performance Analysis

4.1 Threat Model

The threat model deals with multi-level attacks, including eavesdropping via a quantum channel, classical channel tampering, man-in-the-middle attacks, as well as gaining access via social engineering.

The attack targets mainly include the theft of plaintext 3D cost estimation information, manipulating the data content, resulting in illogical decisions, manipulating identities to impersonate authorized users accessing systems, interfering with availability to inhibit regular operations, as well as

gaining access to the encryption keys to decrypt past or future information. The system trust model explicitly specifies trusted versus untrusted components, including physical laws for a quantum system, security-certified QKD hardware, as well as secure internal environments within the nodes, as trusted components, while including channels involving quantum, classical channels, partial nodes on a network, as well as external network environments, as untrusted components.

The threat assessment matrix offers quantitative assessment results of various threats issued from three aspects: attack possibility, effect degree, and detection difficulties. Eavesdropping attacks, even with a high possibility, are believed to have a low effect due to their real-time detection by the mechanism of quantum state collapse. Man-in-the-middle attacks, with extremely high effect degree, could be well protected by the mechanism of identity authentication.

4.2 Attack Scenarios and Defense Mechanisms

The simplest type among eavesdropping attacks is the intercept and resend attack, where the eavesdropped states are measured, and the resulting states are re-sent. Owing to the no-cloning theorem, eavesdropping action causes an increase in errors. Calculations show that if there is no eavesdropping, the system QBER is around 1-2%, while with eavesdropping, the QBER becomes around 25%. The system implements eavesdropping detection by monitoring QBER values, raising an alarm if QBER is greater than 5% and halting key generation if QBER is greater than 11%.

The system protects against photon number splitting attacks by decoy state approaches and man-in-the-middle attacks by combined schemes for authenticity. The integration approach with machine learning-based anomaly detection will allow detection of attack patterns by analyzing network patterns and performance [28].

4.3 Security Proof

The security of quantum key distribution is rooted in information theory and is independent of the computational power of potential eavesdrovers. The theory of perfect secrecy by Shannon shows that the one-time pad offers perfect secrecy if the key is at least as long as the message, the key is randomly generated, and the key is reused nowhere. The keys produced by a QKD are physically random, and the bits produced by a measurement of a quantum state are, by their nature, random.

The GLLP formula provides rigorous lower bound estimates for secure key generation rates in BB84 protocols. Research on the security of imperfect devices [29] emphasizes the impact of device defects on security in practical QKD systems. The system ensures reliable security guarantees even with imperfect devices through device calibration, parameter optimization, and security margin design.

As shown in Figure 3, system performance versus transmission distance curves demonstrate the patterns of key generation rate, QBER, and transmission efficiency changes with distance. Within 50km distance, key generation rates remain at high levels (8-40 kbps), sufficient to meet engineering data transmission requirements. QBER increases slowly with distance but remains within the safe range below 5% even within a 100km distance.

Security proof also needs to consider composable security, i.e., how the security of individual QKD links extends to the security of the entire network. The hierarchical key management system ensures long-term security of the entire system through measures such as minimizing the usage frequency of high-level keys, adopting forward-secure key derivation functions, and implementing secure key destruction.

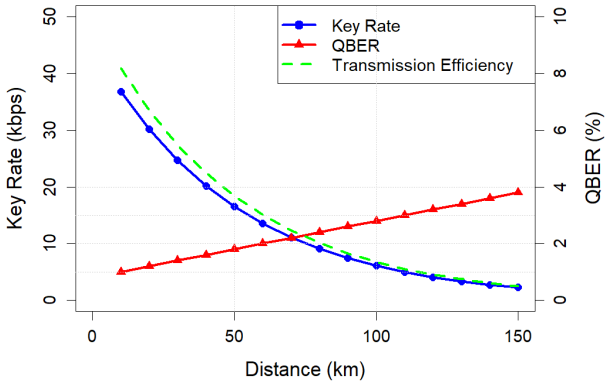

Figure 3. Key Generation Rate and System Performance vs. Transmission Distance.

4.4 Simulation Verification

Comprehensive simulation validation employed QuTiP for the quantum layer, NetSquid for the network layer, and Python/NetworkX for application analysis, with network modeling guided by software-defined network research [30]. Parameters included 1550nm wavelength, 1GHz pulse frequency, 0.1 average photon number, 20% detection efficiency, 0.2dB/km fiber loss, and 10-50 node networks across 10-100km distances. The simulation verification involves areas like the performance verification of single-link QKD, network performance comparison among multiple nodes, verification of the load balancing algorithm, fault recovery, and security verification.

As presented in Table 3, simulation results show that the quantum communication model has a marked advantage over traditional communication models. When analyzing the level of security, the quantum communication model has information-theoretic security, whereas traditional communication models can offer computational security at best. When analyzing resistance to quantum attack, the quantum communication model is totally resistant to the threat of quantum computing. When analyzing eavesdropping detection, the quantum communication model can

immediately identify eavesdropping, with a detection rate of 98.5%.

Table 3: Simulation Results and Comparison with Classical Methods

Metric	Classical Method	QKD Method	Improvement
Security Level	Computational	Information-theoretic	✓ Fundamental upgrade
Key Exchange Time	0.05 s	2.1 s	-4100%
Data Encryption Speed	1.2 GB/s	1.2 GB/s	0% (Same AES)
Quantum Attack Resistance	Vulnerable	Immune	✓ Complete protection
Forward Secrecy	Limited	Perfect	✓ Enhanced
Eavesdropping Detection	Not available	Real-time	✓ New capability
Key Consumption (1GB data)	2048 bits	25,600 bits	-12.5×
Deployment Cost (10 nodes)	$10,000	$500,000	+50×
Attack Detection Rate	Not applicable	98.5%	✓ New metric
System Availability	99.5%	99.2%	-0.3%

Hybrid topology shows cost-effectiveness over scales ranging between 10-50 nodes, providing a 23% improvement over star topology and over 80% cost savings compared to mesh topology. The simulation results show a 23% improvement in throughput performance and a 28% improvement in response time due to the load-balancing algorithm, assuming dynamic weight approaches are taken by the algorithm. The fault recovery simulation shows the system's fault detection and recovery process completed within 60 seconds with a 0% data loss rate.

Researches related to security protection for the control infrastructure of the power grid identify significantly valuable references related to security requirements for critical infrastructure [4]. The verification process confirms the security by simulation tests to validate defenses against attacks. The decoy state approach proves to be efficient against PNS attacks, identity authentication approaches are successful in preventing any man-in-the-middle attack, and detection rates for DoS attacks are 98%, signifying strong security protections provided by the system.

5. Discussion

5.1 Main Advantages

The devised quantum communication framework reaches a level of information-theoretic security that satisfies 30-50-year engineering archive confidentiality requirements, and real-time eavesdropping detection via QBER monitoring, which are unachievable by traditional frameworks [21].

The three-layer structure designed for the system ensures the smooth integration of quantum security technology and engineering information systems. The application layer guarantees full transparency of security schemes when users are accessing BIM software through API gateway designs [19]. The hybrid key transmission scheme between the classical and quantum worlds significantly reduces key usage by over 99.99%, making the applicability of quantum communication technology viable at the engineering data transmission scale. The hierarchical key management system developed is fully compatible with the organizational structure and engineering projects' lifecycle dynamics of substation engineering projects [26]. The dynamic role-based and engineering project phase-based permission management guarantees detailed data management permissions by the hierarchical key management system.

5.2 Limitations and Challenges

Although the security benefits are substantial, various technological hurdles remain to make the technology viable in a cost-effective manner. The physical constraints relating to the rates of key generation are the primary technical hurdle being overcome by this technology, with the current state-of-the-art QKD technology averaging key generation rates measured in kilobits per second [29]. The distance of transmission is restricted by the loss in the fibers, which usually does not exceed 150 kilometers, so trusted relay nodes or satellite-based QKD are required for engineering applications involving extensive areas.

The main difficulties are high investment costs (ranging between 50 and 200 times over standard technology), strict environmental conditions, a competitive standard, integration requirements with BIM or CAD technology [30], training, and undefined legal frameworks. Even if the applications developed with quantum communication technology guarantee high security at a technological level, they could be vulnerable to other types, like social engineering, attacks, or internal threats [4].

5.3 Practical Deployment Recommendations

The strategy involving phased progression will be beneficial to mitigate technology investment risk. The initial pilot stage should identify 2-3 core nodes, with primary tests conducted around the verification of simple system functions and operation robustness. The ideal choice for pilot nodes should consider major participants, including project owners and principal design institutes, to validate technological feasibility by point-to-point QKD channels, as they accumulate operational experience. The expansion deployment phase will extend network scale to 5-10 major collaborators, adopting a hybrid topology design balancing performance and cost [23].

Cost optimization strategies could effectively lower investment by implementing a core-edge hierarchical topology, whereby core business data is protected by quantum security, and general collaboration data is protected by traditional encryption approaches. It is advised to explore a 'QKD as a Service' approach, as this could lower upfront investment expenses by leasing or renting services. Geographical distribution features of projects should be taken into account when network topology optimization is performed to enhance system effectiveness via intelligent loading approaches [25].

Integration with legacy systems should focus on API gateway patterns, ensuring compliant, secure encryption services by utilizing middleware integration [27]. API gateway patterns manage conversion protocols, keying, and security policy enforcement, enabling top-layer BIM applications to obtain coverage by the quantum security shield without any modifications. The integration processes should evaluate all areas, including data type compatibility, performance, and usability, to prevent disruptions by the integration of new technology into the system.

5.4 Future Research Directions

The future will see technological advances in the areas of quantum relay and satellite technology, leading to the development of global networks, while storage technology will facilitate asynchronous communication and mobile communication. The development space given by the expansion of the application domain will continue to drive the development of quantum communication technology. The areas involving engineering services, space engineering, military engineering, and fields characterized by strong security requirements will all be applicable cases for the development and utilization of quantum communication technology [28]. The complete quantization of smart grids will allow the entirety of the energy sector to achieve the primary guarantee of security, including the security of SCADA systems, distributed energy communication, as well as the security of trading data.

The promotion of standardization activities has crucial meaning to technological industrialization. The formation of industry standards for the quantum transmission of engineering data, key management specifications, and security level certification systems will create institutional guarantees for technology promotion and application. The participation in international standard activities will guarantee that technology development routes are synchronous with international trends, as well as enhance technology ecosystem quality by reducing compatibility difficulties among devices via technology improvement. The promotion of standardization will greatly lower technology barriers to applications, pushing the transformation of quantum communication technology achievements into applications.

6. Conclusion

A quantum communication model is proposed for secure 3D cost estimation data transmission between substation, which will tackle security challenges in the post-quantum era via a three-layered structure with hybrid protocols supporting both quantum and classical systems, resulting in information-theoretic security with 99.99% less key usage. The simulation results show 8-40 kbps key rates are achieved between 50-100km, and hybrid topology results in an optimal cost-effective solution with 99.9% availability, making this a totally new full-scale quantum communication-based solution applicable to the engineering field, promoting a secure multi-party collaboration solution through the project duration while fully integrated with BIM systems seamlessly. Quantum communication technology applied to engineering applications will be made possible by this study, providing foundational security tools for critical infrastructure data, marking an important milestone toward securing a post-quantum world.

Author Contribution

Conceptualization, J.L. and F.Y.; methodology, J.L.; software, F.Y.; validation, J.L., F.Y. and D.C.; formal analysis, J.L.; investigation, F.Y.; resources, D.C.; data curation, F.Y.; writing—original draft preparation, J.L.; writing—review and editing, J.L. and D.C.; visualization, F.Y.; supervision, J.L.; project administration, D.C.; funding acquisition, J.L. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

The datasets generated and analyzed during this study are available from the corresponding author upon reasonable request due to privacy and security considerations related to substation engineering data.

Funding

This research received no external funding.

Ethics Statement

Not applicable.

Conflict of interest statement

The authors have no relevant financial or non-financial interests to disclose.

References

[1] Achaal, B., et al., *Study of smart grid cyber-security, examining architectures, communication networks, cyber-attacks, countermeasure techniques, and challenges.* Cybersecurity, 2024. **7**(1): p. 10.

[2] Knake, R.K., *A Cyberattack on the U.S. Power Grid*. 2017, Council on Foreign Relations.

[3] Holik, F., S.Y. Yayilgan, and G.B. Olsborg, *Emulation of Digital Substations Communication for Cyber Security Awareness.* Electronics, 2024. **13**(12): p. 2318.

[4] Jarmakiewicz, J., K. Parobczak, and K. Maślanka, *Cybersecurity protection for power grid control infrastructures.* International Journal of Critical Infrastructure Protection, 2017. **18**: p. 20-33.

[5] Abraham, D., et al., *Consequence simulation of cyber attacks on key smart grid business cases.* Frontiers in Energy Research, 2024. **Volume 12 - 2024**.

[6] García, C.R., et al., *Enhanced Network Security Protocols for the Quantum Era: Combining Classical and Post-Quantum Cryptography, and Quantum Key Distribution.* IEEE Journal on Selected Areas in Communications, 2025. **43**(8): p. 2765-2781.

[7] Lo, H.-K., M. Curty, and K. Tamaki, *Secure quantum key distribution.* Nature Photonics, 2014. **8**(8): p. 595-604.

[8] Mummadi, S. and S. Fathima. *A Comprehensive Study on Quantum Key Distribution Protocols*. in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. 2024.

[9] Padamvathi, V., B.V. Vardhan, and A.V.N. Krishna. *Quantum Cryptography and Quantum Key Distribution Protocols: A Survey*. in *2016 IEEE 6th International Conference on Advanced Computing (IACC)*. 2016.

[10] Mangla, C., S. Rani, and A. Abdelsalam, *QLSN: Quantum key distribution for large scale networks.* Information and Software Technology, 2024. **165**: p. 107349.

[11] Cao, Y., et al., *The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet.* IEEE Communications Surveys & Tutorials, 2022. **24**(2): p. 839-894.

[12] Purohit, K. and A.K. Vyas, *Quantum key distribution through quantum machine learning: a research review.* Frontiers in Quantum Science and Technology, 2025. **Volume 4 - 2025**.

[13] Kong, P.Y., *A Review of Quantum Key Distribution Protocols in the Perspective of Smart Grid Communication Security.* IEEE Systems Journal, 2022. **16**(1): p. 41-54.

[14] Liu, J., et al., *Traceable Attribute-Based Encryption Scheme Using BIM Collaborative Design.* Buildings, 2024. **14**(3): p. 731.

[15] Das, M., X. Tao, and J.C.P. Cheng, *BIM security: A critical review and recommendations using encryption strategy and blockchain.* Automation in Construction, 2021. **126**: p. 103682.

[16] Wang, J., et al., *Research on multi-person collaborative design of BIM drawing based on blockchain.* Scientific Reports, 2022. **12**(1): p. 16312.

[17] Feng, M. and H. Wu, *Construction of a BIM smart building collaborative design model combining the Internet of Things.* Nonlinear Engineering, 2025. **14**(1).

[18] Tache , M.D., O. Păscuțoiu, and E. Borcoci, *Optimization Algorithms in SDN: Routing, Load Balancing, and Delay Optimization.* Applied Sciences, 2024. **14**(14): p. 5967.

[19] Kong, L., et al., *Open BIM exchange on Blockchain 3.0 virtual disk: A traceable semantic differential transaction approach.* Frontiers of Engineering Management, 2025. **12**(3): p. 510-528.

[20] Forghani, M., M. Soltanaghaei, and F. Zamani Boroujeni, *Dynamic optimization scheme for load balancing and energy efficiency in software-defined networks utilizing the krill herd meta-heuristic algorithm.* Computers and Electrical Engineering, 2024. **114**: p. 109057.

[21] Wei, D.S.L., et al., *Guest Editorial: Building a More Secure Future: Developing Unbreakable Communication Protocols for the Quantum Era.* IEEE Journal on Selected Areas in Communications, 2025. **43**(8): p. 2728-2731.

[22] Durr, E.S., et al., *Quantum Cryptography for Future Networks Security: A Systematic Review.* IEEE Access, 2024. **12**: p. 180048-180078.

[23] Rostami, M. and S. Goli-Bidgoli, *An overview of QoS-aware load balancing techniques in SDN-based IoT networks.* Journal of Cloud Computing, 2024. **13**(1): p. 89.

[24] Farahi, R., *A comprehensive overview of load balancing methods in software-defined networks.* Discover Internet of Things, 2025. **5**(1): p. 6.

[25] Sharma, A., V. Balasubramanian, and J. Kamruzzaman, *A Temporal Deep Q Learning for Optimal Load Balancing in Software-Defined Networks.* Sensors, 2024. **24**(4): p. 1216.

[26] Mahmoudi, M., et al., *A new method for load balancing in DSDN-Based data centers using adaptive clustering and normal Cone-Based estimation approaches.* Expert Systems with Applications, 2025. **280**: p. 127606.

[27] Cheng, Y., et al., *Optimizing incremental SDN upgrades for load balancing in ISP networks.* Theoretical Computer Science, 2023. **962**: p. 113927.

[28] Alhilali, A.H. and A. Montazerolghaem, *Artificial intelligence based load balancing in SDN: A comprehensive survey.* Internet of Things, 2023. **22**: p. 100814.

[29] Gottesman, D., et al. *Security of quantum key distribution with imperfect devices*. in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.* 2004.

[30] Houhamdi, Z. and B. Athamena. *Load Balancing Algorithms for Software-Defined Networks*. in *2023 Tenth International Conference on Software Defined Systems (SDS)*. 2023.