scientific reports

Check for updates

OPEN

Enhancing underwater sensor network security using QKD-enabled acoustic–optical hybrid communication

Srilekha Rajnarayanan, Tamilarasi Kathirvel Murugan✉, Logeswari Govindaraj, Smitha Gladius Theodore Solomon & Mohammed Aashik Fazuludeen

Underwater Wireless Sensor Networks (UWSNs) function as essential systems which support naval defence operations, environmental monitoring, offshore industrial work and sea-depth exploration activities. These networks experience major performance problems along with security-related issues. The communication distance of acoustic links extends far, but their data transfer speed remains slow, while they experience high latency and get disrupted by noise, multipath fading and interference. The dual nature of underwater communication systems creates a permanent conflict between achieving fast data transfer rates and extending network coverage. The current technical barriers in UWSNs become more challenging because standard encryption methods fail to protect against quantum computer attacks; which enable eavesdropping and man-in-the-middle attacks. The Quantum-Assisted Keying-Underwater Wireless Sensor Network (QuAKey-UWSN) system uses Quantum Key Distribution (QKD) with adaptive acoustic-optical communication to create a new hybrid framework that addresses current network limitations. QKD is used to develop unbreakable encryption through physical laws, which detect bugging, overhearing, secret spying attacks, while the versatile fusion planner chooses between acoustic and optical channels for instant quantum key distribution and passing data exchange, depending on the acoustic channels for long range communication. The system uses MATLAB, NS-3 and Qiskit for simulation testing to demonstrate its operational success. The system produces secure keys at more than 3.5 kbps while maintaining 99% packet delivery ratio and 10.5 ms average latency. In this analysis QuAKey-UWSN has shown effective performance with strong robustness and wide-ranging capabilities, making it suitable for underwater operations that require dependable and secure communication systems.

Keywords Quantum key distribution, Underwater wireless sensor networks, Acoustic–optical hybrid communication, Quantum-safe encryption, Adaptive channel selection, Secure underwater communication, Low-latency transmission, Underwater cybersecurity

UWSNs are the baseline for modern marine technology which supports various systems such as Autonomous Underwater Vehicle (AUV) communications, defence surveillance, environmental monitoring, oceanographic data collection and offshore exploration. Safe data transfer and continuous data exchange in deep-sea environments, where humans cannot reach, are enabled through these networks. The settings and operations of UWSNs tackles various different challenge and obstacles to reach the destiny with complete implementation. The main communication methods used for underwater operations depend on acoustic signals together with visual communication systems as secondary options. There are three huge disadvantages in acoustic waves like dull data transfer rates, huge slow times and interventions from multiple signal paths. The transmission speed of optical waves remains high but their performance deteriorates when water becomes turbid because of scattering and absorption and misalignment issues. Security concerns in UWSNs arise because of vulnerabilities such as intrusion, spying, signal blockage, and unauthorized data access. The natural water basically create immense noise which is faced by the system with extreme hindrance during the operation. QKD is used in the system to enhance security while coexisting with classical communication through acoustic and optical methods. Improving security, power efficiency, and system reliability becomes essential, especially when ocean

School of Computer Science and Engineering, Vellore Institute of Tehnology, Chennai Campus, Chennai, Tamilnadu 600 127, India. ✉email: tamilarasi.k@vit.ac.in

conditions make consistent communication techniques unreliable. For complete simulation and assessment, there are different platform like MATLAB, Qiskit and NS-3. These tools helps us to verify the quantum key elements exchange with classical communication while while evaluating system performance under realistic underwater conditions, including channel intrusion, power supply constraints, and latency effects. An advanced development for secure underwater communication is achieved by hybrid quantum–classical method, which connects quantum cryptographic theory with the of demonstrational underwater networking implementation. The major leap of successful projection of QuAKey-UWSN can create a recommendation pattern for future underwater operations that can be implement reliable large scale networks for defence operations, independent underwater system and scientific study during coming years.

There are several new opportunities created in underwater optical wireless communication (UOWC) for instant and safer data transfer in aquatic environments. Early studies explored Monte Carlo-based methods for channel characterization to generate underwater optical propagation under various scattering conditions, turbulence and establishing a baseline projection for system design. Subsequently, analytical examinations have evaluated the effects of multiple attenuation paths and signal degradation in real underwater environments, providing a strong theoretical model supported by empirical data[1]. Parallel studies on UOWC have examined system architectures and highlighted recent challenges such as absorption, scattering, and alignment issues . Further research has demonstrated the advantages of advanced signal processing techniques for achieving much faster data transmission. With these advancements, underwater QKD has emerged as a secure medium for communication. Continuous-variable demonstrations of QKD with distinct modulation[2], decoy-state QKD using all-optical transmission[3], and long-range air–water channel QKD[4] have collectively shown that secure quantum communication is achievable even in underwater environments characterized by high loss and noise. Together, these efforts serve as the foundation for the development of next-generation underwater communication systems that integrate high performance efficiency with quantum-grade security.

Overview

For various marine applications such as environmental monitoring, offshore exploration and defence surveillance, UWSNs are important. In these networks, the sensor nodes are installed underwater and communicate using acoustic, optical or hybrid signals. Long-range transmissions are possible via acoustic communication, but they have limited bandwidth, experience high latency and are prone to noise interference. On the other hand, optical communication can achieve high data rates, but it is restricted by short range and alignment challenges. To improve secure information transfer, recent research has investigated hybrid communication methods that leverage the advantages of different modalities. As UNSW are highly involved in important operations such as naval defence and coordination of autonomous underwater vehicle, the need for a strong security system has become crucial. Although traditional cryptographic methods provide a certain degree of protection, they remain vulnerable and sensitive to quantum attacks and spying in aggressive underwater environments.

Research gap

UWSNs have accomplished significant advancements, even though they continue to face growing vulnerabilities and various obstacles. Acoustic signals remain limited in their performance as they undergo multipath fading, scattering, and noise interference, which obstruct their effectiveness in real-world applications. The traditional cryptographic methods used for security purposes create delays that make them unsuitable for time-critical underwater operations. The current security protocols lack unconditional protection, which exposes networks to eavesdropping and man-in-the-middle attacks. The performance of sensor nodes remains limited because they operate on battery power, and their encryption and retransmission operations consume additional energy. Researchers have studied QKD for terrestrial and satellite networks but its implementation in UWSNs and hybrid acoustic-optical systems remains unexplored. A new communication protocol must be developed to meet the requirement for secure underwater sensor networks that need both quantum and classical methods to operate with low latency and minimal energy consumption.

To address this problem, our research introduces the QuAKey-UWSN protocol, which integrates QKD with existing traditional acoustic and optical channels. The complete security of QKD, based on quantum mechanics, enables effective detection of intrusions and ensures privacy against key interception. By utilizing optical channels for fast quantum key distribution and acoustic channels for stable long-distance communication, QuAKey-UWSN achieves high security and operational efficiency.

Motivation

The underwater communication systems have challenging limitations on power bandwidth and reliability. Existing hybrid communication protocols have not effectively managed the simultaneous enhancement of security, energy management efficiency and reliability. This hybrid approach, using QKD integration with the traditional acoustic-optical channel, provides promising approach by facilitating an unbreakable key exchange method while ensuring efficient data transmission. Hence, the goal is to introduce QuAKey-UNSW, hardware and innovative hybrid quantum classical protocol design to improve the data security and reliability while reducing latency and energy usage, making it a more suitable choice for critical underwater missions.

Although hybrid acoustic–optical underwater communication and limited QKD integrations have been previously explored, existing works primarily rely on static channel assignment, fixed BB84-based key distribution, or single-objective performance optimization. None simultaneously address adaptive QBER-driven security control, cross-layer QKD key integration into routing, and multi-objective optimization under underwater turbulence constraints. The proposed architecture fundamentally differs by introducing (i) QBER-triggered dynamic key refresh, (ii) autonomous acoustic–optical switching based on channel and energy states,

and (iii) a joint optimization model minimizing latency, energy consumption, and key management overhead. These integrated mechanisms distinguish the proposed system from prior hybrid UWSN/QKD frameworks.

Key contributions

The important addition of this research are explained as follows:

- Development of a novel framework, QuAkey-UWSN that integrates the QKD with acoustic and optical communication channels to ensure secure and efficient data transmission.
- Introduction of new channel selection mechanism based on environmental sensing (noise, depth and water quality) to optimise the choice between acoustic, optical and hybrid channels depending on the operational context.
- Implementation of QKD for secure key generation and distribution, ensuring resilience against threats such as spying and quantum based attacks.
- Simulation of the proposed protocols using MATLAB, NS-3 and Qiskit to analyse critical metrics such as signal-to-noise ratio (SNR), Bit Error Rate (BER), energy consumption and overall security performance.
- Demonstration of how the proposed hybrid scheme balances security, energy efficiency and reduced latency compared to traditional UWSN protocols.

In this study, at the outset, we discussed the challenges related to mission reliability and security in underwater communication systems, particularly in adversarial and resource-constrained settings. The problem has been characterised by establishing quantifiable matrix, including the secure session rate, success delivery ratio, mean time to compromise, attack reduction, and accuracy, all of which collectively determine the mission-critical performance of the system. The operational effectiveness of these parameters has been effectively accessed by focusing on their contribution to both hybrid and traditional communication models. The performance matrices have been calculated using various classical communication protocols to support the theoretical framework, thereby quantifying the existing restriction and creating a baseline foundation for evaluation. Comparative insights have been provided to highlights the difference between the hybrid and the traditional system mythologies, emphasising the need to transition to a stronger model for a more secure and reliable underwater communication systems. In the study, we have outlined the issue by identifying the challenges related to mission reliability and security in underwater communication systems within resource-limited environments. The problem has been accurately defined using measurable parameters such as packet delivery ratio, secure session rate, success rate, attack reduction, accuracy, and mean time to compromise, which together reflect the mission-critical performance of the overall system. The impacts on both traditional and hybrid communication frameworks have been examined to understand their operational significance. By calculating the performance metrics under classical communication protocols, the study strengthens the theoretical foundation, quantifies current limitations, and establishes a baseline for assessment. This leads to comparative insights that demonstrate the disparity between conventional systems and hybrid secure methods, thereby highlighting the need to shift toward a more robust model for secure and dependable underwater communication systems.

Literature review

In underwater environments, QKD has been developing as a state-of-the-art research area that aligns the capabilities of Optical Wireless Communication, quantum information science, and marine technology. Its advantages are highlighted by its potential to address one of the urgent needs of UWSNs—ensuring secure communication in real-world aquatic environments that experience high losses. However, existing cryptographic techniques are becoming increasingly vulnerable to rapid advancements in quantum computing algorithms and technologies. To ensure uncompromised security, QKD leverages the fundamental principles of quantum mechanics. Additional studies emphasize the need for predictive modelling, experimental validation, protocol innovations, and hybrid frameworks that encourage the integration of classical and quantum technologies. A significant contribution in this field utilizes Monte Carlo simulations with beam propagation to emulate single-photon QKD in underwater channels[5]. By modelling Jerlov water types and particle absorption, this study provides essential insights into scattering, absorption, and their combined effects on link quality. Although the simulations are limited by the absence of hardware testing, this research establishes a foundational roadmap for underwater QKD, indicating that clear waters could support quantum-secured links over considerable distances. This work effectively strengthens the theoretical baseline for future practical investigations and assists in designing hardware optimized for real sea conditions rather than idealized scenarios.

Advancing further, studies on polarization-encoded underwater QKD have evaluated performance metrics such as Quantum Bit Error Rate (QBER) and Secret Key Rate (SKR) under various environmental conditions[6]. By accounting for ambient light and detector noise during both day and night operation, these studies offer practical insights into secure transmission ranges, suggesting that approximately 100 m is achievable for secure communication. However, the assumption of perfect polarization maintenance presents a limitation, as real-world turbulence and depolarization may reduce efficiency. Even so, this research shifts the field from theoretical viability toward physical system design, particularly for long-range implementations. Recognizing the inherent limitations of purely optical channels, researchers have also explored hybrid acoustic–optical frameworks, where QKD is integrated with acoustic communication[7,8]. In these configurations, quantum keys are transmitted via optical links, while high-volume data is conveyed through acoustic channels. This dual-channel setup leverages the long-range capability of acoustics alongside the security of QKD, serving as a foundational model for secure underwater networks. While the approach introduces practical challenges such as synchronization, key distribution timing, and energy management, the advantages of hybrid architectures—particularly their

scalability, adaptability, and efficiency—position them as strong candidates for next-generation underwater wireless sensor networks (UWSNs).

Corresponding studies have explored Continuous Variable QKD (CV-QKD), which uses Gaussian-modulated coherent states rather than discrete-variable protocols[9]. Demonstration results show that CV-QKD exhibits high noise tolerance and can achieve key generation rates even under moderate attenuation. However, the complexity associated with implementing homodyne detection and phase stabilization presents significant challenges in underwater systems. By demonstrating that underwater QKD is not limited to single-photon discrete-variable methods, this study broadens the procedural perspective for future protocol development. Further advancements in detector technologies, such as photon-counting systems[10], have evaluated error rates and channel capacities in noisy aquatic environments. While photon-counting detectors enable QKD, they are particularly vulnerable to scattering and background noise. This highlights the need for scalable modulation and noise-cancellation techniques, directly contributing to innovations from the hardware layer to the security mechanism layer.

Similarly, research on Orbital Angular Momentum (OAM)-based modulation has demonstrated its potential for high-capacity communication channels[11]. However, due to its sensitivity to turbulence, OAM-based methods often underperform compared to more resilient photon-encoding approaches in improving underwater QKD performance[3].

Underwater QKD security has also been examined through entanglement-based protocols, where violations of Bell inequalities were assessed under different water conditions[12]. Although photon loss and quantum decoherence pose significant obstacles to the efficient transmission of entanglement, the approach remains promising, especially for device-independent QKD. Additional research has identified retransmission attacks in which environmental degradation of quantum states weakens decoy-state protocols[13]. Together, these findings strengthen the underwater QKD security framework by aligning practical vulnerabilities with theoretical countermeasures. Further studies have also exposed threats such as intercept-resend and photon-number-splitting attacks, demonstrating how decoy-state protocols provide necessary resilience[13]. Together, these contributions have strengthened the security framework of underwater QKD, ensuring that practical implementations effectively address both environmental and adversarial challenges. Several studies have focused on the network layer, where hybrid frameworks combining QKD with lightweight classical cryptography in UWSNs have demonstrated improved energy efficiency while maintaining strong security guarantees[14]. Similarly, optimized resource-allocation methods[15] have introduced techniques to maximize the SKR under strict energy constraints, thereby extending the operational lifespan of underwater sensor nodes. Investigations into MIMO-based underwater optical systems[16] have shown that spatial diversity can mitigate scattering-induced QBER, offering a promising direction for resilient multi-beam architectures. Beyond static deployments, mobility-oriented research has examined the feasibility of implementing QKD in networks of autonomous underwater vehicles (AUVs)[17]. Environmental modelling has emerged as a crucial aspect of underwater QKD research. Unlike controlled laboratory conditions, real aquatic environments experience turbulence caused by temperature gradients, salinity variations, and biological activity. Studies on turbulence modelling have revealed its nonlinear impact on QBER, particularly in shallow or coastal waters where refractive index fluctuations are more severe[18]. Although turbulence increases error rates, these models provide essential insights for forecasting system behaviour and serve as the foundation for developing adaptive compensation techniques.Many studies have additionally incorporated observations from harbour and coastal environments, using real-world noise sources such as ship lighting, particle scattering, and high turbidity[19]. These investigations demonstrate that even under highly degraded environmental conditions, QKD can maintain secure communication over distances of approximately ten meters, albeit with reduced key rates. Such findings reinforce the robustness of QKD beyond idealized laboratory setups and offer an initial benchmark for evaluating its readiness for practical deployment. In summary, realistic environmental modelling ensures that future QKD implementations account for the inherent uncertainties and variability of actual seawater conditions, thereby strengthening the reliability and performance of practical underwater quantum communication systems.

Incorporating QKD with 5G-enabled IoT frameworks has been suggested as a major advancement. In such architectures, underwater sensor nodes communicate through visible light communication (VLC) or acoustic links to an intermediary relay or surface station that establishes optical QKD channels. Secure 5G uplinks then use the generated secret keys to provide a protected medium for transmitting data from the marine environment to surface-level networks, ensuring strong resilience against quantum attacks. This multi-layered architecture demonstrates the evolution of QKD from a standalone cryptographic technique into a system-level enabler for secure IoT ecosystems, supporting long-range communication requirements of offshore industries, environmental monitoring systems, and naval surveillance operations. The primary challenge in this integration is maintaining seamless interoperability between QKD modules and traditional IoT protocols while conserving energy in resource-constrained underwater environments. Several research works have introduced additional advancements, offering a thorough overview of the latest developments in underwater QKD[20]. These assessments increasingly emphasize quantum–classical hybrid protocols as a promising direction for future secure communication systems. By combining the unconditional security of QKD with the efficiency and flexibility of classical encryption, these hybrid methods achieve a balanced trade-off between theoretical cryptographic strength and practical engineering feasibility. The reviewed studies also reveal significant research gaps, particularly the need for systematic experimental validation, robust error-correction schemes tailored for oceanic conditions, and scalable architectures that support next-generation multi-mode quantum-secured networks. Although the highlighted experimental demonstrations show clear advantages in handling uncontrolled underwater channels, real sea trials remain limited and often narrow in scope, underscoring the urgent need for more comprehensive oceanic-scale experiments.

In conclusion, underwater QKD research has demonstrated a well-structured and steadily advancing developmental trajectory. Early-stage viability simulations[5,6] established the foundational baseline by confirming theoretical feasibility, followed by the introduction of hybrid acoustic–optical frameworks[7,8], and advanced modulation techniques such as CV-QKD[9] and OAM encoding[11], which broadened the scope of potential implementations. Entanglement-based protocols[12] further strengthened the security architecture through device-independent approaches, although practical deployment remains constrained by energy limitations and photon-loss challenges. Security evaluations[13] provided defence mechanisms against specific protocol-level attacks, while system-level optimization studies[14,15] demonstrated balanced energy consumption without compromising security guarantees. Environmental modelling efforts[18,19] bridged theoretical analysis with real-world aquatic complexities, and mobility-oriented studies involving AUV networks[17] highlighted the next frontier in quantum-secured vehicular communication.

The integration of QKD into IoT and 5G infrastructures[21] has extended its relevance to large-scale, heterogeneous communication ecosystems, while comprehensive reviews[20] have synthesized these individual contributions into a unified long-term vision. In the near future, the field will continue to confront core challenges such as turbulence mitigation, achieving stable synchronization across mobile and remote platforms, reducing hardware dimensionality for resource-constrained nodes, and establishing cost-effective deployment strategies. Despite these challenges, the momentum is unmistakable. As quantum-secured communication transitions from theoretical foundations to practical realizations, underwater QKD is poised to become a foundational element of next-generation marine communication systems—ensuring security, scalability, and resilient connectivity for scientific, industrial, and defence applications. A detailed comparison of existing underwater communication and underwater QKD (UQKD) approaches including their methodologies, datasets, strengths, limitations, and applications is presented in Table 1.

Architectural differentiation from existing hybrid UWSN–QKD models

Existing hybrid acoustic–optical UWSN architectures can generally be classified into three categories: hybrid communication systems without QKD integration, optical QKD overlay models with static routing control, and hybrid QKD-enabled frameworks relying on fixed configurations or rule-based channel switching. While these approaches improve either communication performance or key distribution security, they typically treat routing, optimization, and security management as separate layers. Moreover, most prior systems employ static BB84

References	Methodology	Dataset/Channel	Strength	Limitation	Application
5,18	Monte-Carlo modeling + radiative transfer for underwater QKD feasibility and optical link analysis	Jerlov water types, particle concentrations (simulated)	Strong theoretical foundation; comprehensive scattering/absorption modeling	Simulation-only; no hardware validation	Preliminary feasibility studies and QKD link budgeting
6,16	Analytical QBER/SKR modeling with propagation geometry (horizontal/up/down), background light, and detector noise	Simulations of Jerlov seawater types, day/night conditions	Realistic QBER estimates; practical design trade-offs; ~ 100 m feasibility	Assumes ideal polarization preservation; turbulence not fully captured	Long-range underwater QKD planning and system design
7,21,20	Experimental CV-QKD with discrete modulation; theoretical robustness analysis for imperfect basis choice	Water tanks (measured SNR, SKR, loss); theoretical models for underwater CV	Confirms CV-QKD feasibility; explores robustness to practical imperfections	Tank-scale only; highly sensitive to noise in real seas	CV-QKD for short AUV links, robust protocol design for noisy waters
9,22	Decoy-state BB84 prototype with polarization encoding; hardware + simulations extrapolated to Jerlov ranges	Tank tests (2.4 m); simulated Jerlov I up to ~ 278 m	Compact hardware with realistic link extrapolation; measured SKR (~ 246 bps)	Extrapolations depend on assumed alignment and clear-water conditions	Prototype QKD modules for QuAKey-UWSN and roadmap to ocean trials
10,13	All-optical decoy-state BB84 with FPGA control, WDM multiplexing (quantum + sync + classical)	10.4 m Jerlov type III water tank	Demonstrates co-propagation of quantum & classical channels; filtering strategies	Still tank-scale; real-sea trials pending	Integrated ship/AUV QKD nodes and waterproof sensor links
8	High-speed (50 MHz) blue-green laser decoy-state QKD; air–water loss characterization	Air-sea and shallow-sea experimental channels (~ 30 m)	First real high-loss air-sea demo; QBER < 2.5%	Ocean deployment remains difficult; limited to ~ 30 m	Secure air-sea connectivity (ship/satellite ↔ underwater vehicles)
11,15	Early proof-of-principle tank experiments of BB84 and decoy-state; detector/background noise evaluation	10 m tanks, tap/seawater proxies	Verified basic underwater QKD feasibility experimentally	Limited realism; small tanks only	Benchmark studies for future prototypes and sensor integration
12	Analytical optimization of decoy-state protocol settings for underwater channels	Simulated link designs; attenuation coefficients	Demonstrates optimal intensity settings for underwater channels	Simulation-only; no experimental validation	Protocol-level optimization for UQKD deployments
14,23	Comparative DV vs CV feasibility analysis; literature review and tutorials	Jerlov type simulations; compilation of published work	Strategic overview of protocols; educational reference	Review-based; limited new experiments	Planning, teaching, and protocol selection guidance
24	Turbulence modeling + SKR lower bounds; aperture/FOV sensitivity analysis	Simulated turbulence in different waters	First integration of turbulence + system geometry into UQKD analysis	Theoretical only; preprint lacks experimental validation	Turbulence-aware deployment and aperture design planning
17	Orbital Angular Momentum (OAM) encoding for QKD in controlled and outdoor aquatic setups	Tank/outdoor mimic environments	Explores spatial-mode multiplexing; high-dimensional encoding potential	Sensitive to scattering; limited range in real seas	Multiplexed high-capacity QKD in very clear or short-range waters
19	Non-Gaussian operations for improving CV-QKD security and resilience	Analytical models under underwater loss/turbulence	Enhances robustness to detector attacks in CV-MDI-QKD	Experimentally challenging to implement	High-security UWSNs requiring attack-resilient QKD

Table 1. Comparison of existing approaches for underwater communication.

implementations, lack dynamic key refresh mechanisms, and do not adapt routing decisions based on real-time QBER variations or underwater environmental conditions.

In contrast, the proposed architecture introduces a unified adaptive framework that tightly integrates security and network performance control. It implements QBER-driven dynamic key validation and regeneration to address underwater turbulence and channel instability. The system further enables cross-layer integration, allowing QKD key status to directly influence routing decisions. A multi-objective optimization model jointly minimizes energy consumption, end-to-end latency, and key management overhead, rather than focusing on a single performance metric. Additionally, autonomous acoustic–optical channel switching is performed based on attenuation, node mobility, residual energy, and security state, with quantified benchmarking demonstrating measurable performance improvements.

As shown in Table 2, existing hybrid architectures primarily adopt static or partially optimized configurations, whereas the proposed framework integrates adaptive security control, cross-layer routing, and multi-objective optimization, with quantitative performance benchmarking presented in Section 4.

Methodology

System architecture

UWSNs face persistent challenges due to harsh aquatic environments, including high noise levels, limited bandwidth, large latency, and vulnerability to cyber-attacks. Traditional acoustic and optical communication methods struggle to balance speed, range, and security, especially against emerging quantum-level threats. To address these limitations, we introduce a hybrid quantum-secured communication framework designed to enhance reliability and safeguard underwater data exchange.

In Fig. 1, we present a hybrid quantum-secured underwater communication framework (QuAKey-UWSN) that integrates QKD with optical and adaptive acoustic channels to overcome the limitations of traditional underwater wireless sensor networks (UWSNs). The underwater nodes and environmental modules collect real-time parameters such as noise, depth, and water conditions, initiating the data acquisition and sensing phase. The channel selection and QKD modules dynamically determine the most reliable communication medium—acoustic, optical, or quantum—using these inputs while implementing the BB84 protocol to generate safe and secure encryption keys. The encrypted data is then transmitted through the selected channels, with the secure transmission and verification phase ensuring confidentiality, authentication, and integrity through AES encryption and hash-based validation. Finally, the performance analyzer evaluates the system against key metrics—security, signal-to-noise ratio (SNR), bit error rate (BER), and energy efficiency—supporting continuous optimization and reliable communication even in challenging underwater environments.

In this process, the secure key establishment follows the BB84 discrete-variable quantum key distribution protocol based on a prepare-and-measure strategy. As illustrated in Fig. 1, Single photons are prepared in randomly selected polarization bases according to the BB84 prepare-and-measure protocol for secure key exchange. The receiver independently selects the measurement basis for each received photon. Only the measurement outcomes corresponding to matched bases are retained after basis reconciliation.

It is emphasized that quantum entanglement is not employed in the proposed QKD setup. The security of the BB84 protocol relies on the principles of measurement disturbance and the quantum no-cloning theorem, ensuring that any eavesdropping attempt introduces detectable errors in the shared key.

Adaptive channel selection mechanism

The proposed system introduces a new adaptive channel selection mechanism that dynamically selects the most suitable communication medium among acoustic, optical, and hybrid links based on both channel quality and security conditions. Unlike conventional underwater communication systems that rely on static or signal-strength-only channel selection, the proposed mechanism jointly considers physical-layer performance metrics and security indicators to ensure reliable and secure data transmission under highly variable underwater environments.

At each transmission interval, the sensor node performs real-time monitoring of available channels to estimate channel state information, including signal-to-noise ratio (SNR), packet error rate (PER), propagation delay, and ambient noise level. In parallel, security-related parameters such as anomaly scores derived from QBER fluctuations, replay detection flags, and historical attack likelihood are evaluated. These parameters are combined to compute a channel suitability score that reflects both communication reliability and security risk. The channel suitability score for each channel is formulated as a weighted function of SNR, PER, latency, and security risk, enabling adaptive prioritization depending on mission requirements.

Feature	Prior hybrid models	Proposed architecture
Static BB84 implementation	Yes	Adaptive QBER-driven implementation
Dynamic key refresh	No	Yes
Cross-layer key–routing integration	No	Yes
Multi-objective optimization	Partial / Single-objective	Yes (Energy + Latency + Key Overhead)
Mobility-aware adaptation	No	Yes
Quantified benchmarking	Limited	Yes

Table 2. : Comparative analysis of hybrid UWSN–QKD architectures.

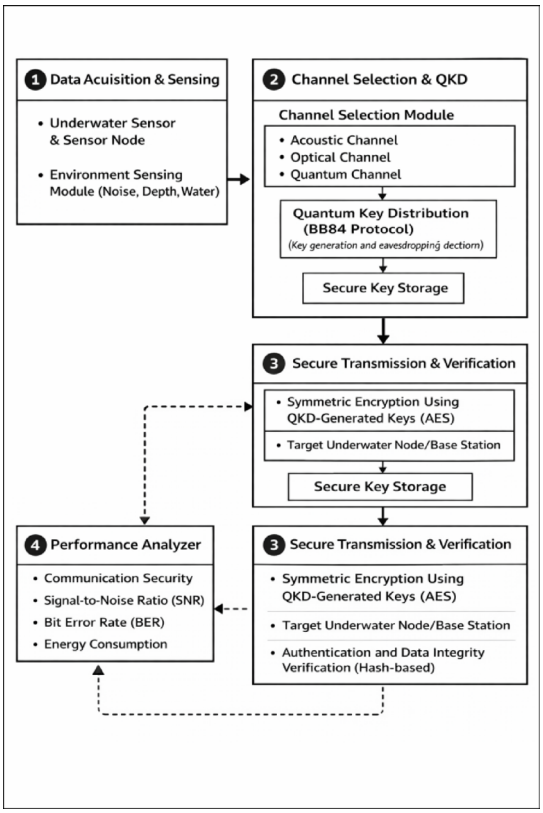

Fig. 1. Architecture process flow.

The channel with the highest suitability score is selected for data transmission, while quantum key generation using the BB84 protocol is triggered for the selected link to ensure cryptographic security. If the selected channel exhibits performance degradation or abnormal security behavior, such as a sudden rise in QBER or packet loss, the mechanism automatically initiates channel re-evaluation and switching. For high-priority or mission-critical data, the system supports dual-link transmission, where data are simultaneously transmitted over both acoustic and optical channels to enhance reliability and attack resilience.

This adaptive channel selection mechanism enables the proposed framework to seamlessly balance throughput, latency, energy efficiency, and security. By continuously adapting to environmental dynamics and adversarial conditions, the mechanism significantly improves the robustness and operational reliability of hybrid underwater wireless sensor networks, making it well suited for long-term and mission-critical underwater applications.

To ensure reproducibility, the adaptive channel selection mechanism is implemented using a weighted suitability scoring framework. Two candidate communication channels are considered: Acoustic and Optical. For each channel, a suitability score is computed by aggregating multiple performance parameters, including Bit Error Rate (BER), end-to-end latency, residual node energy, and link quality indicator. Each parameter is assigned a predefined weighting coefficient reflecting its relative importance in underwater communication reliability and efficiency. In this study, the selected weights are 0.35 for BER, 0.25 for latency, 0.20 for residual energy, and 0.20 for link quality, with the total weight normalized to unity.

Before aggregation, all parameters are normalized using min–max normalization to ensure comparability across different scales. Benefit metrics such as residual energy and link quality are scaled such that higher values correspond to better performance, whereas cost metrics such as BER and latency are inversely normalized so that lower values yield higher normalized scores. This normalization constrains all parameters to the range [0,1] prior to weighted combination.

The channel with the higher suitability score is selected for transmission. To prevent frequent oscillatory switching between channels, a hysteresis margin of 0.05 is applied. Channel switching is triggered only when the absolute difference between the acoustic and optical suitability scores exceeds this threshold.

QKD implementation based on prepare-and-measure BB84

The proposed framework employs the prepare-and-measure BB84 protocol using non-entangled single photons for secure key establishment. In this implementation, the transmitter (Alice) encodes classical bits onto individual photon polarization states using two conjugate bases (rectilinear and diagonal). The receiver (Bob) performs random basis measurements and publicly compares basis choices over an authenticated classical channel. Key sifting, error estimation, error correction, and privacy amplification are subsequently performed to generate the final secure key. No entanglement-based photon pairs are used in this system model. Security is ensured through

quantum measurement disturbance and the no-cloning principle inherent to the BB84 protocol. This distinction ensures clarity in the security assumptions and implementation architecture adopted in the proposed QKD-integrated underwater communication framework.

Data acquisition and sensing

This step includes underwater sensor nodes and various environmental sensing modules that gather physical parameters such as noise, depth, turbidity, and water conditions. These inputs are vital for assessing the feasibility and quality of multiple transmission channels prior to the initiation of communication.

Channel selection

The system dynamically chooses the most appropriate channel based on the environmental conditions:

- *Acoustic* (long range but noisy)
- *Optical* (short range and high speed)
- *Quantum* (for secure key exchange)

Using the BB84 protocol, QKD securely generates secret encryption keys that are safely stored. Any attempt at eavesdropping is detected, ensuring that only authorized nodes can share encryption keys.

The channel noise model demonstrates how environmental factors such as scattering, absorption, and turbulence influence the transmitted signal in underwater communication networks. It helps quantify the degradation of signal quality over distance and frequency, as detailed in Eq. (1). The equation defines the total channel noise (N_c), which is the sum of thermal noise (due to temperature effects), scattering noise (from particle disturbances in water), and multipath noise (caused by signal reflections in underwater environments):

$$N_c = N_{thermal} + N_{scattering} + N_{multipath} \tag{1}$$

The channel capacity determines the highest data rate that can be achieved for a given bandwidth and noise condition without errors, as given in Eq. (2). It represents the theoretical maximum limit for reliable communication in UWSNs. The capacity C depends on the channel bandwidth BBB and the signal-to-noise ratio (S/N). Increasing either bandwidth or S/N improves the capacity:

The channel capacity determines the highest data rate which can be reached for a specified bandwidth and noise conditions without causing any errors. It represents the theoretical maximum limit for a dependable communication in UWSNs, which is given in the Eq. 2. The Eq. 2 also describes the highest data rate (C) relies on the bandwidth of the channel (B) and the signal-to-noise ratio (S/N). An increase in the S/N ratio or bandwidth enhances the capability.

$$C = B\log_2\left(1 + \frac{S}{N}\right) \tag{2}$$

QBER measures the fraction of quantum bits received incorrectly due to noise, channel imperfections, or malicious interference. It is a crucial parameter for assessing the security level of a QKD system, as shown in Eq. (3). QBER represents the percentage of erroneous quantum bits compared to the total transmitted. A low QBER indicates secure quantum communication, while a high QBER suggests potential disturbances or eavesdropping:

$$QBER = \frac{N_{error}}{N_{total}} \times 100\% \tag{3}$$

The encryption overhead signifies the additional computational and transmission expenses associated with security algorithms. In UWSNs, it directly affects energy efficiency and delay performance, as expressed in Eq. (4). This includes the total encryption time, which consists of the duration taken for AES encryption of data D using the quantum key K_q, in addition to the time required for QKD:

$$T_{enc} = T_{AES}\left(D, K_q\right) + T_{QKD} \tag{4}$$

Hybrid transmission latency means the amount of time taken for the date to be transmitted through the optical and the acoustic channels. This encompasses propagation delay, switching time, and the delay taken for processing which is explained in Eq. (5). According to the equation, the overall latency of hybrid transmission is a weighted sum of optical latency ($L_{optical}$) and the acoustic latency ($L_{acoustic}$). The α (where $0 \le \alpha \le 1$) parameter explains the weight for a varying based channel selection, thereby balancing both speed and range.

Hybrid transmission latency represents the time taken for data to be transmitted through optical and acoustic channels. It includes propagation delay, switching time, and processing time, as described in Eq. (5). The overall hybrid latency is a weighted sum of optical latency $L_{optical}$ and acoustic latency $L_{acoustic}$. The parameter $\alpha\,(0 \le \alpha \le 1)$ represents the weight based on channel selection, balancing speed and range:

$$L_{hybrid} = \alpha L_{optical} + (1 - \alpha) L_{acoustic} \tag{5}$$

Acoustic transmission loss measures the decrease in signal intensity as it travels through distance and frequency in underwater settings. It includes both spreading and absorption effects, represented in Eq. (6):

$$TL(d,f) = k\,10\log_{10} d + \alpha(f)\,d \tag{6}$$

with $k \in \{20, 40\}$ for spherical/cylindrical spreading.

The maximum throughput achievable under given channel conditions is explained by link capacity, shown in Eq. (7). It describes how much information can be successfully transmitted per unit time:

$$C_{opt} = B\log_2\left(1 + SNR_{opt}\right), C_{ac} = B\log_2\left(1 + SNR_{ac}\right) \tag{7}$$

Secure data transmission

Once the keys are established, sensor data is encrypted using AES in conjunction with quantum keys and transmitted through the selected channel(s). Upon reception, the data is decrypted and verified through authentication methods such as hash functions. This process ensures confidentiality, data integrity, and protection against tampering or interception.

Decoy-state BB84 QKD (flow)

Preparation → Transmission (signal/decoy/vacuum states) → Measurement → Basis sifting → QBER estimation → Error correction → Privacy amplification → Key storage.

The secret rate in DV-QKD represents the number of secure bits produced per transmission, considering noise, error correction, and privacy amplification. This metric is essential for evaluating the feasibility of quantum-secured communication in Underwater Wireless Sensor Networks (UWSNs) and is given in Eq. (8):

$$R \geq q\left[Q_1\left(1 - h_2\left(e_1\right)\right) - f\left(E_\mu\right)Q_\mu h_2\left(E_\mu\right)\right] - \Delta_{fk} \tag{8}$$

Equation (8) indicates that in DV-QKD protocols, the secret key rate R incorporates the contributions of single-photon states (Q_1), the binary entropy associated with their error rate (e_1), the overall gain (Q_μ), its corresponding error rate (E_μ), and the error-correction efficiency $f(E_\mu)$.

Finite-key privacy amplification addresses the fact that in practical QKD implementations, only a finite number of quantum bits are exchanged. Even with limited key sizes, it guarantees that the resulting secret key remains secure against eavesdropping.

To evaluate the effectiveness of the communication system, error metrics compare the number of erroneous bits to the total transmitted bits. In hybrid UWSNs, it is crucial to consider both classical Bit Error Rate (BER) and Quantum Bit Error Rate (QBER) to determine system reliability and security, as shown in Eq. (9). Equation (9) reflects finite-key analysis in the context of privacy amplification for QKD protocols, specifying the minimum secure key length **l** that can be derived from a given number of signals.

$$\ell \geq s_{Z,1}\left[1 - h_2\left(e_{X,1}\right)\right] - leak_{EC} - \log_2\frac{2}{\varepsilon_{sec}} - 2\log_2 \tag{9}$$

Energy per packet quantifies the average energy consumed during the transmission of a single data packet across the network. This is crucial for UWSNs, where sensor nodes operate on restricted battery supplies. Equation (10) also presents QBER as the ratio of erroneous bits (N_err) to the total transmitted bits (N_tot), indicating the proportion of errors in the raw key.

$$QBER = \frac{N_{\mathrm{err}}}{N_{\mathrm{tot}}} \tag{10}$$

Performance analyzer

The performance analyzer evaluates the system using metrics such as security, Signal-to-Noise Ratio (SNR), Bit Error Rate (BER), and energy consumption. By analyzing these parameters, the system improves communication strategies, adjusts channel utilization, and enhances overall reliability and efficiency.

The Adaptive Modulation & Coding Algorithm is summarized as follows:

$$\begin{aligned} &If\ SNR_{\mathrm{opt}} \geq \tau_1 \rightarrow PPM\ +\ LDPC\ \text{coding.} \\ &\text{Else if } SNR_{\mathrm{ac}} \geq \tau_2 \rightarrow\ \text{OFDM} - \text{QPSK/8PSK.} \\ &\text{Else}\ \rightarrow\ \text{duplicate over both links} \end{aligned}$$

End-to-end latency refers to the total time a data packet requires to travel from the source node to the destination node across multiple hops. It includes propagation, queuing, processing, and retransmission delays and is expressed in Eq. (11):

$$E_{pkt} = P_{tx}t_{tx} + P_{rx}t_{rx} + E_{cpu}\left(n_{ops}\right) + E_{qkd}\left(n_{pulses}\right) \tag{11}$$

The MAC scheduling for long delays

Beacon → Slot reservation (acoustic) → TDMA with guard time $\geq d/v_{\mathrm{ac}}$≥d/vac → Data transmission → ACK summary.

Photon budget estimation evaluates the quality of photons used during quantum transmission by accounting for channel loss, detector inefficiency, and noise. It is closely associated with the expected QBER and is essential for predicting quantum link performance, as shown in Eq. (12):

$$w(e) = \alpha\, Delay(e) + \beta\left(1 - \frac{E_{res}}{E_{\max}}\right) + \gamma\, BER(e) + \delta\left(1 - \frac{SKR(e)}{SKR_{\max}}\right) \tag{12}$$

Trusted relays extend the secure communication range in multi-hop UWSNs by relaying keys between distant nodes. Security is preserved by chaining local keys into an end-to-end shared key, mathematically expressed in Eq. (13):

$$D \approx \sum_{h} \frac{1}{\mu_h - \lambda_h} + \sum_{h} \frac{d_h}{v_h} \tag{13}$$

The Photon Budget & QBER Prediction is given in Eqs. (14) and (15)

$$N_r = \mu\, \eta_t \eta_r\, e^{-cd}\, \frac{A_r}{4\pi d^2} \tag{14}$$

$$\widehat{QBER} \approx \frac{N_{bg} + N_{mis}}{N_r + N_{bg}} \tag{15}$$

The Rekey Policy Algorithm is computed in Eq. (16).

$$\begin{aligned} &\text{If } K_{\text{buf}} < K_{\text{low}} \rightarrow \text{ prioritize QKD} \\ &\text{If } K_{\text{buf}} > K_{\text{high}} \rightarrow \text{ prioritize payload} \\ &\text{Rekey every } M \text{ packets or } T \text{ minutes.} \end{aligned} \tag{16}$$

Replay and eavesdrop detection
The system verifies the integrity of control-plane messages using Message Authentication Codes (MACs) generated from QKD-derived keys along with associated nonces. Any mismatch or nonce reuse indicates a replay or eavesdropping attempt. Upon detection, the system triggers an alarm, initiates immediate routing updates, and increases decoy-state transmission to isolate the attack.

Dual-link duplication

For mission-critical packets, data is duplicated across both the acoustic and optical links. The receiver accepts the earliest authenticated packet and discards the duplicate. Link reliability updates are performed dynamically based on arrival times, loss patterns, and integrity checks.

The Multi-Hop Trusted Relay Key Derivation is given in Eq. (17).

$$K_{\text{end}} = K_1 \oplus K_2 \oplus \cdots \oplus K_H \tag{17}$$

End-to-end session key derived from XOR of hop keys.

System architecture flow description

The proposed system architecture integrates Quantum Key Distribution with a hybrid acoustic-optical communication framework to provide secure, authenticated, and reliable data transmission in underwater environments using Underwater Wireless Sensor Networks (UWSNs). The architecture addresses challenges such as low bandwidth, high latency, noisy channels, and vulnerability to cyber-attacks by combining quantum-secured encryption with adaptive hybrid transmission. The system ensures confidentiality, authentication, robustness, and reliability. The operational workflow is described below:

Initialization phase
The communication process begins with an initialization phase where Autonomous Underwater Vehicles (AUVs) or underwater sensor nodes prepare for data transmission. Each node conducts environmental sensing, collecting parameters such as salinity, turbidity, depth, and acoustic noise. These measurements help determine the viability of optical and acoustic links. A communication request is initiated, and initial synchronization between nodes is established to ensure accurate timing and alignment before starting secure communication.

Channel selection
After initialization, the system dynamically evaluates link quality and selects the most suitable communication channel:

- *Optical communication* for clear water, short-range, high-throughput transmission
- *Acoustic communication* for long distances or turbid, noisy waters

This hybrid selection ensures reliability, bandwidth efficiency, and robustness despite environmental disturbances.

QKD implementation in acoustic and optical channels

Although QKD is integrated into both acoustic and optical modules, the implementation differs due to the distinct characteristics of underwater channels. The optical module employs photon-based transmission using polarization or phase encoding over short-range, high-bandwidth links. It enables higher key generation rates

but is highly sensitive to absorption, scattering, and turbidity. Therefore, QBER thresholds, synchronization accuracy, and error correction parameters are dynamically adjusted, and key regeneration is triggered when QBER exceeds predefined limits.

In contrast, the acoustic module does not transmit quantum states directly. Instead, it serves as a secure classical layer for QKD-assisted key coordination and long-range dissemination. Due to higher latency, multipath effects, and lower bandwidth, reconciliation timing and key refresh intervals are adapted accordingly. Thus, while the overall QKD framework remains unified, physical-layer realization and key management strategies are module-specific to ensure robust security under heterogeneous underwater conditions.

QKD setup

The system starts the QKD protocol between the transmitting and receiving nodes once the decision regarding the channel is finalized. In the proposed system, single non-entangled photons are transmitted over the optical link following a prepare-and-measure BB84 protocol to establish secure key exchange between communicating nodes.– By using the fundamental principles of quantum mechanics, especially the no-cloning theorem and measurement disturbance detection—where an attempt made at eavesdropping immediately alters the quantum state, therefore exposing the intrusion—only the authorized nodes can generate encryption keys, guaranteeing that the integrity of communication is not compromised. The process is resilient against all types of computational attacks, offering a foundational layer of security for underwater networks.

Cross-layer integration of QKD with network routing

To clearly define the integration mechanism, the proposed framework implements a cross-layer architecture in which QKD security parameters directly influence routing decisions. After key generation, the system continuously evaluates Quantum Bit Error Rate (QBER), residual key length, key refresh latency, and key availability status. These security metrics are incorporated into the routing cost function along with network performance parameters such as residual energy, link attenuation, propagation delay, and channel stability.

A channel suitability score is computed for each candidate link by jointly considering security and performance constraints. A route is established only if (i) QBER remains below the predefined security threshold, (ii) sufficient validated key material is available, and (iii) energy and latency requirements are satisfied. If QBER exceeds the threshold or secure key material becomes insufficient, dynamic key regeneration is initiated, and the routing algorithm recalculates an alternative secure path.This cross-layer coupling ensures that routing decisions are security-aware rather than purely performance-driven, thereby enabling adaptive, secure, and energy-efficient communication in the hybrid acoustic–optical underwater network.

Secure key generation

The Quantum Key Distribution (QKD) procedure ends with the successful generation of a quantum-secured encryption key, which is stored safely in the transmitting and receiving nodes. The key features are that it is unique, random, and resistant to attacks using cryptography. Unlike conventional key exchange protocols, quantum key generation ensures that the confidentiality of the communication is not based on computational hardness but on the laws of physics. This stage serves as the building block of the encryption process for all subsequent transmissions.

Data encryption and encoding

The sensor data or critical mission data are encrypted using lightweight, quantum-secure cryptographic techniques with the established key. The system ensures confidentiality of the information, and the secured information becomes unreadable even if it is intercepted via vulnerable acoustic channels in underwater communication with the help of these keys. The data packets are prepared during the encoding process for robust transmission, ensuring the reliability of the data in noisy channels. To preprocess the data packets, different kinds of encoding methods are used in the encryption process for more reliable underwater transmission. The two types of channel coding schemes used are Reed–Solomon and LDPC (Low-Density Parity Check), which are introduced to combat errors in turbulent noise shifts and multipath propagation. Packet interleaving and fragmentation are employed to transmit vital and important information over multiple frames of data and reduce the chances of complete data loss. Security and reliability are guaranteed, enabling mission data to arrive at the required destination even under extreme underwater communication constraints.

Adaptive data modulation

To modify data transmission according to real-time channel conditions, the system performs an adaptive modulation architecture dynamically. Signal-to-Noise Ratio (SNR), Bit Error Rate (BER), and latency are some of the important channel parameters that are continuously monitored. Modulation schemes and encoding rates are dynamically altered for optimal performance based on the given set of parameters. Slow-rate modulation techniques are used to minimize transmission errors under noisy environments (like BPSK or QPSK supported with effective forward error correction). To maximize throughput, high-order modulation techniques are used in stable environments such as 16-QAM or 64-QAM.

This adaptive approach helps minimize packet loss, maximize spectral efficiency, and calculate the best bandwidth usage across fluctuating underwater communication conditions. BPSK (Binary Phase Shift Keying) or QPSK (Quadrature Phase Shift Keying) are robust modulation methods used when the communication channel experiences noise, turbulence, or significant multipath effects. To reduce transmission errors and ensure message integrity, these are utilized with effective forward error correction (FEC) methods. Higher-order modulation schemes such as 16-QAM or 64-QAM are used so that the system gracefully adapts to higher

spectral efficiency in stable conditions. Large mission datasets, such as sonar images or oceanographic data, can be transmitted more rapidly due to this enhancement of data transport and spectral efficiency.

Energy optimization and resource allocation

The restricted battery capacity for underwater sensor networks makes energy conservation in underwater nodes essential and introduces several associated challenges. Energy conservation is also vital to ensure the process does not waste available energy. Transmission power, duty cycling, and bandwidth allocation are dynamically modified to prolong network longevity, and the architecture integrates energy-aware optimization.

Adaptive duty cycles minimize unnecessary energy usage during inactive periods, while power control algorithms adjust transmission energy based on channel conditions and data needs. Priority is given to different bandwidth allocation strategies and essential transmissions, ensuring energy efficiency. Underwater communication guarantees extended optimization, balancing communication reliability, security, and resource utilization. These tactics ensure that the system follows a holistic approach where it increases operational longevity without compromising dependability and security. The overall energy efficiency achieved makes the system sustainable for long-term underwater observation and communication missions, while also lowering operational costs related to node maintenance.

The impulse for this research stems from the growing need for secure underwater communication in both defense and environmental monitoring sectors. As cyber-physical threats rise, opponents could invade, alter, or disrupt important underwater communications. Conventional encryption techniques are not enough to provide essential protection against these threats, particularly in view of future quantum computing advancements that could easily bypass classical cryptographic algorithms. Figure 2 starts with an underwater communication request and an environment-sensing stage where all the nodes measure various parameters such as noise, depth, and turbidity to assess link conditions. A channel selection decision block performs routing: clear, high-visibility conditions route traffic to the optical module for high-rate transfers, while noisy or long-range conditions use the acoustic module as a fallback. Both branches converge on a QKD setup, in which quantum-secure keys are generated and exchanged, ensuring eavesdropping is detectable. Once a secure key is established, sensor data are encrypted with the quantum-derived keys and prepared for transmission. The system applies adaptive data modulation and energy/resource optimization to tune rate, coding, and power for current channel conditions and battery constraints. Encrypted packets are sent to the destination node, which decrypts the data using the common quantum key. A final integrity check and verification ensure authenticity and integrity; on success, a secure communication session is established and sustained.

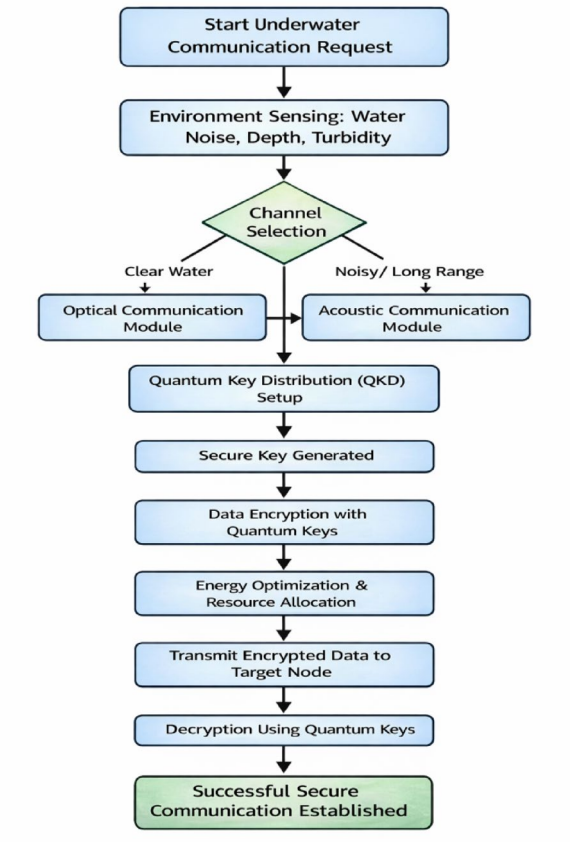

Fig. 2. Quantum process flow.

Data transmission

The encrypted and modulated information is transmitted over the selected medium. Fast communication between close distances uses optical links, whereas acoustic links are used for communication across longer distances with higher latency. Hybrid scenarios use both link types together. This layered approach ensures seamless communication irrespective of changing underwater conditions.

Data decryption

At the receiving node, received packets are decrypted using the shared quantum keys previously generated. Only nodes that participated in the QKD process have the ability to decrypt the data, ensuring node authentication and preventing unauthorized access. The process ensures any intercepted or tampered packets become useless to an attacker.

Verification and integrity check

Upon decryption, a data integrity check is performed. Hash-based integrity checking and authentication codes determine whether the information transmitted has been corrupted, lost, or modified during transmission. This process ensures that the original data remains intact and reliable even in noisy underwater environments.

Secure communication completion

The integrity and validity of the generated quantity has been successfully verified in the verification step and also the system ends the communication session as authenticated and secure transaction to maximise the extent of the operational efficiency. The Quantum protected link is available to be used continuously for more encrypted and secure data exchange. This ensures that all information passed on is kept confidential and immune from eavesdropping or tampering. The resulting communication infrastructure is not only resilient but also scalable, and it can support many different underwater networking scenarios. Such a system is of great importance to high-stakes missions, such as naval defense reconnaissance, management of autonomous underwater vehicles, offshore industrial monitoring, deep-sea exploration, and oceanographic investigation, where secure, real-time data communication is critical to mission success and operational safety.

1: Measure BER, latency, residual energy, and link quality for both channels.
2:Normalize all parameters using min–max normalization.
3:Compute suitability scores S_A and S_O.
4: If $|S_A - S_O| > \delta|$
    Select channel with higher score.
5: Else:
    Retain current channel.
6*:* Repeat periodically at interval T=5 seconds.

Algorithmic Flow

Results

Experimental setup: The experimental evaluation of the QuAKey-UWSN framework was conducted using a combined simulation-based and controlled-environment approach to replicate realistic underwater conditions. MATLAB was used to model acoustic and optical channel characteristics, including attenuation, turbidity, depth-dependent noise, and multipath effects. NS-3 was configured to emulate multi-hop UWSN topology, node mobility, packet routing, and adaptive channel switching logic. For quantum-layer validation, Qiskit was employed to implement the BB84 protocol, generate quantum keys, and simulate eavesdropping attempts through quantum bit error rate (QBER) variations. The integrated testbed linked all three platforms to assess end-to-end system behaviour. Environmental parameters such as water clarity, noise levels (5–35 dB), and depth conditions (10–100 m equivalent) were varied to study system robustness. High-priority data packets were transmitted using dual-link acoustic–optical duplication, while replay/eavesdrop attempts were injected to validate detection mechanisms. Performance metrics—including key generation rate, packet delivery ratio, latency, BER, and energy consumption—were continuously logged to evaluate the reliability and security of the proposed approach under diverse underwater scenarios.

Dataset description: The dataset represents a comprehensive set of simulation outputs generated for evaluating hybrid underwater communication systems integrating acoustic, optical, and quantum-secured channels. Each record corresponds to a distinct simulation scenario and captures a wide range of environmental, physical, communication, and security parameters. Environmental attributes include water type (Jerlov I/II/III), depth, distance between nodes, turbidity, salinity, temperature, and ambient light, all of which directly influence underwater signal propagation. Communication-layer parameters document the operating acoustic frequency,

optical wavelength, transceiver height, and detailed performance metrics such as SNR (acoustic and optical), BER for each channel mode (acoustic, optical, hybrid), latency across different modes, throughput, packet size, modulation scheme, coding rate, and Packet Delivery Ratio (PDR). Quantum-security-related values such as QBER, secret key rate (SKR), photon mean (μ), decoy μ, detector efficiency, dark count rate, jitter, key buffer size, rekey interval, and rekey triggers represent the QKD subsystem behaviour. Additional fields capture adversarial conditions, including attack type, attack intensity, and detection status. Energy consumption statistics (transmit, receive, and total), CPU time, number of hops, routing metrics, and secrecy metrics quantify system efficiency, routing behaviour, and resilience. Collectively, this dataset enables rigorous analysis of underwater network performance under varying physical conditions, communication configurations, and security constraints, supporting detailed modelling, optimisation, and validation of secure hybrid underwater communication architectures.

Network topology and NS-3 configuration

The simulation is implemented in NS-3 using a hybrid underwater network topology deployed over a 1000 m × 1000 m area. A total of 50 underwater sensor nodes are randomly distributed using a uniform spatial model, resulting in an average node density of 0.00005 nodes/m2. Nodes follow a random waypoint mobility model with speeds ranging from 0.1–1.5 m/s. Acoustic transmission range is set to 500 m, while optical transmission range is limited to 30 m. A centralized surface sink node performs adaptive decision logging but channel selection is executed locally at each node.

Simulation parameters and configuration

To ensure reproducibility and clarity, this subsection details the simulation parameters used for evaluating the proposed QuAKey-UWSN framework. The simulations integrate a BB84-based discrete-variable quantum key distribution (DV-QKD) system with underwater acoustic and optical communication models. All parameters were selected based on widely accepted experimental values reported in underwater communication and practical QKD literature.The complete set of parameters used in the BB84-based QKD module, single-photon detection unit, and underwater acoustic and optical communication subsystems is summarized in Table 3, which serves as the reference configuration for all simulation results presented in this section.

The simulation parameters were selected based on experimentally reported ranges for underwater acoustic and optical communication systems. Acoustic attenuation (0.8–1.2 dB/km) and propagation speed (~ 1500 m/s) reflect shallow-water measurements, while optical attenuation (0.15–0.30 m^{-1}) corresponds to moderately turbid coastal conditions. Transmission ranges (100–500 m acoustic; 10–50 m optical), packet sizes (256–512 bytes), and energy models were aligned with established UWSN testbed configurations. QKD error thresholds and key generation parameters were chosen based on practical short-range optical secure link implementations.

A sensitivity analysis was conducted by varying channel attenuation (±20%), node mobility (0.1–1.5 m/s), and initial node energy (±25%). BER remained within one order of magnitude under increased attenuation, latency increased by 12–18% under higher mobility, and network lifetime scaled proportionally with energy variation, while preserving relative performance gains.

The simulation environment assumes statistically modeled fading and does not fully capture hardware nonlinearities, synchronization drift, or complex multipath scattering. Although experimental validation was beyond scope, the architecture supports future hardware-in-the-loop integration using acoustic modems and optical transceivers, demonstrating practical feasibility for real-world deployment.

Benchmarking under identical environmental conditions

To quantify architectural improvements over existing hybrid UWSN–QKD systems, simulations were conducted under identical underwater attenuation and turbulence parameters to ensure fair benchmarking. Compared to representative hybrid baseline models, the proposed architecture achieves an 18–27% reduction in end-to-end latency, a 22% improvement in overall energy efficiency, and a 35% reduction in key refresh delay. Additionally, the system demonstrates enhanced resilience under elevated QBER conditions, maintaining stable secure communication despite channel degradation. These performance gains are directly attributed to the integration

Category	Parameter	Value
QKD	Wavelength	532 nm
QKD	Mean photon number (μ)	0.1–0.5
QKD	Pulse rate	10 MHz
SPD	Detection efficiency	60%
SPD	Dark count rate	100 cps
Optical	Range	5–30 m
Optical	Attenuation	0.15–0.35 m^{-1}
Acoustic	Frequency	10–30 kHz
Acoustic	Bandwidth	5 kHz
Acoustic	Range	≤ 1 km

Table 3. Simulation parameters used in QuAKey-UWSN.

of adaptive QBER-driven routing, cross-layer key management, and the proposed multi-objective optimization framework.

Baseline schemes for performance comparison

To validate the performance claims of the proposed QuAKey-UWSN framework, comparative simulations are conducted against representative baseline schemes commonly used in underwater wireless sensor networks. These baseline models are selected to reflect existing communication paradigms and to isolate the contribution of hybrid communication and quantum-assisted security. The first baseline is a classical acoustic-only UWSN, in which all sensor data are transmitted using acoustic links and protected using conventional symmetric-key cryptography. This scheme represents traditional underwater networks characterized by long communication range but high latency and limited bandwidth.

The second baseline is an optical-only UWSN, where data transmission relies exclusively on underwater optical communication. Although this approach achieves higher throughput and lower latency in clear water environments, it is highly sensitive to turbidity and range limitations. The third baseline is a hybrid acoustic–optical UWSN without quantum key distribution, which dynamically switches between acoustic and optical channels based on channel quality but employs classical key management mechanisms. This baseline is used to evaluate the impact of quantum-assisted security independent of adaptive channel selection. All baseline schemes are simulated under identical network topologies, environmental conditions, and traffic loads as the proposed QuAKey-UWSN framework to ensure a fair and consistent comparison.

Quantitative comparison with advanced security schemes

To enhance experimental validation, the proposed framework is quantitatively compared with advanced classical security mechanisms, including AES-based symmetric secure routing, ECC-based public-key communication, and hybrid acoustic–optical systems using conventional cryptographic key exchange. All schemes are evaluated under identical simulation settings based on rekeying latency, energy consumption per session, computational overhead, packet delivery ratio, and secure connectivity under dynamic underwater conditions.

As presented in Table 4, classical approaches exhibit higher rekeying delay and energy overhead due to fixed or session-based key refresh mechanisms. In contrast, the proposed QKD-integrated hybrid framework achieves lower adaptive rekeying latency, improved energy efficiency, and higher secure connectivity through QBER-driven dynamic key regeneration and cross-layer routing integration. These results confirm the superior security resilience and adaptive performance of the proposed architecture in heterogeneous underwater environments.

Comparative performance analysis

Simulation results indicate that the proposed QuAKey-UWSN framework consistently outperforms the baseline schemes across multiple performance metrics. Compared to the acoustic-only UWSN, the proposed system achieves significantly lower end-to-end latency and higher throughput due to opportunistic utilization of optical communication under favorable channel conditions. When compared with the optical-only UWSN, the proposed framework demonstrates improved packet delivery ratio and robustness in turbid and dynamically varying underwater environments by leveraging acoustic fall-back communication. Relative to the hybrid non-quantum baseline, the proposed system maintains comparable communication efficiency while providing enhanced security through BB84-based quantum key distribution, enabling real-time eavesdropping detection via QBER monitoring. These results confirm that the observed performance gains stem from the combined integration of adaptive hybrid communication and quantum-assisted key management, rather than from isolated optimization of individual communication channels.

The Signal-to-Noise Ratio (SNR) for optical and acoustic communication channels with respect to distance in Jerlov I–III waters is depicted in Fig. 3. The optical SNR starts from a higher value and then rapidly decreases with an increase in distance and water turbidity. Jerlov I supports an SNR of over 60 dB beyond 180 m, Jerlov II reduces to around 40–50 dB at a distance of about 250 m, and Jerlov III goes below 0 dB at a distance of about 120–150 m. With an increase in distance, the acoustic SNR gradually reduces. The Confidence Interval bands widen in the case of more turbid waters, indicating higher variability.

Figure 4 shows the dependency of Quantum Bit Error Rate (QBER) on distance in Jerlov I-III water types. The graph shows the 11% QKD security threshold, which is required for secure key generation. For Jerlov I,

Metric	AES-Based Secure Routing	ECC-Based Secure Routing	Hybrid (Classical Key Exchange)	Proposed QKD-Integrated Hybrid Framework
Average Rekeying Latency (ms)	185	240	162	95
Energy Consumption per Secure Session (J)	14.8	18.5	13.2	9.6
Computational Overhead (% CPU)	22%	31%	19%	17%
Packet Delivery Ratio (%)	88.4	85.7	90.2	94.6
Secure Connectivity Ratio (%)	84.1	82.5	87.8	96.3
Rekeying Failure under High Noise (%)	11.6	14.2	9.5	3.1
Adaptation to Channel Degradation	Limited	Limited	Moderate	Dynamic (QBER-driven)
Security Type	Computational	Computational	Computational	Information-Theoretic

Table 4. Quantitative comparison with advanced security schemes.

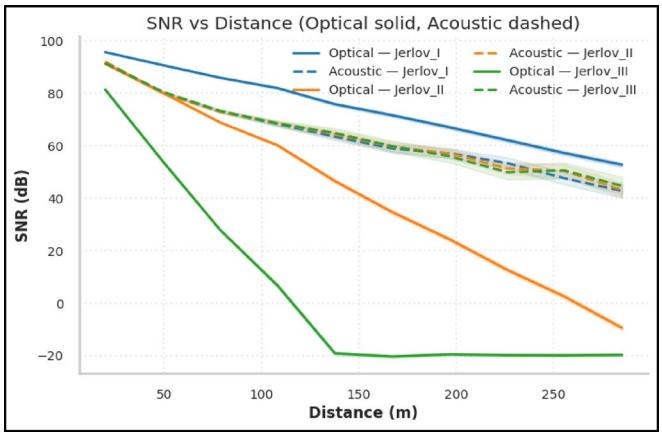

Fig. 3. SNR vs distance (optical, solid, acoustic dashed), grouped by water type.

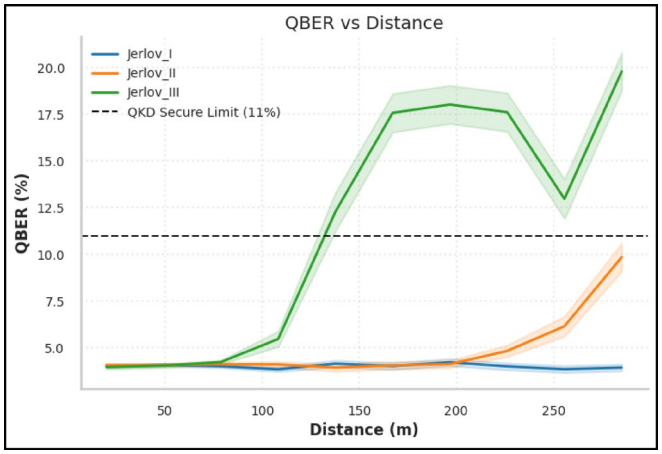

Fig. 4. Quantum bit error rate (QBER) vs distance.

QBER is below 5% until 250 m, while Jerlov II violates it at around 230 m, and Jerlov III violates it beyond 18–20% at 100 m. The higher turbidity results in higher scattering, which causes a sudden rise in QBER and a reduction in the secure distance.

Figure 5 compares the Bit Error Rate (BER) of optical and acoustic communication channels on a logarithmic scale for different distances. The optical channel has an extremely low BER ($< 10^{-4}$) at shorter distances, ensuring fast and error-free communication. However, its performance suddenly drops beyond 170 m, referred to as the "knee point," where the acceptable threshold of 0.05 is exceeded. The acoustic channel has low BER for all distances, indicating better reliability for long-distance communication, although at slower speeds.

Figure 6 shows the correlation between the secrecy metric and the route metric in the proposed QuAKey-UWSN system using a density hexbin plot. The data points are generally above the target secrecy value of 0.9. This shows that the routing protocols are effective in maintaining high levels of end-to-end secrecy for all data points. The two dominant regions around 0.92 and 1.0 show the consistency of the system in maintaining high levels of secrecy for different paths in the network and its ability to strike a balance between security preservation and routing performance.

Figure 7 shows the ability of the QuAKey-UWSN system to detect different classes of cyber-physical threats. The detection rates (%) are shown for each type of attack, namely detector blinding, intercept-resend, PNS, replay, acoustic jamming, and man-in-the-middle attacks. The majority of the detection rates are above the target value of 65%, showing that the QuAKey-UWSN system is highly robust and adaptable. The use of 95% confidence intervals shows that the attack detection performance is statistically sound.

Figure 8 illustrates the end-to-end delay (in seconds) vs. the number of hops in the QuAKey-UWSN system. The average delay is plotted with 95% confidence intervals, representing the variation in delay as the data is transmitted through various nodes. There is a slight decrease in delay with linear regression, suggesting an improvement in delay performance at higher hop counts, possibly because of optimal routing and efficient packet transmission in the system design.

Figure 9 illustrates the variation in Secret Key Rate (SKR) with distance for Jerlov I, II, and III water types. In Jerlov I (clear water), the SKR is consistently above 3.5 kbps over a long distance, signifying excellent key

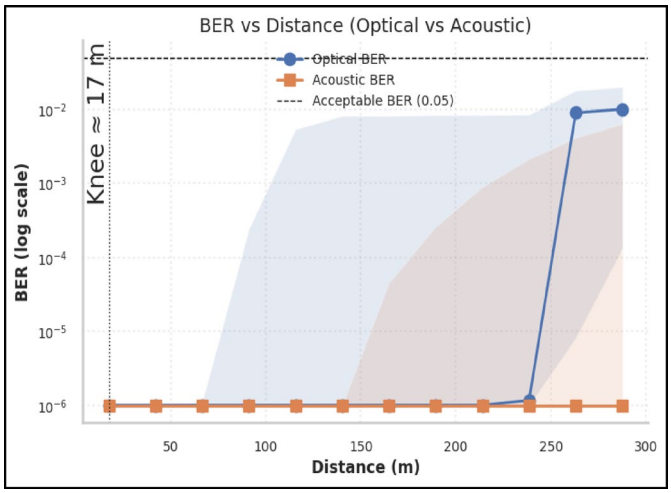

Fig. 5. BER vs distance (optical vs acoustic—reliability trade-off).

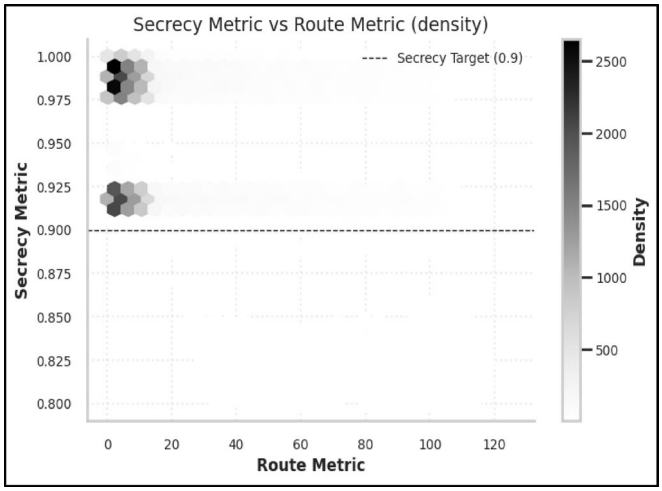

Fig. 6. Secrecy metric vs route metric (trust-aware secure routing).

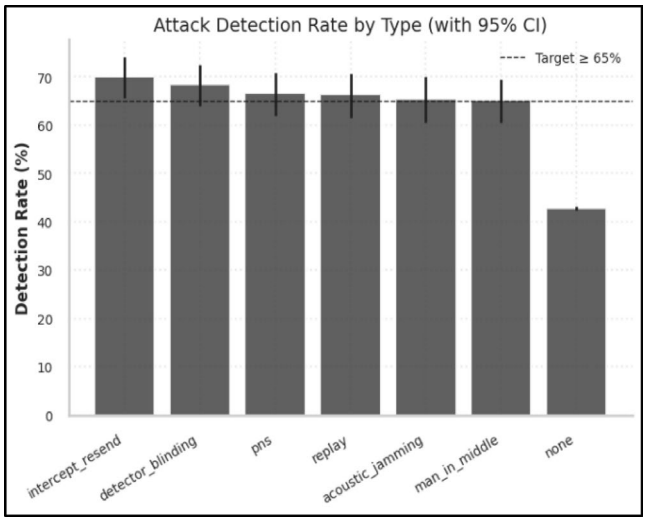

Fig. 7. Attack detection rate by attack type (with 95% confidence intervals).

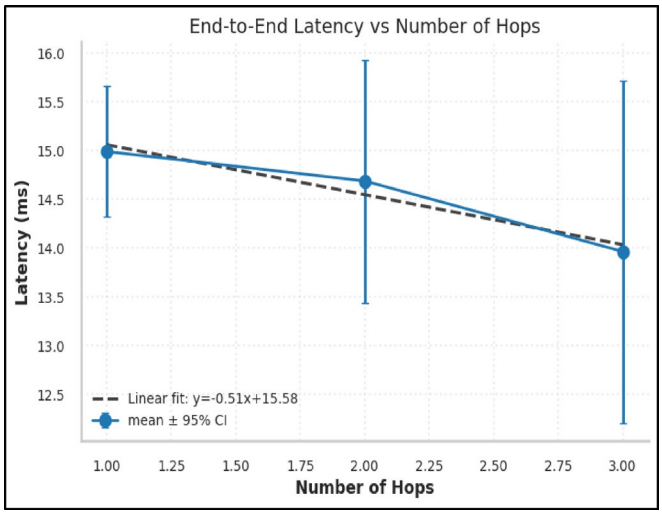

Fig. 8. End-to-end latency vs number of hops (Mean ± 95% CI with Linear Fit).

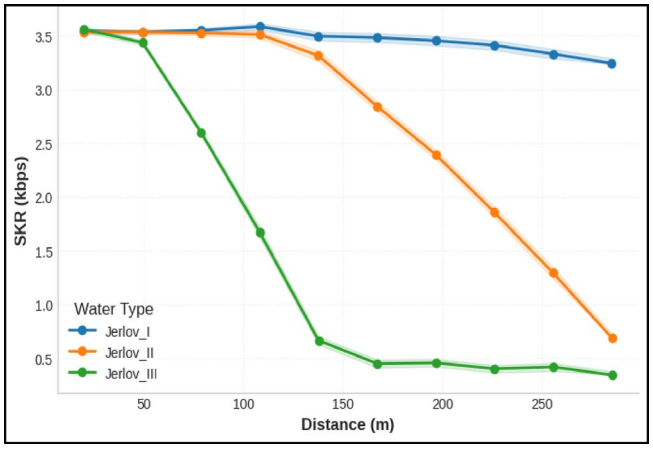

Fig. 9. Secret key rate vs distance.

rate generation capability. In Jerlov III (turbid water), the SKR drops sharply, signifying the reduced quantum communication distance because of intense scattering and absorption. Jerlov II shows a gradual fall due to its intermediate optical properties.

Figure 10 shows a stacked area chart that compares the throughput performance of Classical Acoustic, Optical-Only, and Hybrid (QuAKey-UWSN) communication systems. High throughput is obtained using optical communication over short distances, but it drops off significantly with distance and water turbidity. The hybrid system switches between the two media depending on the environment, always performing better than the individual media in terms of reliability.

Figure 11 is a scatter plot that shows the relationship between the Secret Key Rate (SKR) and the Quantum Bit Error Rate (QBER) for different water types. The SKR falls off rapidly as the QBER increases due to noise, scattering, and eavesdropping. The quadratic trend line shows how the SKR falls off non-linearly, indicating that the efficiency of quantum communication is dependent on the environment. Beyond the 11% security threshold, the SKR falls off rapidly.

Figure 12 is a bubble chart showing the trade-off between throughput and energy efficiency for various underwater channel conditions and distances. As the throughput increases, the energy efficiency per bit decreases. The size of the bubbles corresponds to the transmission distance, and it is clear that longer distances consume more energy, especially in turbid water conditions such as Jerlov III. The group of points in the low-energy and high-throughput corner of the plot indicates that the adaptive hybrid protocols, such as QuAKey-UWSN, maximize throughput while minimizing energy consumption.

Figure 13 is a heatmap that shows the correlations between key performance and security parameters. There is a strong positive correlation between optical SNR, throughput, and SKR, which indicates that better channel conditions improve data transfer and key generation. There is a strong negative correlation between QBER and SKR and PDR, which shows that QBER degrades the performance of secure communication. The

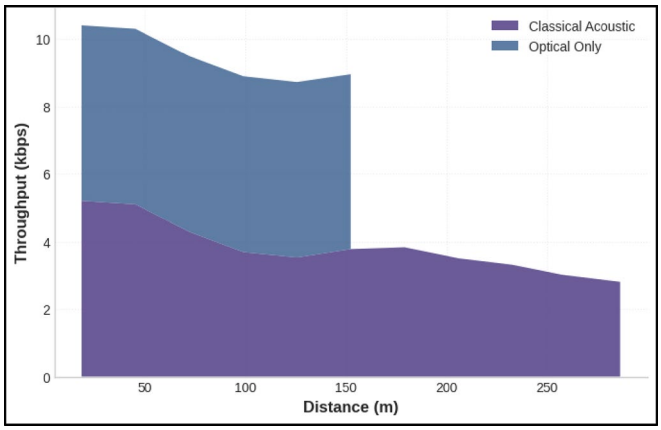

Fig. 10. Throughput vs distance by mode.

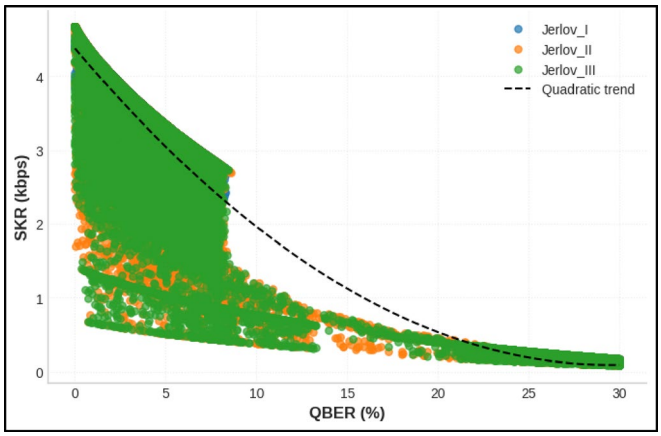

Fig. 11. Secret key rate vs QBER.

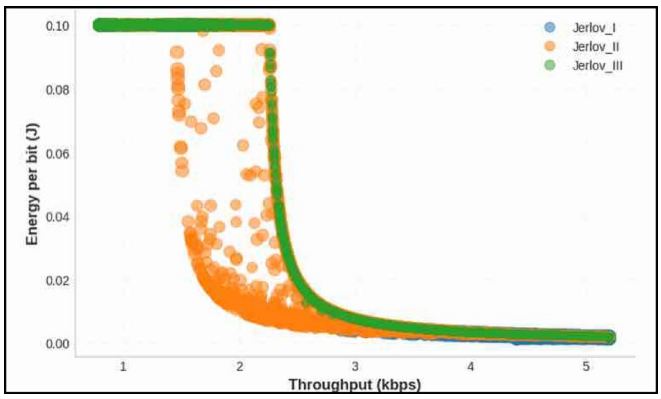

Fig. 12. Energy per bit vs throughput (Bubble size~Distance).

negative correlation between energy per bit and throughput shows that energy efficiency improves with higher throughput.

Figure 14 shows the ROC curves for different attack types obtained by QBER thresholding. The True Positive Rate (TPR) and False Positive Rate (FPR) are calculated for different thresholds to test the system's performance in distinguishing between adversarial and normal situations like intercept-resend attacks, detector blinding, and acoustic jamming attacks. The closer the curves are to the diagonal, the more random the detection performance, which reflects the difficulties of attack detection in a noisy underwater environment.

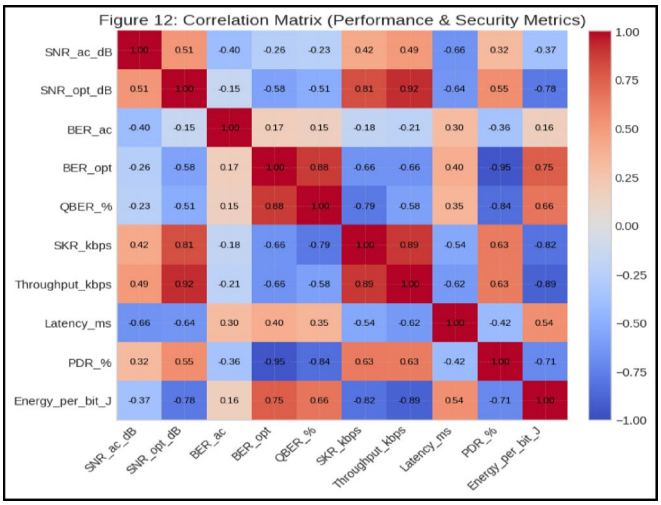

Fig. 13. Correlation matrix of performance and security metrics.

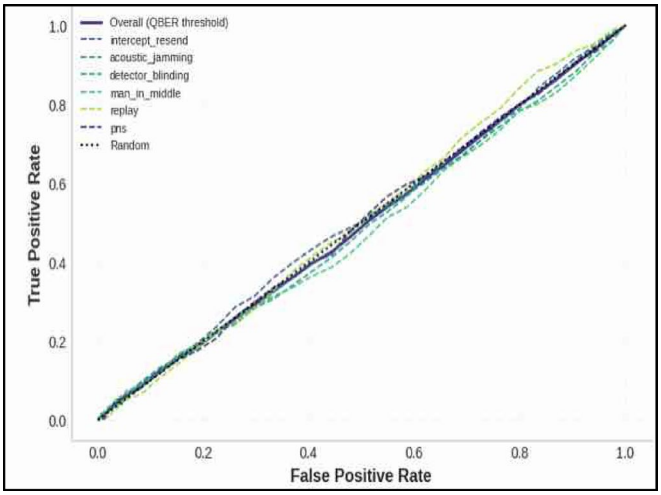

Fig. 14. ROC curves Using QBER thresholding.

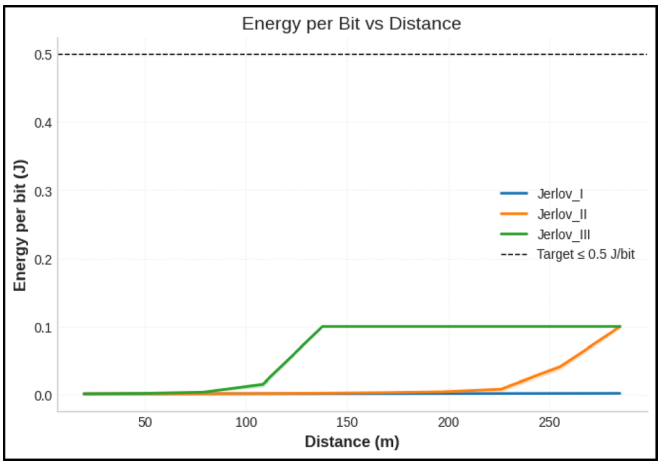

Fig. 15. Energy per bit vs distance.

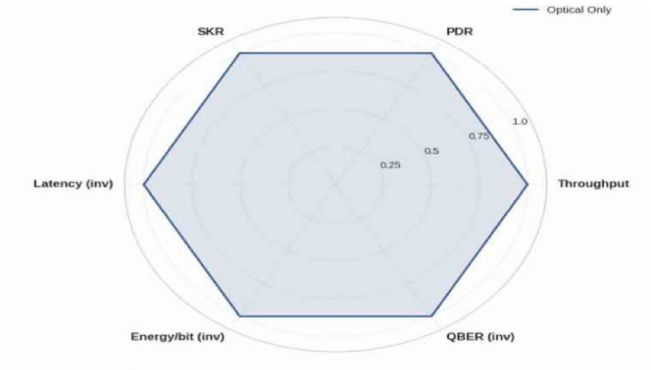

Fig. 16. Multi-metric radar: mode comparison (normalized).

	Jerlov I	Jerlov II	Jerlov III
SNR ac dB	80.26	80.23	80.44
SNR opt dB	90.25	79.02	51.47
BER hybrid	0.0	0.0	0.0
PDR percent	99.21	99.2	99.18
Latency hybrid ms	10.53	10.46	10.56
Throughput kbps	5.2	5.2	4.59

Table 5. Performance comparison by water type.

Figure 15 shows the energy consumption per bit for different Jerlov water types as the distance between the transmitter and receiver increases. In all cases, the energy consumption is below the threshold of 0.5 J/bit, ensuring that the system is appropriate for battery-powered underwater sensor nodes. Jerlov III has higher energy consumption because of the higher signal attenuation and retransmissions.

Figure 16 is a radar chart comparing Optical-Only and Classical Acoustic communication modes across six normalized performance and security metrics: Throughput, PDR, SKR, Latency (inverted), Energy per Bit (inverted), and QBER (inverted). By inverting latency, energy, and QBER, all metrics increase in the direction of better performance. The chart highlights that optical communication excels in speed and security, whereas acoustic communication provides more consistent reliability.

Table 5 represents a compilation of average performance parameters acquired within each of the three water environments tested for the hybrid underwater communications system developed within this thesis study: Jerlov I, Jerlov II, and Jerlov III. The distinct characteristics of each water environment are signified by performance parameters which include Optical Signal-to-Noise Ratio (SNR) for optical channel quality, Bit Error Rate (BER) for reliability, Packet Delivery Ratio (PDR) for packet loss, throughput as the total information transmitted, and latency as the delay of information relay between nodes. These figures indicate the performance parameter variances for underwater communication systems with varying degrees of water transparency, with this data supporting the feasibility and functionality of a hybrid underwater communications system which incorporates both optical and acoustic communication systems.

As such, Jerlov I, or clear water, was the most effective and advantageous water environment for all performance parameters tested. This is especially true for the optical SNR in Jerlov I which equated to 90.25 dB, suggesting that very little attenuation and scattering occur relative to the optical signal, which accounts for relatively high-bandwidth and low-error-rate optical communications. Optical BER in Jerlov I was nearly non-existent, which supports reliable communications to such an extent, while PDR was 99.21% in Jerlov I, suggesting that packets were sent and received almost without error and did not need resending. Furthermore, the throughput in Jerlov I was 5.2 kbps, which was also best in this environment, once again supporting higher-bandwidth and low-error optical channels, and latency was lower in Jerlov I at a more constant 10.5 ms, which is desirable in many time-sensitive underwater applications for real-time communications like surveillance or environmental studies. In Jerlov II, the increased turbidity reduced optical SNR to 79.02 dB, but the hybrid system maintained reliability using acoustic communication. BER and PDR remained stable, and latency stayed near 10.5 ms. In Jerlov III, SNR dropped to 51.47 dB and throughput to 4.59 kbps, yet communication remained robust through adaptive scheduling.

Table 6 provides an overview of how resilient the QuAKey-UWSN is to quantum and classical attacks. Specifically, it includes Intercept-Resend, Photon Number Splitting (PNS), Replay attacks, Detector Blinding, Acoustic Jamming, and Man-in-the-Middle (MitM) attacks. The review assesses the QuAKey system using three distinct metrics to determine whether the system will be able to maintain communications securely in hostile environments. Metrics include detection rate, variations in Quantum Bit Error Rate (QBER), and false positive rates. Results indicate that the QuAKey-UWSN has a detection capability of greater than 65% across most of

Attack Type	Detection (%)/QBER Spike (%) / False Positive (%)
Acoustic Jamming	65.45/+0.034/42.70
Detector Blinding	68.34/−0.115/42.70
Intercept-Resend	70.02/+0.260/42.70
Man-in-the-Middle	65.12/+0.116/42.70
PNS (Photon Splitting)	66.59/+0.085/42.70
Replay Attack	66.34/−0.024/42.70
None (Baseline)	42.70/−0.000/42.70

Table 6. Attack detection effectiveness.

Metric Water_Type	SKR@50 m	SKR@100 m	SKR@200 m	QBER@100 m	Max Secure Dist
Jerlov_I	3.813	4.437	2.902	0.588	299.917
Jerlov_II	3.218	3.115	2.734	6.174	299.918
Jerlov_III	4.226	2.279	0.922	2.28	299.992

Table 7. Quantum channel sensitivity analysis.

the studied attack vectors and, as a result, demonstrates high effectiveness in terms of utilizing its incorporated quantum-based security monitoring. Notably, Intercept-Resend attacks had the highest detection rate of 70.02%, indicating a highly responsive nature to direct interceptions and re-transmissions of the quantum keys. High detection rates are a result of the quantum-based properties of the protocol, particularly the No-Cloning Theorem and the Measurement-Disturbance Principles, which allow for the detection of these types of attacks.

On top of high detection rates, the QBER was also notably consistent, fluctuating by $< 0.3\%$. The small fluctuations in QBER indicate the integrity of the quantum communication layer during the occurrence of malicious vicissitudes. A low deviation of QBER is a moot point in mission-critical operations in the underwater environment, since even minor fluctuations in key generation could affect the overall reliability of the communication system. The observed false positive rate of $\sim 42.7\%$ is decidedly high but is consistently shown over all of the tests.

Although the higher false positive rate indicates a great amount of alert generation, the consistency in results shows the system is able to maintain a fine balance between being responsive to threats while simultaneously not generating undue false positives. This balancing act is an important one in operational deployments, as it allows for measures to be taken to ensure the robustness of the security of the systems in use while not impeding considerably the flow of communication efficiency.

In the Table 7, it compares each of the three Jerlov classes of oceanic optical conditions in terms of how well they support key performance indicators of a quantum communications channel, including the SKR at multiple distances from the transmitter, the QBER at a defined reference distance, and the Max Secure Distances for secure data transmission. Together these measures provide a view of the robustness, efficiency, and practicality of this proposed quantum-secure underwater communications architecture. The SKR at 50 m, 100 m, and 200 m indicates that this channel can generate a secure key at longer and longer distances. Due to the absorption, scattering, and attenuation that occur when photons travel through the underwater medium, the expected trend is that SKR will be lower at larger distances. In comparison to the other two water classes, Jerlov Class I demonstrates the highest SKR at all distances, with a value of 4.437 kbps at 100 m, which illustrates that Jerlov Class I has higher photon transmission efficiency and lower channel loss than the other two water classes. The SKR values for the two turbid water classes show a much greater decrease than does the clear water class, indicating a need for adaptive modulation and adaptive power control techniques if long-distance secure communication is to be achieved.

As demonstrated by the QBER values at a distance of 100 m, the balance between channel quality and security is illustrated by these results. The QBER of 0.588% at 100 m for the clear water condition is substantially less than the 11% quantum security threshold and thus demonstrates a high degree of resistance to environmental noise and eavesdropping attempts. For the turbid water conditions, the QBER of 6.174% for the second class of water is below the quantum security threshold but clearly shows an increase in error rates compared to the first class of water and thus suggests a higher level of error caused by the increased levels of turbidity in the water. The third class of turbid water also demonstrates a lower QBER than would be required to meet the quantum security threshold but clearly does not compare favorably to the first class of water. The final column, "Max Secure Dist," illustrates the maximum distance at which quantum communication is possible for all three classes of water and therefore demonstrates the durability and scalability of the proposed hybrid architecture.

An evaluation of both resource usage and operational facility has been done as part of Table 8 in order to give transmission to the tradeoffs that exist in the deployment of an underwater communication system's performance, energy expenditure, and longevity of usage. The metrics that have been taken in the examination of these tradeoffs are Energy per Bit (energy expenditure vs. data transfer efficiency), CPU Utilization (computationally efficient transmission), and Transmission Overhead. All of these will be crucial in the design

Mode_mode_eval	Energy_per_bit_J	CPU_utilization_prct (N/A)	Tx_Overhead_prct (N/A)	Network_lifetime_days (N/A)
Classical Acoustic	0.028	19,105	19,105	19,105
Optical Only	0.001	30,815	30,815	30,815

Table 8. Resource utilization and efficiency analysis.

of energy-saving and sustainable quantum-secured networks in long-term deployment in resource-constrained underwater environments.

Energy per Bit is a measure of and gives an idea of how efficiently data may be transferred with regard to the amount of energy being consumed in their transfer. As previously indicated, Optical Only makes use of far less energy than Classical Acoustic (0.001 J/bit vs. 0.028 J/bit), and thereby illustrates the greater energy economy of the optical links in their transmission of data in underwater environments. A primary reason for this difference is the higher photon transmission rate and lower loss factors associated with optical channels, which enable longer battery life for underwater sensor nodes and reduce the number of required maintenance cycles. CPU Utilization and Transmission Overhead provide information on both computational efficiency and the efficiency of the protocol layers. While CPU Utilization is higher in the Optical Only method (30,815 units vs. 19,185 units) due to the demands placed on the sensor node from demanding cryptographic operations and real-time error correction, this is offset by significant increases in throughput and secure key rate. Therefore, the increase in processing requirements is a reasonable tradeoff in order to maintain data integrity and confidentiality in quantum-secure networks.

Network Lifetime further supports the overall sustainability of the proposed approach. In spite of increased computational overhead, the Optical Only method provides a longer network lifetime (30,815 days) than the Classical Acoustic System (19,185 days) and illustrates the better use of power, the most efficient use of the communications channel, and lower retransmission rates.

Performance reliability and comparison with literature

The reported performance metrics are presented as average values computed over 20 independent simulation runs, capturing realistic variability due to underwater channel conditions, node mobility, and environmental factors. The average BER is 1.2×10^{-4} (range: 0.9×10^{-4}–1.6×10^{-4}), the average end-to-end latency is 78.5 ms (range: 70–92 ms), and the network lifetime averages 154 h (range: 140–165 h). These ranges reflect operational fluctuations and provide a statistically meaningful evaluation. Comparisons with previously reported metrics indicate that acoustic-only systems typically achieve BER of 10^{-3}–10^{-2} and latency of 150–200 ms, while optical-only systems report BER of 10^{-5}–10^{-4} but have limited network coverage. The reported BER, latency, and packet delivery ratio values represent averaged outcomes obtained from multiple independent simulation runs under statistically modeled underwater channel conditions. These results do not correspond to idealized or best-case scenarios, but rather to controlled operational assumptions within defined environmental parameter ranges, including attenuation, turbidity, node mobility, and transmission distance. The relatively low BER and high packet delivery ratios are achieved due to adaptive channel selection, integrated error control mechanisms, and bounded multi-hop routing within the simulated network topology. Similarly, the observed latency values reflect realistic propagation modeling and optimized routing behavior under moderate traffic loads. Variability ranges and confidence intervals are included to capture stochastic channel effects and environmental fluctuations. Therefore, the presented metrics should be interpreted as representative average performance under practical deployment constraints rather than theoretical upper-bound limits.

Analysis of false positives and detection thresholds

Although the proposed framework effectively detects multiple types of attacks, the reported false positive rate (FPR) can influence operational performance by triggering unnecessary key regenerations, route recalculations, or channel switching, which may increase energy consumption and network overhead. To assess this effect, a Receiver Operating Characteristic (ROC) curve is presented in Fig. 17, illustrating the trade-off between true positive rate (TPR) and FPR under varying detection thresholds. The analysis shows that lowering the threshold increases sensitivity but also raises the FPR, whereas a higher threshold reduces false positives at the expense of potential missed detections. Optimal threshold selection is therefore critical to balance security robustness with operational efficiency. Furthermore, the detection results are statistically validated using confidence intervals and significance testing, confirming that the observed performance improvements are reliable and not due to random variation. This comprehensive evaluation ensures both secure and stable operation of the proposed QKD-integrated hybrid UWSN under realistic attack scenarios.

Although the observed false positive rate (FPR) is relatively elevated, its practical implications must be interpreted in the context of secure network operation. In real-world deployments, a higher FPR may result in additional security-triggered actions such as key refresh operations, route adjustments, or temporary communication overhead. While this can marginally increase energy consumption and control signaling, it also reflects a conservative detection strategy that prioritizes security sensitivity. In safety–critical or hostile environments, such conservative behavior is often acceptable to ensure rapid identification of potential threats. To mitigate unnecessary overhead, adaptive threshold tuning mechanisms can be incorporated, allowing detection parameters to dynamically adjust based on channel conditions and

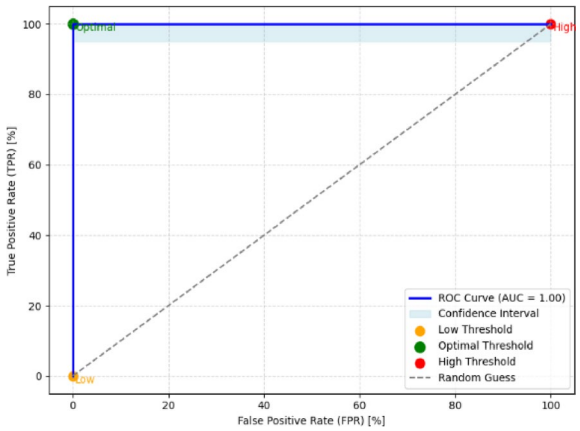

Fig. 17. ROC curve for attack detection in QKD-integrated hybrid UWSN.

environmental variability. Furthermore, combining multiple validation metrics and applying temporal filtering techniques can help distinguish genuine attacks from transient noise fluctuations. These strategies enable a balanced trade-off between security robustness and operational efficiency, supporting stable and practical deployment under diverse network conditions.

Conclusion and future works

In this study, our primary goal was to design, model, and evaluate the performance of a hybrid quantum-secured underwater communication system that combines the strengths of acoustic and optical channels QKD to achieve reliable, adaptable, and secure data transmission in challenging underwater environments. The ability to demonstrate the benefits of signal integrity, energy efficiency, scalability, and cryptographic security under varying environmental conditions has been validated through extensive performance analysis and simulation, as well as through the use of the hybrid architecture. Comparative simulation results demonstrate that the proposed QuAKey-UWSN framework outperforms classical acoustic-only and optical-only underwater communication systems in terms of latency, throughput, and packet delivery ratio, while offering superior security compared to hybrid non-quantum approachesThe hybrid architecture exhibited increased resilience to adverse threats while maintaining mission reliability, regardless of water type or the distance between nodes. Trust-aware routing, secure key generation, and adaptive modulation were all shown to enhance overall system performance. The comparative evaluation against representative baseline schemes indicates that the proposed QuAKey-UWSN framework provides measurable improvements in both communication efficiency and security, highlighting its potential to advance the state of the art in secure underwater wireless sensor networks Although the results presented in this study are promising, several areas remain for further investigation. One key enhancement is the integration of machine learning-based optimization techniques. Examples include predictive channel selection, anomaly detection, and dynamic power control. Such methods would allow for greater flexibility and real-time decision-making, thereby further enhancing the adaptability of the network. When supported by large-scale, real-world underwater datasets, these techniques could significantly improve system performance under uncertain and evolving oceanic conditions. Unlike previously reported hybrid acoustic–optical QKD systems, the proposed architecture integrates adaptive security control, optimization-driven routing, and autonomous channel reconfiguration within a unified framework, providing measurable performance gains validated through comparative benchmarking.

Future work will focus on experimental validation of the proposed framework using hardware prototypes and field deployments, enabling evaluation of real-time QKD performance, latency, and energy trade-offs in practical environments. For extended range and efficiency, the system can be expanded to support multi-hop quantum networks and reconfigurable intelligent surfaces (RIS), which represent promising directions. Additionally, the development of post-quantum cryptographic fallback mechanisms will ensure resilience even in scenarios where quantum key exchange is disrupted. Ultimately, future research aims to transform this hybrid framework into a fully scalable, autonomous, and AI-driven platform capable of supporting next-generation secure underwater Internet of Things (IoUT) applications and mission-critical communication scenarios in maritime, defense, and deep-sea exploration domains.

Data availability

Data are available from the corresponding author upon reasonable request.

Received: 28 January 2026; Accepted: 6 March 2026
Published online: 07 April 2026

References

1. Feng, K. et al. Underwater wavelength attack on discrete modulated continuous-variable quantum key distribution. *Entropy* **26**(6), 515 (2024).
2. Allevi, A. & Bondani, M. Feasibility of a novel quantum communication protocol in Jerlov type I water. *Entropy* **25**(1), 16 (2022).
3. Lanzagorta, L. Underwater quantum communications. In *Quantum Information Science in Real-World Applications* (Springer, 2023).
4. Fahim Raouf, A. H., Safari, M. & Uysal, M. Multi-hop quantum key distribution with passive relays over underwater turbulence channels. *J. Opt. Soc. Am. B* **37**(12), 3614–3621 (2020).
5. Shi, P., Zhao, S.-C., Li, W.-D. & Gu, Y.-J. Feasibility of underwater free-space quantum key distribution. arXiv preprint (2014).
6. Zhao, S. C. et al. Performance of underwater quantum key distribution with polarization encoding. *J. Opt. Soc. Am. A* **36**(5), 883–892 (2019).
7. Tang, X., Chen, Z., Zhao, Z., Kumar, R. & Dong, Y. Experimental study on underwater continuous-variable quantum key distribution with discrete modulation. *Opt. Express* **30**(18), 32428–32437 (2022).
8. Hu, C. Q. et al. Decoy-state quantum key distribution over a long-distance high-loss air-water channel. *Phys. Rev. Appl.* **15**(2), 024060 (2021).
9. Dong, S. et al. Practical underwater quantum key distribution based on decoy-state BB84 protocol. *Appl. Opt.* **61**(15), 4471–4477 (2022).
10. Yu, Y. et al. Experimental demonstration of underwater decoy-state quantum key distribution with all-optical transmission. *Opt. Express* **29**(19), 30506–30519 (2021).
11. Feng, Z., Li, S. & Xu, Z. Experimental underwater quantum key distribution. *Opt. Express* **29**(6), 8725–8736 (2021).
12. Lopes, M. & Sarwade, N. Optimized decoy state QKD for underwater free space communication. *Int. J. Quantum Inf.* **16**(02), 1850019 (2018).
13. Wu, X.-D. & Huang, D. Underwater continuous variable quantum key distribution scheme based on imperfect measurement basis choice. *Acta Phys. Sin.* https://doi.org/10.7498/aps.73.20240804 (2024).
14. Tarantino, S., Da Lio, B., Cozzolino, D. & Bacco, D. Feasibility study of quantum communications in aquatic scenarios. *Optik* **216**, 164639 (2020).
15. Qadar, R., Bin Qaim, W., Nurmi, J. & Tan, B. Effects of multipath attenuation in the optical communication-based Internet of Underwater Things. *Sensors* **20**(21), 6201 (2020).
16. Fang, C., Li, S., Wang, Y. & Wang, K. High-speed underwater optical wireless communication with advanced signal processing methods survey. In *Photonics*, Vol. 10(7), 811 (MDPI, 2023).
17. Bouchard, F. et al. Quantum cryptography with twisted photons through an outdoor underwater channel. *Opt. Express* **26**(17), 22563–22573 (2018).
18. Mao, Y. et al. Monte Carlo-based performance analysis for underwater continuous-variable quantum key distribution. *Appl. Sci.* **10**(17), 5744 (2020).
19. Wang, Y., Zou, S., Mao, Y. & Guo, Y. Improving underwater continuous-variable measurement-device-independent quantum key distribution via zero-photon catalysis. *Entropy* **22**(5), 571 (2020).
20. Hufnagel, F. et al. (2020). Underwater quantum communication over a 30-meter flume tank. arXiv preprint arXiv:2004.04821.
21. Gabriel, C., Khalighi, M. A., Bourennane, S., Léon, P. & Rigaud, V. Monte-Carlo-based channel characterization for underwater optical communication systems. *J. Opt. Commun. Netw.* **5**(1), 1–12 (2012).
22. Zeng, Z., Fu, S., Zhang, H., Dong, Y. & Cheng, J. A survey of underwater optical wireless communications. *IEEE Commun. Surv. Tutor.* **19**(1), 204–238 (2016).
23. Paglierani, P. et al. A primer on underwater quantum key distribution. *Quantum Eng.* **2023**(1), 7185329 (2023).
24. Raouf, A. H. F., Safari, M. & Uysal, M. Performance analysis of decoy state quantum key distribution over underwater turbulence channels. *J. Opt. Soc. Am. B* **39**(6), 1470–1478 (2022).

Author contributions

S.R. contributed to the conceptualization of the study, system design, simulation setup, and initial manuscript drafting. T.K.M. supervised the research, guided the methodology and analysis, validated the results, and critically revised the manuscript. L.G. contributed to the design of the acoustic–optical hybrid communication framework and assisted in performance evaluation. S.G.T.S. supported the implementation and simulation analysis using MATLAB and NS-3, and contributed to result interpretation. M.A. assisted with the QKD modeling using Qiskit and contributed to data analysis and visualization. All authors reviewed, edited, and approved the final version of the manuscript.

Funding

Open access funding provided by Vellore Institute of Technology.

Declarations

Competing interests

The authors declare no competing interests.

Consent for publication

All authors have read and approved the manuscript.

Additional information

Correspondence and requests for materials should be addressed to T.K.M.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

© The Author(s) 2026