cryptography

MDPI

Article

An Energy-Aware Post-Quantum Ascon–ML-KEM Cryptographic Framework for Low-Latency UAV Remote Sensing Communications

Nedal Y. Al-Tamimi [1], Mahmoud AlJamal [2], Mohammad Q. Al-Jamal [3,*], Ayoub Alsarhan [4,5], Sami Aziz Alshammari [6,*], Nayef H. Alshammari [7], Khalid Hamad Alnafisah [8] and Mohammed Kamel Aleinzi [9]

1 Department of Artificial Intelligence, Science and Information Technology, Irbid National University, Irbid 21110, Jordan; n.tamimi@inu.edu.jo
2 Department of Cybersecurity, Science and Information Technology Faculty, Irbid National University, Irbid 21110, Jordan; m.aljamal@inu.edu.jo
3 Department of Renewable Energy, Technical Faculty, Jadara University, P.O. Box 733, Irbid 21110, Jordan
4 Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Al-Ahliyya Amman University, Amman 19111, Jordan; a.alsarhan@ammanu.edu.jo or ayoubm@hu.edu.jo
5 Department of Information Technology, Faculty of Prince Al-Hussien bin Abdullah, The Hashemite University, Zarqa 13133, Jordan
6 Department of Information Technology, Faculty of Computing and Information Technology, Northern Border University, Rafha 73213, Saudi Arabia
7 Department of Computer Science, Faculty of Computers and Information Technology, University of Tabuk, Tabuk 47512, Saudi Arabia; nh.alshammari@ut.edu.sa
8 Department of Computer Sciences, Faculty of Computing and Information Technology, Northern Border University, Rafha 73213, Saudi Arabia; khalid.alnafisah@nbu.edu.sa
9 Department of Information Systems, Faculty of Computing and Information Technology, Northern Border University, Rafha 73213, Saudi Arabia; mohammed.aleinzi@nbu.edu.sa
* Correspondence: m.aljamal@jadara.edu.jo (M.Q.A.-J.); sami.alshammari@nbu.edu.sa (S.A.A.)

Abstract

UAV-based remote sensing systems are increasingly deployed in smart surveillance, disaster response, environmental monitoring, and critical infrastructure inspection. In these applications, aerial sensing platforms must transmit telemetry, control commands, and observation data securely and reliably under strict latency, energy, and computational constraints. However, existing security approaches often fail to jointly provide lightweight payload confidentiality, quantum-resilient key establishment, and adaptive communication protection suitable for dynamic and resource-constrained aerial sensing environments. To address this challenge, this paper proposes an energy-aware post-quantum hybrid cryptographic framework for secure and low-latency UAV remote sensing communications in UAV–IoT mission networks. The proposed framework integrates Ascon-based authenticated encryption for low-overhead protection of remote sensing payloads and mission telemetry, ML-KEM-based post-quantum session-key establishment for long-term resilience against quantum-era threats, and an AI-driven adaptive rekeying mechanism that dynamically adjusts key-refresh decisions according to threat level, residual energy, mobility state, channel stability, anomaly density, traffic sensitivity, link type, and mission progression. Accordingly, rekeying is treated not as a static maintenance process but as an intelligent and context-aware cryptographic control function that adapts communication security to evolving mission and sensing conditions. The framework is evaluated across twenty progressively demanding scenarios involving different UAV counts, sensor densities, payload sizes, communication modes, and adversarial settings relevant to real-time remote sensing operations. Experimental results demonstrate a secure delivery rate of 99.2%, attack detection and mitigation effectiveness of 98.9%, end-to-end encryption latency

Check for updates

Academic Editor: Josef Pieprzyk

Received: 1 May 2026
Revised: 11 June 2026
Accepted: 12 June 2026
Published: 16 June 2026

Correction Statement: This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

of 8.7 ms, throughput of 5.03 Mbps, energy overhead of 11.6 mJ/session, rekeying overhead of 2.9 mJ/event, session resilience of 96.4%, and integrity verification success of 99.1%. These findings show that the proposed framework provides a practical and scalable contribution to post-quantum secure UAV remote sensing by unifying lightweight authenticated encryption, ML-KEM-based quantum-resilient key establishment, and AI-driven adaptive rekeying within a resilient aerial–terrestrial communication architecture.

Keywords: post-quantum cryptography; ML-KEM; Ascon authenticated encryption; adaptive rekeying; UAV remote sensing communications

1. Introduction

Unmanned Aerial Vehicle (UAV) systems have become increasingly important platforms for modern remote sensing applications, as flexible sensing geometry, rapid deployment, and high spatio-temporal coverage enable efficient observation of dynamic environments [1]. In particular, UAV-enabled remote sensing is now widely used in smart surveillance, environmental monitoring, precision agriculture, disaster response, border observation, battlefield reconnaissance, and critical infrastructure inspection, where timely acquisition and reliable transmission of sensing data are essential for effective decision-making [2]. In these scenarios, UAVs do not operate merely as isolated airborne sensors; rather, they function as intelligent mobile nodes within broader aerial–terrestrial sensing ecosystems that include distributed IoT devices, peer UAVs, edge gateways, and command-and-control stations [3]. Recent studies on UAV-based integrated sensing and communication have further emphasized that future aerial sensing systems must jointly optimize sensing reliability, communication latency, energy efficiency, and security under dynamic wireless conditions [4,5]. This integration supports persistent observation, cooperative sensing, rapid data collection, and adaptive mission execution across geographically dispersed and operationally dynamic environments. However, the effectiveness of such UAV-based remote sensing systems depends not only on sensing capability but also on the ability to communicate telemetry, control commands, and acquired observation data securely, reliably, and with low latency over dynamic wireless links. This challenge is intensified by mobility-driven topology variation, intermittent connectivity, heterogeneous device constraints, fluctuating channel quality, and limited onboard energy and computational resources [6].

Although secure communication is fundamental to trustworthy UAV remote sensing, existing security approaches remain insufficient for many real-world aerial sensing missions [7]. Conventional cryptographic methods can provide strong confidentiality and authentication, but they are often designed for relatively stable environments with less constrained resource budgets, which reduces their practicality for lightweight UAV platforms and constrained field sensing devices [8]. Their computational overhead, memory demand, key-management complexity, and communication delay may directly affect mission continuity, especially in real-time remote sensing settings that require fast control exchange, continuous telemetry delivery, and prompt transmission of sensing outputs [9]. This concern is consistent with recent IoT–edge security studies showing that constrained devices require lightweight cryptography, efficient authentication, and low-overhead communication protection because conventional public-key and heavyweight symmetric configurations can impose excessive processing and energy costs [10]. Conversely, lightweight security mechanisms are usually optimized for efficiency, yet many of them do not adequately address long-term cryptographic resilience, adaptive protection, or cross-layer

communication awareness [11]. This limitation is increasingly important because UAV remote sensing missions often generate telemetry records, sensing streams, and mission archives whose confidentiality and integrity may remain important far beyond immediate mission completion, thereby raising concerns about future quantum-enabled attacks and harvest-now-decrypt-later adversarial models [12]. The recent standardization of ML-KEM as a module lattice-based key-encapsulation mechanism and the growing integration of post-quantum key exchange into low-latency communication protocols further indicate the need to move beyond classical key-establishment mechanisms in mission-critical wireless and IoT systems [13–15]. In addition, many existing frameworks still depend on static rekeying schedules, rigid protection policies, or isolated protocol-layer mechanisms, which are poorly matched to aerial sensing environments in which threat conditions, residual energy, mobility state, channel instability, traffic sensitivity, and anomaly behavior may change continuously during mission execution. Recent work on IoT key provisioning and lightweight post-quantum edge communication also highlights that key establishment and key updating must be treated as operationally adaptive processes rather than one-time initialization tasks [16,17]. As a result, current approaches often fail to achieve the balance required for secure remote sensing communications—namely, lightweight authenticated protection, post-quantum key establishment, context-aware adaptation, and low-latency data continuity—within a unified framework.

To address these challenges, this paper proposes an energy-aware post-quantum hybrid cryptographic architecture for secure and low-latency UAV remote sensing communications in UAV–IoT mission environments. The proposed framework is designed to protect not only communication links in general but also the reliable exchange of remote sensing payloads, telemetry streams, mission commands, and sensing-related control information across UAV-to-sensor, UAV-to-UAV, and UAV-to-ground interactions. Its novelty lies in treating payload encryption, session-key establishment, and key refresh as tightly coupled components of an adaptive cross-layer cryptographic protection strategy rather than as isolated security functions. Specifically, the framework integrates three complementary mechanisms. First, it adopts Ascon-based authenticated encryption to provide lightweight confidentiality, integrity, and authenticity for remote sensing payloads and mission telemetry with low computational and memory overhead, making it suitable for resource-constrained aerial and field sensing nodes. This choice is aligned with the recent NIST Ascon-based lightweight cryptography standard for constrained devices and with implementation-oriented studies showing that Ascon is suitable for efficient authenticated encryption in embedded and IoT environments [18,19]. Second, it incorporates ML-KEM-based post-quantum key establishment to protect session-key exchange against future quantum threats and strengthen the long-term security of remotely sensed data and mission communications. Third, it introduces an AI-driven adaptive rekeying engine that continuously interprets operational context, including threat level, residual energy, mobility state, channel stability, anomaly density, mission priority, traffic sensitivity, link type, and session progression, to determine whether communication should continue normally, undergo lightweight rekeying, trigger immediate key refresh, or enforce stronger protective action under elevated risk. In this way, rekeying is transformed from a static maintenance operation into an intelligent and context-aware cryptographic control function for dynamic remote sensing missions.

The significance of this work extends beyond proposing a secure communication mechanism alone. It establishes a unified operational framework that supports trustworthy UAV remote sensing by combining lightweight authenticated encryption, post-quantum session security, and adaptive risk-aware control within a single aerial–terrestrial communication architecture. This is particularly important because UAV remote sensing missions

depend on the timely and authenticated transfer of sensed observations, control messages, and mission-state information across heterogeneous links with different latency, exposure, and reliability characteristics. A fixed one-size-fits-all protection policy is therefore rarely sufficient. To validate the practicality and robustness of the proposed design, this study adopts a structured evaluation campaign comprising twenty progressively demanding scenarios spanning different UAV counts, sensor densities, payload sizes, communication modes, threat regimes, and adaptive-threshold settings. The results show that the proposed framework achieves strong secure-delivery performance, high attack detection and mitigation effectiveness, low end-to-end encryption latency, modest energy and rekeying overhead, and resilient session continuity under dynamic and adversarial operating conditions. These findings indicate that the proposed architecture provides a practical, scalable, and mission-adaptive contribution for secure UAV-based remote sensing systems operating under resource constraints, mobility-driven instability, and evolving quantum-era threat landscapes.

The main contributions of this study are summarized as follows:

- We propose a novel, energy-aware post-quantum hybrid cryptographic architecture for UAV remote sensing communications that unifies lightweight Ascon authenticated encryption, ML-KEM post-quantum key establishment, and cross-layer protection for aerial–terrestrial sensing missions.
- We introduce an AI-driven adaptive rekeying mechanism that dynamically adjusts key-refresh decisions according to threat conditions, residual energy, mobility dynamics, anomaly behavior, and communication-state variation instead of relying on fixed static schedules.
- We present a comprehensive 20-scenario validation framework demonstrating that the proposed design achieves strong, secure delivery; low latency; low energy and rekeying overhead; and resilient communication performance under increasingly demanding UAV remote sensing mission conditions.

2. Literature Review

The literature related to secure UAV–IoT remote sensing communication can be organized around five interconnected research directions: secure, low-latency communication; post-quantum key establishment; lightweight, authenticated encryption; adaptive rekeying and energy-aware decision-making; and hardware-assisted cryptographic deployment. These directions collectively show that future UAV communication systems cannot rely on isolated cryptographic primitives or static protection policies. Instead, they require integrated security designs that jointly consider mobility, latency, energy consumption, link instability, mission sensitivity, and long-term cryptographic resilience. In this context, Martal'o et al. [20] emphasized the need for cross-layer secure and low-latency communication in next-generation IoT systems, while Banerjee [21], Zhaxygulova et al. [22], and Sarkar et al. [23] highlighted the importance of lightweight cryptography, authentication, privacy preservation, and resource-aware protection in IoT-enabled UAV and drone networks. These studies agree that conventional heavyweight cryptographic schemes may impose excessive processing delay, memory demand, and energy cost on constrained aerial platforms. However, they generally remain broad, survey-oriented, or focused on conventional UAV security, and they do not provide a unified post-quantum, low-latency, and AI-adaptive cryptographic architecture for UAV-to-ground, UAV-to-UAV, and UAV-to-sensor communication links.

A second important research stream focuses on post-quantum cryptography for UAV, wireless, and IoT communication systems. Hafeez et al. [24] proposed a quantum-resilient threat-modeling framework for RIS-assisted UAV corridors by integrating ML-KEM, Fal-

con authentication, secure ISAC scheduling, and RIS-coded scene verification. Their work shows that quantum-era risks, including harvest-now-decrypt-later attacks and post-quantum control-signaling threats, must be considered in future aerial communication systems. Similarly, Aissaoui et al. [25] evaluated post-quantum key-exchange mechanisms such as CRYSTALS-Kyber, BIKE, and HQC on constrained UAV-class hardware, demonstrating that lattice-based key establishment can be feasible under limited computational and memory resources. Khan et al. [26] further reviewed the role of PQC in future-proofing UAV security, whereas Hoque et al. [27] analyzed the performance of NIST-selected post-quantum mechanisms in 5G-and-beyond wireless environments. Collectively, these studies demonstrate that ML-KEM/Kyber-based key establishment is a promising candidate for latency-sensitive and resource-constrained communication systems. Nevertheless, most existing PQC-oriented works focus on feasibility analysis, threat modeling, or protocol-level benchmarking rather than on integrating ML-KEM with lightweight payload encryption, UAV remote sensing traffic, energy-aware operation, and adaptive rekeying within a single mission-driven architecture.

Lightweight authenticated encryption represents another essential requirement for UAV remote sensing, where telemetry, control commands, and sensing payloads must be protected without exhausting onboard resources. Existing IoT and UAV security studies show that lightweight AEAD mechanisms are attractive because they jointly provide confidentiality, integrity, and authenticity with a lower computational burden than conventional heavyweight configurations. In this direction, Mahdi et al. [28] combined Kyber-512 with ASCON for secure IoT communication and demonstrated the practicality of pairing lattice-based key establishment with lightweight authenticated encryption. This line of work is closely related to the present study because it supports the use of hybrid post-quantum and lightweight symmetric protection for constrained systems. However, prior hybrid Kyber–ASCON studies are generally not tailored to UAV remote sensing missions; do not evaluate heterogeneous UAV-to-ground, UAV-to-UAV, and UAV-to-sensor communication modes; and do not consider mission-aware rekeying decisions driven by residual energy, mobility state, channel stability, traffic sensitivity, anomaly density, and threat level.

Adaptive rekeying and energy-aware decision-making have also been investigated but usually outside a unified post-quantum UAV remote sensing framework. Rakshit et al. [29] showed that dynamic session-key rekeying can improve IoT–edge communication security compared with static pre-shared-key approaches, particularly by reducing key reuse and improving session freshness. Mondal et al. [30] addressed energy-aware UAV operation from a routing perspective by proposing a risk-aware and energy-constrained UAV–UGV cooperative routing framework using attention-guided deep reinforcement learning. Although these works highlight the importance of adaptive decisions and energy-aware operation, their objectives differ from secure UAV–IoT cryptographic communication. Existing rekeying studies often remain oriented toward a symmetric key and do not incorporate post-quantum key establishment, while energy-aware UAV studies mainly focus on routing, endurance, or recharging coordination rather than encrypted data exchange, authenticated telemetry protection, or context-sensitive cryptographic control. This leaves an important gap for a framework in which rekeying is not only periodic or static but dynamically controlled by mission context, channel quality, energy availability, and adversarial pressure.

Hardware-assisted acceleration of post-quantum cryptography is also relevant to practical deployment because UAV platforms are constrained by size, weight, power, memory, and real-time responsiveness. Zhang et al. [31] investigated FPGA-oriented acceleration of the number theoretic transform, a core computational component of Kyber/ML-KEM, and showed that optimized polynomial arithmetic can reduce execution overhead. Di

Matteo et al. [32] presented KEM-22 as an ASIC-based ML-KEM accelerator, while Xing and Li [33] proposed a compact FPGA implementation of CCA-secure CRYSTALS-KYBER. These works demonstrate that hardware acceleration can support faster and more efficient post-quantum operations, which may be valuable for UAV systems requiring frequent key establishment or rekeying. However, such studies primarily address cryptographic implementation efficiency at the hardware level and do not evaluate the system-level interaction between post-quantum key establishment, lightweight authenticated encryption, adaptive rekeying, secure delivery, latency, throughput, energy overhead, integrity verification, and session resilience in UAV–IoT mission environments.

The reviewed literature confirms substantial progress in secure, low-latency communication; UAV and drone security; post-quantum key establishment; lightweight authenticated encryption; adaptive rekeying; energy-aware operation; and cryptographic hardware acceleration. However, these contributions are still largely fragmented. Existing approaches usually address one or two aspects of the problem, such as PQC benchmarking, lightweight encryption, UAV routing, IoT rekeying, or hardware acceleration, without integrating them into a unified communication framework for UAV remote sensing. In particular, there remains a clear need for a mission-aware architecture that combines Ascon-based authenticated encryption, ML-KEM-based post-quantum session establishment, AI-driven adaptive rekeying, energy-aware policy control, and multi-link UAV–IoT communication evaluation. The proposed framework addresses this gap by unifying these components within an aerial–terrestrial UAV–IoT security architecture and by evaluating their combined effect on secure delivery, attack detection and mitigation, encryption latency, throughput, energy overhead, rekeying cost, integrity verification, and session resilience across progressively demanding mission scenarios.

3. Methodology

The proposed system was formulated as a mission-critical aerial–terrestrial communication architecture in which unmanned aerial vehicles operate as mobile cyber-physical nodes that simultaneously sense, relay, aggregate, and disseminate data across a heterogeneous IoT field composed of UAV-mounted sensing and communication modules, distributed ground sensors, edge gateways, and a ground control station, all interconnected through dynamic wireless channels characterized by intermittent connectivity, topological variation, bandwidth fluctuation, and strict onboard resource limitations. Within this environment, three communication strata are fundamental to mission continuity: UAV-to-sensor links for data acquisition from constrained field devices; UAV-to-UAV links for cooperative coordination and distributed situational awareness; and UAV-to-ground links for telemetry, command dissemination, mission-state reporting, and decision feedback. Unlike static communication settings, the considered mission space is highly dynamic, since node mobility, energy depletion, link-quality variation, and operational urgency directly influence the security requirements of each transmission path. Consequently, the system model is designed not merely to protect isolated packets but also to secure an evolving communication fabric in which confidentiality, integrity, authenticity, low-latency delivery, and resilient session continuity must be jointly maintained under severe energy and computational constraints.

Correspondingly, the threat model assumes an adversary with broad network-level access and advanced strategic capabilities that is able to observe, intercept, replay, modify, inject, jam, and delay traffic over any exposed UAV–IoT communication segment. The main vulnerability surfaces considered in this model include exposed wireless links, mobility-driven handover periods, constrained onboard computation, limited residual energy, session-key reuse, delayed rekeying, packet-level integrity exposure, and long-term

confidentiality risks associated with stored telemetry and mission logs. At a classical level, the attacker may conduct passive traffic surveillance for sensitive telemetry extraction; active man-in-the-middle manipulation during session establishment; replay-based disruption of mission logic; selective packet tampering targeting command integrity; session-key compromise attempts intended to weaken forward communication secrecy; and jamming-induced degradation of channel stability, packet delivery, throughput, and latency. Beyond these conventional threats, the model also considers a more powerful future-oriented adversary possessing quantum-enabled cryptanalytic capabilities that could render traditional public-key key-establishment mechanisms insecure over long mission lifetimes, particularly in scenarios involving telemetry archives, delayed decryption, and persistent command logs.

Threat severity was assessed according to the expected impact on confidentiality, integrity, availability, session continuity, and mission safety. Passive eavesdropping and delayed packets were treated as medium-to high-severity threats depending on traffic sensitivity; replay, packet modification, man-in-the-middle manipulation, and session-key compromise were treated as high-severity threats; and quantum harvest-now-decrypt-later exposure, persistent jamming, physical capture, and side-channel leakage were treated as critical deployment-level risks. Physical capture and side-channel attacks were included in the threat analysis because direct access to a UAV or sensor node may expose stored secrets, timing behavior, or implementation-dependent leakage. However, these attacks were not modeled as full hardware-level tamper or side-channel experiments in the present simulation. Instead, their operational consequences were represented through elevated-risk session states, key-compromise attempts, forced rekeying events, integrity-failure cases, abnormal latency or energy behavior, and reduced session-resilience conditions.

Figure 1 presents the complete system architecture and threat model of the proposed UAV–IoT security architecture, in which the mission communication space is structured around three tightly coupled interaction domains: UAV-to-ground control exchange, UAV-to-UAV swarm coordination, and UAV-to-sensor/actuator field interaction. In the upper layer, the Ground Control Station, Mission Control Server, and Edge Gateway form the command-and-control backbone that disseminates mission commands and receives telemetry through protected aerial links, while the UAV swarm operates as a distributed mobile communication fabric bridging the infrastructure layer with geographically dispersed IoT sensor clusters and field actuators. The central block, denoted as the cross-layer Hybrid Secure Telemetry and Command Core, captures the main novelty of the framework by integrating Ascon-authenticated telemetry encryption for lightweight, low-latency payload protection; ML-KEM-based post-quantum session key establishment for quantum-resilient secret exchange; an AI-driven adaptive rekeying engine for context-sensitive key refresh; and a threat-scoring and context-awareness unit that continuously interprets operational factors such as residual UAV energy, mobility state, channel instability, packet anomaly density, traffic sensitivity, mission priority, and observed attack intensity. This design is explicitly cross-layer because the security logic is not confined to a single protocol stage; instead, it spans the physical/edge execution layer, the network communication layer, the application/telemetry layer, and the mission layer, thereby enabling encryption-policy selection and session orchestration to react to both communication-state variation and mission-critical urgency. The figure also clearly separates classical and quantum-era threat surfaces. On the left side, conventional adversarial actions, including eavesdropping, replay injection, man-in-the-middle interception, control-message manipulation, and key-compromise attempts, target exposed UAV links and low-level aerial communications. On the right side, more advanced quantum-era risks, including harvest-now-decrypt-later exposure, quantum-assisted key recovery, future public-key break risk, long-term telemetry-

archive compromise, and session hijacking, emphasize the inadequacy of relying solely on traditional public-key protection in long-lifecycle mission environments. The locked communication paths drawn across aerial, sensor, and infrastructure links visually indicate that the proposed framework protects not only payload confidentiality but also session continuity, message authenticity, and trust-preserving command delivery.

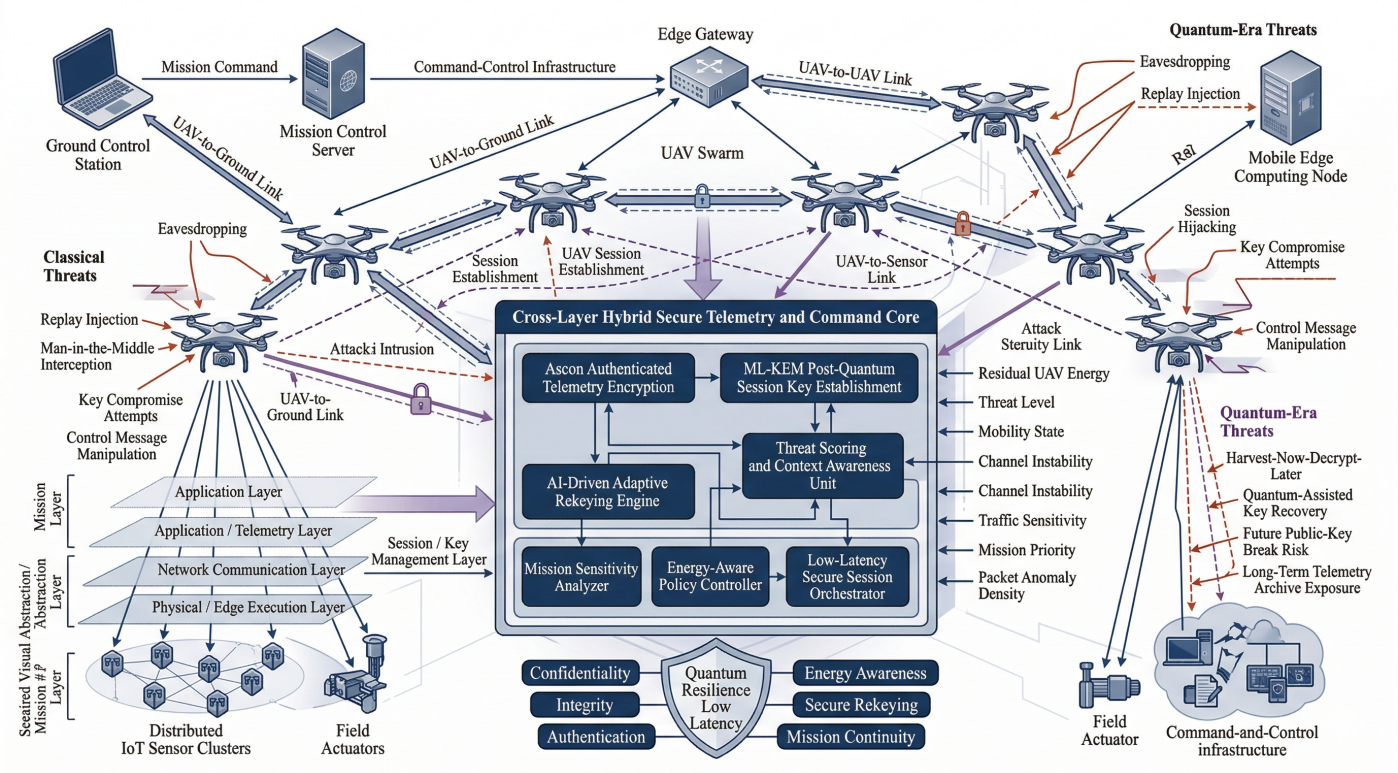


Figure 1. Proposed methodology.

3.1. Generated Cryptographic Benchmarking Dataset

The generated cryptographic benchmarking dataset was constructed as a scenario-driven experimental dataset specifically designed to support the evaluation of the proposed energy-aware post-quantum Ascon–ML-KEM secure communication framework for UAV remote sensing communications. The dataset was generated through a custom Python 3.11.5-based cryptographic simulation and benchmarking procedure rather than being collected from an intrusion-detection or public attack-traffic dataset because the main objective of this study is to evaluate encryption, post-quantum key establishment, adaptive rekeying, authenticated delivery, and secure-session continuity. It should be noted that the generated dataset is based on a controlled Python-based simulation rather than real UAV hardware, a physical radio testbed, or field deployment. Accordingly, the reported latency, throughput, energy-overhead, and rekeying-overhead values should be interpreted as simulation-level comparative indicators, not direct hardware measurements. The simulator adopts simplified assumptions, including an idealized channel abstraction and the exclusion of hardware interrupt latency, cache effects, memory-bus contention, operating-system scheduling jitter, transceiver startup delay, and nonlinear battery-discharge behavior. The generation process began by defining twenty mission-oriented UAV–IoT communication scenarios, each representing different combinations of UAV count, sensor density, payload size, communication link type, threat level, and adaptive rekeying thresholds. For each scenario, the simulator generated protected UAV communication events across UAV-to-ground, UAV-to-UAV, and UAV-to-sensor links. Each event was assigned realistic mission and communication attributes, including mission zone, environmental condition, weather

condition, UAV model, sensor type, altitude, speed, communication distance, residual energy, CPU load, memory usage, RSSI, SNR, packet loss rate, available bandwidth, queue delay, mission phase, and traffic type. These variables were not inserted as fixed constants; instead, they were generated with controlled variation according to the scenario severity, link type, payload size, environmental condition, and threat level, allowing the dataset to represent dynamic and heterogeneous UAV remote sensing communication conditions.

The dataset-generation workflow was organized as a structured sequence consisting of scenario definition, communication-event generation, mission-context assignment, cryptographic-state simulation, adaptive risk scoring, validation-event injection, and metric recording. In each scenario, the same generation logic was applied to the proposed framework and all comparative baselines so that differences in the reported results reflect the cryptographic design and rekeying policy rather than inconsistent data-generation conditions. The simulation inputs included the scenario identifier, UAV count, sensor density, communication link type, payload size range, threat level, residual energy state, channel-quality indicators, and rekeying thresholds. The simulation outputs included cryptographic success flags, authentication-verification status, rekeying decision, latency, throughput, energy overhead, secure-delivery status, integrity-success flag, and session-resilience score. This organization makes the dataset suitable for repeated evaluation because the main performance metrics can be recomputed from event-level records rather than being inferred only from aggregated summary values.

After generating the mission and communication context, each record was passed through a simulated secure-session workflow that emulates the proposed hybrid cryptographic framework. The ML-KEM layer was represented through session-key establishment and refresh attributes, including the selected ML-KEM parameter set, encapsulation status, decapsulation status, shared-secret matching, and session-key refresh state. The Ascon-authenticated encryption layer was represented through encryption and decryption status, nonce counter, associated-data binding, authentication-tag verification, plaintext hash, ciphertext hash, authentication-tag value, and associated-data hash. Full plaintext payloads were intentionally not stored in the released dataset; instead, hash-based representations were used to preserve confidentiality while still documenting payload uniqueness, ciphertext generation, and integrity-verification behavior. The adaptive rekeying mechanism was generated by computing a contextual risk score from operational variables such as threat level, residual energy, mobility state, channel stability, anomaly density, mission priority, traffic sensitivity, session age, packet loss, and link condition. This risk score was then compared with soft, immediate, and critical rekeying thresholds to determine whether the secure session should continue normally, perform soft rekeying, trigger immediate key refresh, or suspend sensitive traffic. Cryptographic validation events such as replay attempts, ciphertext modification, invalid authentication tags, delayed packets, and high-risk contextual states were injected to test how the framework responds to integrity failures and elevated-risk sessions. The final dataset contains 120,000 records and 83 attributes, where each row represents one protected UAV–IoT communication event and records its context, cryptographic state, adaptive rekeying decision, validation outcome, latency, throughput, energy overhead, rekeying overhead, secure-delivery status, integrity-success flag, and session-resilience score. Table 1 also supports reproducibility by identifying the input variables, intermediate cryptographic states, decision outputs, validation indicators, and final performance metrics used throughout the simulation workflow. Table 1 summarizes the main feature groups included in the generated cryptographic benchmarking dataset and explains how each group supports the evaluation of the proposed Ascon–ML-KEM adaptive secure communication framework.

Table 1. Feature groups of the generated UAV–IoT Ascon–ML-KEM cryptographic benchmarking dataset.

Feature Group	Representative Attributes	Purpose in the Dataset
Scenario and mission descriptors	`scenario_id`, `mission_id`, `mission_zone`, `mission_phase`, `environment_condition`, `weather_condition`	Define the operational context of each UAV remote sensing scenario and distinguish different mission conditions under which the secure communication framework is evaluated.
Network topology and node configuration	`uav_count`, `sensor_count`, `source_node`, `destination_node`, `link_type`, `sensor_type`, `uav_model`	Represent the UAV–IoT communication structure, including UAV-to-ground, UAV-to-UAV, and UAV-to-sensor communication paths.
Mobility and physical operating conditions	`altitude_m`, `speed_mps`, `distance_to_destination_m`, `source_latitude`, `source_longitude`, `destination_latitude`, `destination_longitude`	Capture realistic UAV movement and spatial communication conditions that influence link quality, latency, and secure-session stability.
Communication-channel indicators	`rssi_dbm`, `snr_db`, `packet_loss_rate`, `available_bandwidth_mbps`, `queue_delay_ms`, `channel_stability`	Describe wireless-channel quality and transmission constraints affecting encrypted packet delivery, throughput, and end-to-end latency.
Resource and device-state variables	`residual_energy_level`, `residual_energy_percent`, `cpu_load_percent`, `memory_usage_mb`	Represent resource constraints of UAV and IoT nodes, allowing the framework to evaluate energy-aware cryptographic operation and rekeying feasibility.
Payload and traffic descriptors	`traffic_type`, `payload_size_bytes`, `plaintext_payload_type`, `plaintext_size_bytes`	Define the type and size of telemetry, command, coordination, and sensor-data messages protected by the proposed cryptographic framework.
ML-KEM key-establishment features	`mlkem_parameter_set`, `mlkem_encapsulation_status`, `mlkem_decapsulation_status`, `shared_secret_match`, `session_key_refresh_status`	Document post-quantum session-key establishment, shared-secret validation, and session-key refresh behavior during normal and high-risk operation.
Ascon-authenticated encryption features	`nonce_counter`, `associated_data_binding`, `ascon_encryption_status`, `ascon_decryption_status`, `tag_verification_status`	Record lightweight, authenticated encryption, decryption, nonce management, associated-data binding, and authentication-tag verification.
Payload confidentiality and integrity hashes	`plaintext_hash`, `ciphertext_hash`, `auth_tag_hex`, `associated_data_hash`	Provide traceable cryptographic representations without storing raw plaintext, thereby supporting reproducibility while preserving payload confidentiality.
Adaptive rekeying context features	`threat_level`, `packet_anomaly_density`, `mission_priority`, `traffic_sensitivity`, `session_age_ms`, `rekey_counter`	Provide the contextual inputs used by the adaptive rekeying mechanism to estimate session risk and determine whether key refresh is required.
Rekeying decision and policy outputs	`risk_score`, `tau_soft`, `tau_immediate`, `tau_critical`, `policy_decision`, `rekeying_class`, `rekeying_triggered`	Show how the framework maps contextual risk into normal continuation, soft rekeying, immediate rekeying, critical rekeying, or traffic suspension.
Cryptographic validation events	`crypto_validation_event`, `packet_status`, `session_action`, `secure_delivery_flag`, `integrity_success_flag`	Evaluate the framework response to replay attempts, ciphertext modification, invalid tags, delayed packets, and high-risk communication states.
Performance and resilience metrics	`encryption_latency_ms`, `decryption_latency_ms`, `mlkem_latency_ms`, `end_to_end_latency_ms`, `throughput_mbps`, `energy_overhead_mj`, `rekeying_overhead_mj`, `session_resilience_score`	Quantify the practical performance of the proposed framework in terms of latency, throughput, energy cost, rekeying overhead, and secure-session resilience.

3.2. Hybrid Cryptographic Architecture

The hybrid cryptographic architecture was designed to provide lightweight, authenticated, and quantum-resilient protection for mission-critical UAV–IoT communications by coupling Ascon-based telemetry encryption with ML-KEM-based session-key establishment within a unified secure transmission workflow. At the beginning of each communication session, the transmitting node, whether a UAV, sensor, or ground-control entity, initiates a secure handshake in which ML-KEM is used to encapsulate a fresh session key, thereby enabling post-quantum-resistant key agreement without relying on conventional public-key mechanisms that may become vulnerable under future cryptanalytic capabilities. Once the shared secret is derived, Ascon-authenticated encryption is applied to telemetry payloads, control messages, and sensor observations to ensure simultaneous confidentiality,

integrity, and authenticity with minimal computational and memory overhead, making it particularly suitable for resource-constrained aerial and field devices. Therefore, the secure message flow proceeds through four main stages: session initialization, post-quantum key encapsulation and decapsulation, lightweight authenticated payload encryption, and integrity-preserving packet verification at a receiving endpoint. In addition, the architecture supports continuous session protection through tightly coordinated key lifecycle management, where encryption contexts, nonce handling, and message authentication are synchronized with mission-state conditions and link-level security requirements.

The architecture follows a fixed execution sequence with clearly defined inputs, intermediate states, and outputs. The required inputs include sender and receiver identities, node credentials, mission context, payload sequence, associated data, ML-KEM public and private key material, contextual risk features, and rekeying thresholds. The intermediate states include the encapsulated shared secret, decapsulated shared secret, mission-bound session key, nonce value, associated-data binding, contextual risk score, policy decision, and session counter. The final outputs include verified ciphertext packets, authentication-tag status, delivery decision, rekeying state, and session-continuity status. This organization allows the secure-session workflow to be reproduced by executing the same sequence of authentication, ML-KEM encapsulation/decapsulation, key derivation, Ascon encryption, tag verification, and session-state update operations for each protected UAV–IoT communication event.

Figure 2 illustrates the end-to-end secure communication workflow of the proposed hybrid UAV–IoT framework, tracing a session from node authentication to verified encrypted delivery. The process begins with session initiation and identity validation of the requesting UAV, sensor, or ground station using device credentials, communication role, and mission context, thereby blocking unauthorized access before any cryptographic exchange occurs. After successful authentication, the protocol performs post-quantum session establishment through ML-KEM public-key exchange, sender-side encapsulation, and receiver-side decapsulation to derive a shared symmetric key with quantum-resilient protection. The workflow then evaluates the current security context, including threat level, residual energy, mobility state, channel stability, mission priority, traffic sensitivity, and packet anomaly density, allowing the AI policy unit to decide whether normal transmission should continue or adaptive rekeying is required. Once the session state is approved, Ascon AEAD encrypts telemetry, command, or sensor data, while nonce and associated-data binding securely link the ciphertext to mission metadata and packet headers to strengthen integrity. The protected packet is then transmitted over UAV-to-UAV, UAV-to-sensor, or UAV-to-ground links, and the receiver performs decryption and authentication-tag verification before releasing any information to higher layers. Invalid packets are discarded and flagged immediately, whereas verified payloads are delivered securely. Overall, the figure shows that the proposed design operates as a continuous, context-aware secure communication cycle that unifies post-quantum key establishment, lightweight authenticated encryption, adaptive rekeying, and session-continuity preservation within one integrated workflow. The workflow also clarifies the reproducible order of operations: authenticate the communicating endpoints, establish the post-quantum session key, evaluate contextual risk, decide whether rekeying is needed, encrypt and bind the payload with associated data, verify the authentication tag at the receiver, and update the secure-session state.

Algorithm 1 provides an implementation-oriented realization of the proposed hybrid security architecture by organizing the communication process into tightly coupled functional blocks that jointly manage authentication, post-quantum key establishment, contextual risk adaptation, and lightweight authenticated transmission within a persistent session state. The algorithm begins by validating both endpoints through the `AuthenticateNode`

function, where node identity, communication role, and mission-context eligibility are checked before any cryptographic computation is allowed, thereby preventing unauthorized entities from consuming key-establishment resources or entering the protected session space. Secure session initialization is then handled by `EstablishSessionKey`, which executes ML-KEM encapsulation and decapsulation to derive the common secret (K_{sess}) through a key-derivation function that binds the exchanged secret to mission context ($\mathcal{M}$) and timestamp information; this context binding is important because it prevents the reuse of a valid key across different mission states or link conditions. Once the session becomes active, the algorithm enters a controlled transmission loop governed by the session-state object ($\mathcal{S}$), where the packet counter, activity status, and transmission history are explicitly maintained to support nonce generation, replay resistance, and continuity-aware communication. The contextual intelligence of the method is concentrated in the pair of $\textsc{CollectContext}(\cdot)$ and $\Phi(\cdot)$, where the context vector (z) captures operational parameters such as threat level, residual node energy, mobility condition, channel stability, mission priority, traffic sensitivity, and packet anomaly density and these signals are transformed into a scalar risk score ($R = \sum_{i=1}^{7} \omega_i z[i]$) that quantifies the instantaneous security exposure of the link. This weighted formulation is critical because it allows the framework to prioritize different operational pressures depending on mission policy; for example, low residual energy and high anomaly density may jointly justify early rekeying in a contested environment, whereas stable channels and low threat scores allow the session to proceed with minimal overhead.

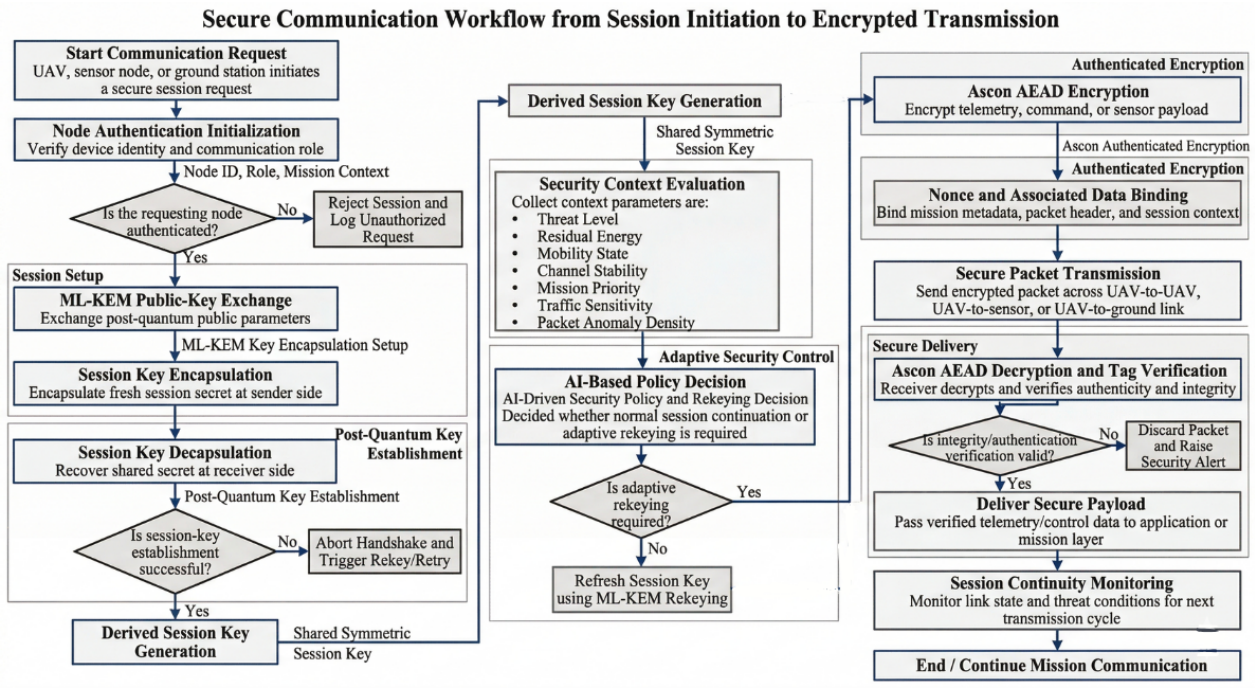


Figure 2. Secure communication workflow of the proposed hybrid Ascon–ML-KEM architecture from session establishment to authenticated transmission.

The AuthenticateNode function defines the admission condition for a node; EstablishSessionKey defines the ML-KEM encapsulation/decapsulation and key-derivation path; RiskScore defines the numerical risk computation; and the main loop defines how each payload element is encrypted, transmitted, verified, delivered, or rejected. The session object ($\mathcal{S}$) records the counter and activity state, ensuring that nonce generation, replay resistance, and mission termination are handled consistently across repeated simulation runs.

Algorithm 1 Adaptive Hybrid Secure Session Procedure

Require: Sender u_s, receiver u_r, payload array $\mathbf{P}[1:m]$, associated data $\mathbf{A}$, mission context $\mathcal{M}$, ML-KEM keys (pk_r, sk_r), policy model Φ, threshold τ
Ensure: Secure ciphertext packets $\mathcal{C}$ or ABORT

function AUTHENTICATENODE($u, \mathcal{M}$)
  if u.id $= \varnothing$ **or** u.role $= \varnothing$ **then**
    return false
  if VERIFYCREDENTIALS($u, \mathcal{M}$) $=$ **false then**
    return false
  return true
function ESTABLISHSESSIONKEY($pk_r, sk_r, \mathcal{M}$)
  $(K_e, ct_{kem}) \leftarrow$ MLKEM.ENCAPS(pk_r)
  $K_d \leftarrow$ MLKEM.DECAPS(sk_r, ct_{kem})
  if $K_e \neq K_d$ **then**
    return $(\perp, \perp)$
  $K_{sess} \leftarrow$ KDF($K_e \,\|\, \mathcal{M} \,\|$ timestamp)
  return (K_{sess}, ct_{kem})
function RISKSCORE($z[1:7]$)
  return $\sum_{i=1}^{7} \omega_i z[i]$
if AUTHENTICATENODE($u_s, \mathcal{M}$) = **false or** AUTHENTICATENODE($u_r, \mathcal{M}$) = **false then**
  LOG(Unauthorized session request)
  return ABORT
$(K_{sess}, ct_{kem}) \leftarrow$ ESTABLISHSESSIONKEY($pk_r, sk_r, \mathcal{M}$)
if $K_{sess} = \perp$ **then**
  LOG(Handshake failure)
  return ABORT
$\mathcal{S}$.counter $\leftarrow 0$; $\mathcal{S}$.active $\leftarrow$ **true**
$\mathcal{C} \leftarrow [\,]$
while $\mathcal{S}$.active $=$ **true and** $\mathcal{S}$.counter $< m$ **do**
  $z \leftarrow$ COLLECTCONTEXT($u_s, u_r, \mathcal{M}$)
  $R \leftarrow$ RISKSCORE(z)
  $\pi \leftarrow \Phi(z, \mathcal{M}, \mathcal{S})$
  if $R > \tau$ **or** $\pi =$ REKEY **then**
    $(K_{sess}, ct_{kem}) \leftarrow$ ESTABLISHSESSIONKEY($pk_r, sk_r, \mathcal{M}$)
    if $K_{sess} = \perp$ **then**
      RAISEALERT(Rekey failure)
      return ABORT
  $N \leftarrow$ NONCEGEN($K_{sess}, \mathcal{S}$.counter)
  $A^\star \leftarrow \mathbf{A} \,\|\, \mathcal{M} \,\|\, R$
  $(C, T) \leftarrow$ ASCON.ENC($K_{sess}, N, \mathbf{P}[\mathcal{S}.\text{counter} + 1], A^\star$)
  SEND($ct_{kem}, N, A^\star, C, T$)
  $P' \leftarrow$ ASCON.DEC($K_{sess}, N, C, A^\star, T$)
  if $P' = \perp$ **then**
    DISCARDPACKET()
    RAISEALERT(Integrity/authentication failure)
    return ABORT
  else
    DELIVERPAYLOAD(P')
    Append (C, T) to $\mathcal{C}$
  $\mathcal{S}$.counter $\leftarrow \mathcal{S}$.counter $+ 1$
  if MISSIONENDED($\mathcal{M}$) $=$ **true then**
    $\mathcal{S}$.active $\leftarrow$ **false**
return $\mathcal{C}$

The AI policy model (Φ) adds a second decision layer beyond thresholding by inferring whether rekeying is required from the joint evolution of context, mission state, and session

history, meaning that key refresh is not triggered only by a single abnormal value but by the broader behavioral pattern of the communication state. When either $R > \tau$ or the policy output is REKEY, the algorithm re-enters the ML-KEM key-establishment routine to replace a session secret before further payload transmission, which makes the design resilient to context drift, prolonged exposure windows, and escalating threat conditions. Payload protection is then achieved through ASCON.ENC, where each payload unit ($P[\mathcal{S}.\text{counter} + 1]$) is encrypted under K_{sess} using a nonce ($N = \text{NONCEGEN}(K_{\text{sess}}, \mathcal{S}.\text{counter})$) and bound associated data ($A^{\star} = A \parallel \mathcal{M} \parallel R$), ensuring that confidentiality, integrity, and authenticity are simultaneously enforced while also cryptographically linking the ciphertext to mission metadata and the current contextual risk state. On the receiver side, ASCON.DEC performs tag verification and authenticated decryption, and any invalid output immediately triggers packet discardingand alert escalation, thereby preventing corrupted, replayed, or adversarially manipulated packets from propagating to the mission layer. The use of arrays, loop-controlled session progression, explicit state variables, and modular functions makes the algorithm not only mathematically coherent but also directly translatable into practical implementations for embedded UAV and IoT platforms. Overall, the algorithm demonstrates that the proposed framework is more than a conventional encryption routine; it is a state-aware secure communication controller in which the K_{sess}, ct_{kem}, z, R, τ, N, $A^{\star}$, and $\mathcal{S}$ parameters cooperate with the `AuthenticateNode`, `EstablishSessionKey`, `RiskScore`, Φ, ASCON.ENC, and ASCON.DEC components to sustain quantum-resilient, low-latency, and mission-adaptive protection throughout the full transmission lifecycle. The variables used in the algorithm correspond directly to the dataset attributes and metric records: z is derived from contextual features, R is stored as the risk-score output, π corresponds to the policy-decision field, rekeying events are reflected in the session-key refresh state and rekeying counter, and successful or failed packet verification is recorded through the delivery and integrity-status indicators.

The mathematical core of the proposed hybrid cryptographic architecture is formalized through four primary operations: post-quantum key encapsulation, key decapsulation, lightweight authenticated encryption, and authenticated decryption. First, during session establishment, the receiver generates an ML-KEM key pair (pk_r, sk_r), where pk_r is published to the sender and sk_r is kept private. The sender then applies the encapsulation function to derive a temporary shared secret (K_e), together with a ciphertext capsule (ct_{kem}), as expressed in Equation (1). After receiving this capsule, the receiver applies the decapsulation function in Equation (2) to recover the corresponding shared secret (K_d), which must match the sender-side secret to ensure successful session establishment. The shared secret is subsequently transformed into a mission-bound session key (K_{sess}) through the key derivation process in Equation (3), where the derived key is explicitly tied to the mission context ($\mathcal{M}$), the communication-link type, and timestamp metadata in order to prevent context-independent reuse. Once the session key has been established, the payload ($\mathbf{P}$) is protected using Ascon-authenticated encryption, where nonce N and associated data ($\mathbf{A}^{\star}$) are jointly processed with K_{sess} to generate ciphertext $\mathbf{C}$ and authentication tag $\mathbf{T}$, as shown in Equation (4). On the receiver side, the authenticated decryption operation in Equation (5) either reconstructs a valid plaintext ($\mathbf{P}'$) or returns the failure symbol ($\perp$), thereby ensuring that any tampered, replayed, or malformed packet is rejected before entering the mission layer. Together, these formulations show that the proposed framework combines quantum-resilient session establishment with lightweight authenticated data protection in a coherent end-to-end secure communication model. The same equations are used consistently across the proposed method and baseline implementations, with differences arising from the selected key-establishment primitive, payload-protection primitive, and rekeying policy.

$$(K_e, ct_{\text{kem}}) = \text{Encaps}(pk_r) \tag{1}$$

Equation (1) represents the ML-KEM encapsulation step executed by a sender, where the receiver's public key (pk_r) is used to generate a fresh shared secret (K_e) and the corresponding ciphertext capsule (ct_{kem}).

$$K_d = \text{Decaps}(sk_r, ct_{\text{kem}}) \tag{2}$$

Equation (2) defines the decapsulation process performed by a receiver, where the private key (sk_r) is used to recover a shared secret (K_d) from the received ciphertext capsule (ct_{kem}).

$$K_{\text{sess}} = \text{KDF}\big(K_e \parallel \mathcal{M} \parallel L_{\text{type}} \parallel t\big) \tag{3}$$

In Equation (3), the shared secret produced through encapsulation is transformed into the operational session key (K_{sess}) using a key derivation function, where $\mathcal{M}$ denotes the mission context, L_{type} denotes the communication-link type, and t denotes the session timestamp.

$$(\mathbf{C}, \mathbf{T}) = \text{AsconEnc}\big(K_{\text{sess}}, N, \mathbf{P}, \mathbf{A}^{\star}\big) \tag{4}$$

Equation (4) represents the Ascon-authenticated encryption step, where the plaintext payload ($\mathbf{P}$) is encrypted under the session key (K_{sess}) using nonce N and associated data $\mathbf{A}^{\star}$ to produce ciphertext $\mathbf{C}$ and authentication tag $\mathbf{T}$.

$$\mathbf{P}' = \text{AsconDec}\big(K_{\text{sess}}, N, \mathbf{C}, \mathbf{A}^{\star}, \mathbf{T}\big) = \begin{cases} \mathbf{P}, & \text{if tag verification succeeds} \\ \perp, & \text{otherwise} \end{cases} \tag{5}$$

Equation (5) defines the authenticated decryption and verification operation on the receiver side, where successful tag validation reconstructs the original plaintext payload, whereas any integrity or authenticity failure yields the rejection symbol ($\perp$).

$$\mathbf{A}^{\star} = \mathbf{A} \parallel \mathcal{M} \parallel H \parallel R \tag{6}$$

As expressed in Equation (6), the associated data ($\mathbf{A}^{\star}$) are formed by concatenating the original header-level metadata ($\mathbf{A}$) with mission context ($\mathcal{M}$), packet header information (H), and contextual risk score (R) so that integrity protection extends beyond the payload itself and covers the broader session state.

$$N = \text{NonceGen}\big(K_{\text{sess}}, c, t\big) \tag{7}$$

Equation (7) defines nonce generation, where c denotes a packet counter and t denotes time information, ensuring the uniqueness of the encryption nonce across repeated transmissions within the same secure session.

Table 2 provides a functional decomposition of the proposed hybrid secure communication framework and shows that its security is achieved through the coordinated operation of cryptographic, contextual, and session-management components rather than through a single encryption primitive alone. The table makes clear that the protection pipeline begins with the Node Authentication Module, where the sender (u_s), receiver (u_r), credential sets ($\mathcal{C}_s$ and $\mathcal{C}_r$), and mission context ($\mathcal{M}$) are jointly verified before any cryptographic state is created, thereby preventing unauthorized nodes from consuming security resources or entering the session lifecycle. Once admission is granted, the ML-KEM Encapsulation and Decapsulation Units generate the shared secrets (K_e and K_d) through the public key (pk_r), private key (sk_r), and ciphertext capsule (ct_{kem}), after which the Key Derivation Function

transforms these values into the operational session key (K_{sess}) by binding the secret to link type L_{type} and timestamp t, ensuring context-specific session isolation. The middle layers of the table reveal the adaptive intelligence of the framework: the Context Collection Engine gathers runtime variables such as link state, residual energy, mobility condition, anomaly level, and mission attributes into the context vector (z); the Risk Scoring Module converts these features into the scalar exposure measure (R) using weights $\omega_1, \ldots, \omega_7$; and the AI Policy Engine (Φ) interprets $(z, \mathcal{M}, \mathcal{S}, R)$ to produce the protection decision (π), which directly governs the Adaptive Rekeying Controller whenever the observed risk exceeds the operational threshold (τ). This means that key refresh is not only periodic but also driven by the communication state, mission urgency, and security pressure. The lower layers show how this intelligence is enforced during transmission, where the Nonce Generation Unit produces the unique nonce (N); the Associated Data Binder constructs $\mathbf{A}^\star$ from the metadata ($\mathbf{A}$), mission context ($\mathcal{M}$), packet header (H), and risk score (R); and the Ascon Encryption Unit processes $(K_{\text{sess}}, N, \mathbf{P}, \mathbf{A}^\star)$ to generate ciphertext $\mathbf{C}$ and authentication tag $\mathbf{T}$. The Transmission Interface forwards the protected packet across UAV–IoT links, while the Ascon Decryption Unit validates and reconstructs $\mathbf{P}'$ or returns $\perp$ under integrity failure. Finally, the Integrity Alert Manager and Session State Manager close a control loop by reacting to tampering, replay, or verification anomalies and updating the session state ($\mathcal{S}$), counters, and continuity variables for subsequent transmissions.

The logical dependency among the modules can be expressed as an ordered composition of mappings, where the output of each stage becomes either a control signal or cryptographic input for the next stage. The admission decision (d_{auth}) determines whether the protocol proceeds to ML-KEM session establishment. The encapsulated and decapsulated secrets are then reduced to the mission-bound session key (K_{sess}), which becomes the common input for nonce generation, Ascon encryption, and Ascon decryption. In parallel, mission and link-state variables are mapped into the context vector (z), converted into the exposure score (R), and interpreted by the policy engine (Φ) to produce the protection decision (π). This decision determines whether the current session key is retained or replaced through the adaptive rekeying controller. The packet-level path is then completed by binding $\mathbf{A}^\star$, generating $(\mathbf{C}, \mathbf{T})$, verifying the authentication tag, and updating the session state ($\mathcal{S}^+$).

$$
\begin{aligned}
d_{\text{auth}} &= f_{\text{auth}}(u_s, u_r, \mathcal{C}_s, \mathcal{C}_r, \mathcal{M}),\\
(K_e, K_d, ct_{\text{kem}}) &= f_{\text{kem}}(pk_r, sk_r),\\
K_{\text{sess}} &= f_{\text{kdf}}(K_e, \mathcal{M}, L_{\text{type}}, t),\\
z &= f_{\text{ctx}}(\text{link}, \text{energy}, \text{mobility}, \text{anomaly}, \text{mission}),\\
R &= f_{\text{risk}}(z, \omega) = \sum_i \omega_i z_i,\\
\pi &= \Phi(z, \mathcal{M}, \mathcal{S}, R),\\
(K^+_{\text{sess}}, ct^+_{\text{kem}}) &= f_{\text{rekey}}(\pi, R, \tau, pk_r, sk_r),\\
N &= f_{\text{nonce}}(K^+_{\text{sess}}, c, t),\\
\mathbf{A}^\star &= f_{\text{bind}}(\mathbf{A}, \mathcal{M}, H, R),\\
(\mathbf{C}, \mathbf{T}) &= f_{\text{enc}}(K^+_{\text{sess}}, N, \mathbf{P}, \mathbf{A}^\star),\\
\mathbf{P}' \text{ or } \perp &= f_{\text{dec}}(K^+_{\text{sess}}, N, \mathbf{C}, \mathbf{A}^\star, \mathbf{T}),\\
\mathcal{S}^+ &= f_{\text{state}}(\mathcal{S}, R, \pi, c, \text{verification}).
\end{aligned}
\tag{8}
$$

Table 2. Cryptographic components, functions, inputs, outputs, and input–output mapping relations in the proposed hybrid secure communication framework.

Component	Function	Input(s)	Output(s)	Mapping Relation
Node Authentication Module	Validates endpoint identity, role, and mission eligibility	$u_s, u_r, \mathcal{C}_s, \mathcal{C}_r$, and $\mathcal{M}$	Authentication status, and admission decision	$d_{\text{auth}} = f_{\text{auth}}(u_s, u_r, \mathcal{C}_s, \mathcal{C}_r, \mathcal{M})$
ML-KEM Encapsulation Unit	Generates sender-side post-quantum shared secret	pk_r	K_e and ct_{kem}	$(K_e, ct_{\text{kem}}) = \text{Encaps}(pk_r)$
ML-KEM Decapsulation Unit	Recovers receiver-side shared secret	sk_r and ct_{kem}	K_d	$K_d = \text{Decaps}(sk_r, ct_{\text{kem}})$
Key Derivation Function	Derives mission-bound session key	K_e, $\mathcal{M}$, L_{type}, and t	K_{sess}	$K_{\text{sess}} = f_{\text{kdf}}(K_e, \mathcal{M}, L_{\text{type}}, t)$
Context Collection Engine	Gathers runtime communication and mission-state features	Link state, energy state, mobility, anomalies, and mission attributes	Context vector (z)	$z = f_{\text{ctx}}(\text{link}, \text{energy}, \text{mobility}, \text{anomaly}, \text{mission})$
Risk Scoring Module	Quantifies instantaneous communication risk	$z = \{z_1, \ldots, z_7\}$ and $\omega_1, \ldots, \omega_7$	Risk score (R)	$R = f_{\text{risk}}(z, \omega) = \sum_i \omega_i z_i$
AI Policy Engine Φ	Determines adaptive rekeying and protection policy	z, $\mathcal{M}$, $\mathcal{S}$, and R	Decision (π)	$\pi = \Phi(z, \mathcal{M}, \mathcal{S}, R)$
Adaptive Rekeying Controller	Refreshes session key under elevated risk conditions	π, R, τ, pk_r, and sk_r	Updated K_{sess} and refreshed ct_{kem}	$(K^+_{\text{sess}}, ct^+_{\text{kem}}) = f_{\text{rekey}}(\pi, R, \tau, pk_r, sk_r)$
Nonce Generation Unit	Produces unique nonce for each transmission cycle	K_{sess}, c, and t	Nonce N	$N = f_{\text{nonce}}(K_{\text{sess}}, c, t)$
Associated Data Binder	Binds metadata and contextual state for integrity protection	$\mathbf{A}$, $\mathcal{M}$, H, and R	$\mathbf{A}^\star$	$\mathbf{A}^\star = f_{\text{bind}}(\mathbf{A}, \mathcal{M}, H, R)$
Ascon Encryption Unit	Performs lightweight authenticated encryption	K_{sess}, N, $\mathbf{P}$, and $\mathbf{A}^\star$	Ciphertext $\mathbf{C}$ and tag $\mathbf{T}$	$(\mathbf{C}, \mathbf{T}) = \text{AsconEnc}(K_{\text{sess}}, N, \mathbf{P}, \mathbf{A}^\star)$
Transmission Interface	Delivers protected packet over UAV–IoT communication links	ct_{kem}, N, $\mathbf{A}^\star$, $\mathbf{C}$, and $\mathbf{T}$	Protected transmitted packet	$\mathcal{P}_{\text{tx}} = (ct_{\text{kem}}, N, \mathbf{A}^\star, \mathbf{C}, \mathbf{T})$
Ascon Decryption Unit	Executes authenticated decryption and tag verification	K_{sess}, N, $\mathbf{C}$, $\mathbf{A}^\star$, $\mathbf{T}$	$\mathbf{P}'$ or $\perp$	$\mathbf{P}'$ or $\perp = \text{AsconDec}(K_{\text{sess}}, N, \mathbf{C}, \mathbf{A}^\star, \mathbf{T})$
Integrity Alert Manager	Detects invalid, tampered, or replayed packets	Verification result and anomaly count	Packet discard, alert trigger, and session update	$a_{\text{alert}} = f_{\text{alert}}(\text{verification}, \text{anomaly})$
Session State Manager	Maintains secure session continuity and counters	$\mathcal{S}$, R, c, and mission status	Updated session state ($\mathcal{S}$)	$\mathcal{S}^+ = f_{\text{state}}(\mathcal{S}, R, \pi, c, \text{mission})$

Equation (8) defines the component chain at the system level. It shows that authentication controls session admission, ML-KEM establishes the cryptographic seed, key derivation binds the seed to the mission context, context collection and risk scoring quantify exposure, the policy function selects the protection action, rekeying updates the session secret when required, nonce generation and associated data binding define packet uniqueness and integrity scope, and Ascon decryption determines whether the payload is accepted or rejected.

3.3. AI-Driven Adaptive Rekeying Mechanism

Figure 3 presents the unified AI-driven adaptive rekeying architecture and its operational workflow, showing that rekeying in the proposed framework is not treated as a static periodic maintenance task but as an intelligent cross-layer control mechanism driven by the runtime mission and communication conditions. On the left side, the architectural layer formalizes how the system constructs the contextual decision space from ten key inputs—namely, threat level, residual energy, mobility state, channel stability, packet anomaly density, mission priority, traffic sensitivity, link type, session age, and rekey counter, all of which collectively describe the instantaneous exposure, urgency, and resource state of the UAV–IoT session. The parameters are first processed by the context collection and normalization engine to generate the context vector ($z = \{z_1, z_2, \ldots, z_n\}$), ensuring that heterogeneous features with different physical meanings and numerical scales can be fused into a consistent representation for downstream decision making. The risk scoring

module then transforms the normalized vector into the scalar risk estimate ($R = \sum_{i=1}^{n} w_i z_i$), where the weights ($w_i$) encode the relative security importance of each factor, allowing the framework to emphasize, for instance, anomaly density and channel instability under adversarial conditions or residual energy and session age under endurance-constrained mission phases. The risk descriptor, together with the current session state ($\mathcal{S}$) and mission context ($\mathcal{M}$), is fed into the AI policy engine (Φ), which acts as the core adaptive intelligence layer by inferring whether the ongoing communication should continue normally, undergo soft rekeying, trigger immediate rekeying, or suspend sensitive transmission altogether. The lower cryptographic-core interface further clarifies that these decisions are not abstract policy outputs but directly control concrete security components, including the ML-KEM rekeying controller, key derivation function, session key store, and Ascon AEAD encryption context, thereby tightly coupling contextual intelligence with quantum-resilient key refresh and lightweight authenticated payload protection. The central adaptive rekeying control bus visually reinforces this coupling by linking the decision architecture to the right-side execution workflow, where the operational logic translates policy into secure communication behavior. In that workflow, the session is first initialized through ML-KEM-based key establishment and derivation of the operational session key, after which each transmission cycle repeatedly collects fresh context, computes the new risk score (R), and evaluates the policy function ($\Phi(z, \mathcal{M}, \mathcal{S})$). The "Is rekeying required?" decision node is followed by a second severity-aware branch, which distinguishes low/moderate, high, and critical exposure levels, enabling differentiated responses rather than a binary refresh decision. In the soft-rekey path, the system performs a lightweight key refresh while preserving communication continuity; in the immediate-rekey path, it forces re-encapsulation, session-key replacement, and nonce/counter reset to rapidly reduce cryptographic exposure; and in the critical path, it halts sensitive packet release, raises a security alert, executes emergency key refresh, and re-validates session continuity before resuming operation. All branches then converge into the Ascon AEAD protection stage, secure packet transmission, and integrity/authentication verification, ensuring that packet confidentiality, authenticity, and context-bound integrity remain enforced after every rekeying event. The final update of the session state, risk history, and rekey counter shows that the system continuously learns from the evolving communication history, making future decisions dependent not only on instantaneous measurements but also on session progression and accumulated exposure [34].

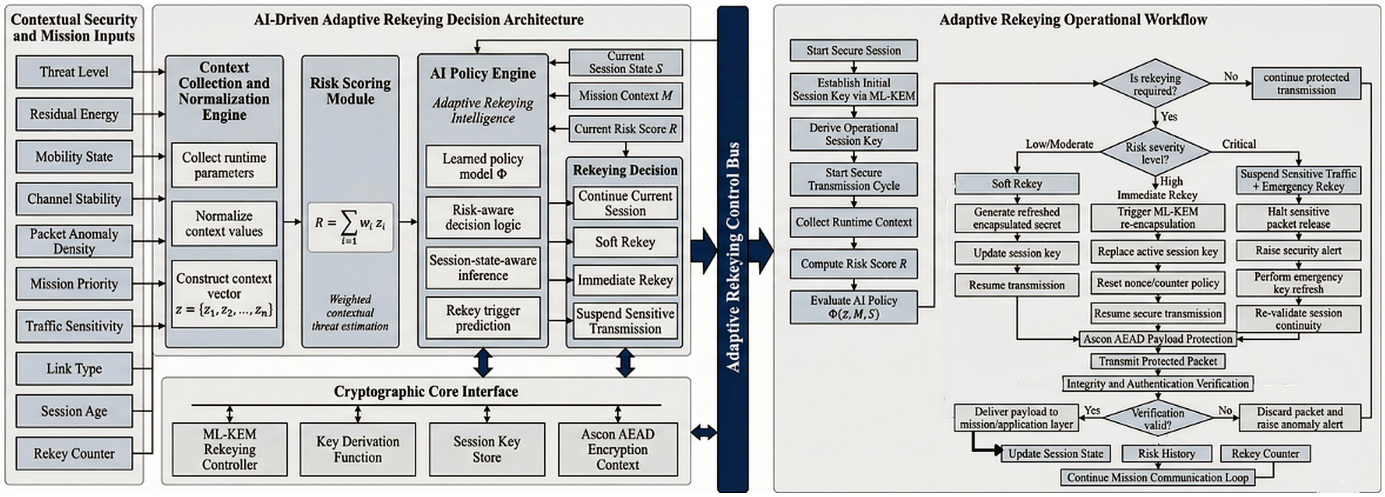


Figure 3. AI-driven adaptive rekeying architecture and context-aware decision workflow of the proposed Ascon–ML-KEM UAV–IoT Security Framework.

The adaptive rekeying model is specified through an explicit input–state–decision mapping. The input vector is defined as [35]

$$z = \begin{bmatrix} z_{\text{threat}}, & z_{\text{energy}}, & z_{\text{mobility}}, & z_{\text{channel}}, & z_{\text{anom}}, \\ z_{\text{priority}}, & z_{\text{sensitivity}}, & z_{\text{link}}, & z_{\text{age}}, & z_{\text{rekey}}, \end{bmatrix}$$

where the elements denote the threat level, residual energy, mobility state, channel stability, packet anomaly density, mission priority, traffic sensitivity, link type, session age, and rekey counter, respectively. These variables are normalized before risk estimation so that categorical, bounded, and continuous indicators can be combined within one decision vector. The scalar exposure score (R) represents the weighted contribution of the normalized context variables, whereas the policy output ($\rho = \Phi(z, \mathcal{M}, \mathcal{S}, R)$) represents the learned decision associated with the current mission context and session state. The threshold set ($\{\tau_{\text{soft}}, \tau_{\text{imm}}, \tau_{\text{crit}}\}$) maps the risk score into four operational classes: normal continuation, soft rekeying, immediate rekeying, and critical-session handling. This formulation separates numerical exposure estimation from policy-based decision inference, allowing the rekeying controller to account for both threshold-defined risk and contextual session behavior.

Algorithm 2 formalizes the proposed AI-driven adaptive rekeying mechanism by integrating contextual feature acquisition, weighted risk scoring, learned policy inference, severity-aware rekey classification [36], ML-KEM-based key refresh, and Ascon-protected payload transmission within a closed-loop secure session controller. The procedure defines the decision sequence, from context acquisition to packet verification, through a fixed set of state transitions. During each transmission cycle, the context vector (z) is collected and normalized, the exposure score (R) is computed from the weight vector ($\mathbf{w}$), the policy output (ρ) is inferred from Φ, and the severity class (σ) is assigned according to the threshold set. If the resulting state requires rekeying, the session key is regenerated through ML-KEM encapsulation and decapsulation, then bound to the mission context, session counter, and epoch through the key-derivation function. The nonce counter and epoch are updated only for immediate or critical states, which distinguishes low-disruption key refresh from emergency session recovery. Packet encryption, authentication-tag verification, delivery, rejection, and session-state update are then executed in sequence, creating a traceable control path from context variables to cryptographic action.

The four rekeying classes define distinct operational actions. NORMAL maintains the current session key and permits uninterrupted encrypted transmission. SOFT performs a low-disruption refresh to limit exposure caused by session age or moderate contextual risk. IMMEDIATE indicates elevated risk and forces key replacement, nonce-counter reset, and epoch advancement before further protected transmission. CRITICAL represents severe exposure and suspends sensitive packet release until emergency rekeying and session-continuity validation are completed. This severity-based structure specifies how risk estimates are translated into concrete cryptographic operations rather than treating rekeying as a fixed periodic event or a binary refresh decision.

Algorithm 2 AI-Driven Adaptive Rekeying Procedure

Require: $K_{\text{sess}}, \mathcal{M}, \mathcal{S}, \{\tau_{\text{soft}}, \tau_{\text{imm}}, \tau_{\text{crit}}\}, \mathbf{w}, \Phi, pk_r, sk_r$
Ensure: Updated session state $\mathcal{S}$

function RISK($z, \mathbf{w}$)
  return $\sum_i w_i z[i]$
function REKEY($pk_r, sk_r, \mathcal{M}, \mathcal{S}$)
  $(K_e, ct_{\text{kem}}) \leftarrow$ MLKEM.ENCAPS(pk_r)
  $K_d \leftarrow$ MLKEM.DECAPS(sk_r, ct_{kem})
  if $K_e \neq K_d$ **then**
    return $(\perp, \perp)$
  return $(\text{KDF}(K_e \| \mathcal{M} \| \mathcal{S}.\text{counter} \| \mathcal{S}.\text{epoch}), ct_{\text{kem}})$
$\mathcal{S}$.active $\leftarrow$ **true**
while $\mathcal{S}$.active **do**
  $z \leftarrow$ NORMALIZE(COLLECTCONTEXT())
  $R \leftarrow$ RISK($z, \mathbf{w}$); $\rho \leftarrow \Phi(z, \mathcal{M}, \mathcal{S}, R)$
  $\sigma \leftarrow \begin{cases} \text{NORMAL}, & R < \tau_{\text{soft}} \\ \text{SOFT}, & R < \tau_{\text{imm}} \\ \text{IMMEDIATE}, & R < \tau_{\text{crit}} \\ \text{CRITICAL}, & \text{otherwise} \end{cases}$
  if $\rho \neq$ CONTINUE **or** $\sigma \neq$ NORMAL **then**
    $(K_{\text{new}}, ct_{\text{kem}}) \leftarrow$ REKEY($pk_r, sk_r, \mathcal{M}, \mathcal{S}$)
    if $K_{\text{new}} = \perp$ **then**
      if $\sigma =$ CRITICAL **then**
        $\mathcal{S}$.active $\leftarrow$ **false**; **break**
      else
        RAISEALERT(Rekey failure); **continue**
    $K_{\text{sess}} \leftarrow K_{\text{new}}$; $\mathcal{S}$.rekeyCounter $\leftarrow \mathcal{S}$.rekeyCounter $+ 1$
    if $\sigma \in \{$IMMEDIATE, CRITICAL$\}$ **then**
      $\mathcal{S}$.nonceCounter $\leftarrow 0$; $\mathcal{S}$.epoch $\leftarrow \mathcal{S}$.epoch $+ 1$
    if $\sigma =$ CRITICAL **then**
      SUSPENDSENSITIVETRAFFIC(); VALIDATESESSIONCONTINUITY($\mathcal{S}, \mathcal{M}$)
  $N \leftarrow$ NONCEGEN($K_{\text{sess}}, \mathcal{S}$.nonceCounter)
  $A^\star \leftarrow \mathbf{A} \| \mathcal{M} \| R \| \mathcal{S}$.epoch
  $(C, T) \leftarrow$ ASCON.ENC($K_{\text{sess}}, N, \mathbf{P}, A^\star$)
  SEND($ct_{\text{kem}}, N, A^\star, C, T$)
  if ASCON.DEC($K_{\text{sess}}, N, C, A^\star, T$) $= \perp$ **then**
    DISCARDPACKET(); RAISEALERT(Integrity/authentication failure)
  else
    DELIVERPAYLOAD()
  $\mathcal{S}$.nonceCounter $\leftarrow \mathcal{S}$.nonceCounter $+ 1$
  UPDATESESSIONSTATE($\mathcal{S}, R, \rho, \sigma$)
  if MISSIONENDED($\mathcal{M}$) **then**
    $\mathcal{S}$.active $\leftarrow$ **false**
return $\mathcal{S}$

3.4. Secure Communication Protocol and Cross-Layer Operation

Figure 4 illustrates the end-to-end secure communication protocol and cross-layer operation of the proposed framework, showing how mission-control infrastructure, aerial nodes, and field-level IoT entities are tightly integrated with an adaptive cryptographic core during live communication. At the top of the figure, the Ground Control Station, Mission Control Server, Edge Gateway, UAV swarm, distributed sensor cluster, and field actuator node define the real operational environment in which telemetry, control traffic, contextual measurements, and secure commands continuously circulate across ground-to-UAV, UAV-to-UAV, UAV-to-sensor, and sensor-to-actuator links. Rather than treating security as

an isolated lower-layer function, the proposed design embeds protection logic across the full protocol stack, from mission-level control and application-layer telemetry handling to session management, network communication, and protected payload execution. This is reflected in the central AI-Driven Adaptive Rekeying Control Core, where the context collection engine gathers protocol-relevant runtime parameters, including the threat level, residual UAV energy, mobility state, channel stability, packet anomaly density, mission priority, traffic sensitivity, link type, session age, and rekey counter, and transforms them into the normalized context vector (z). The risk scoring module then computes the contextual exposure score ($R = \sum_i w_i z_i$), which is interpreted jointly with mission context and session state by the AI policy engine (Φ) to determine whether the current session should continue, undergo soft rekeying, trigger immediate rekeying, or suspend sensitive traffic under critical conditions. The lower protocol-flow region clarifies how this decision intelligence is operationalized: nodes are first authenticated using UAV identity, sensor role, gateway role, and mission-context validation; an initial session key is then established through ML-KEM encapsulation, decapsulation, and shared-secret verification; and once the session state (S) becomes active, the protocol enters a persistent secure transmission cycle in which context is repeatedly collected, normalized, scored, and evaluated before every protected transmission phase. The decision logic in the center of the workflow is especially important because it distinguishes between no-rekey continuation, low/moderate-risk soft rekeying, high-risk immediate rekeying, and critical-state emergency handling, thereby enabling the framework to adapt key refresh intensity to the actual communication threat surface rather than relying on static timers. After rekeying decisions are resolved, the packet enters the Ascon AEAD protection stage, where the active session key, nonce N, payload $\mathbf{P}[i]$, and associated data ($A^\star$) are combined to produce authenticated ciphertext for transmission over UAV–IoT links.

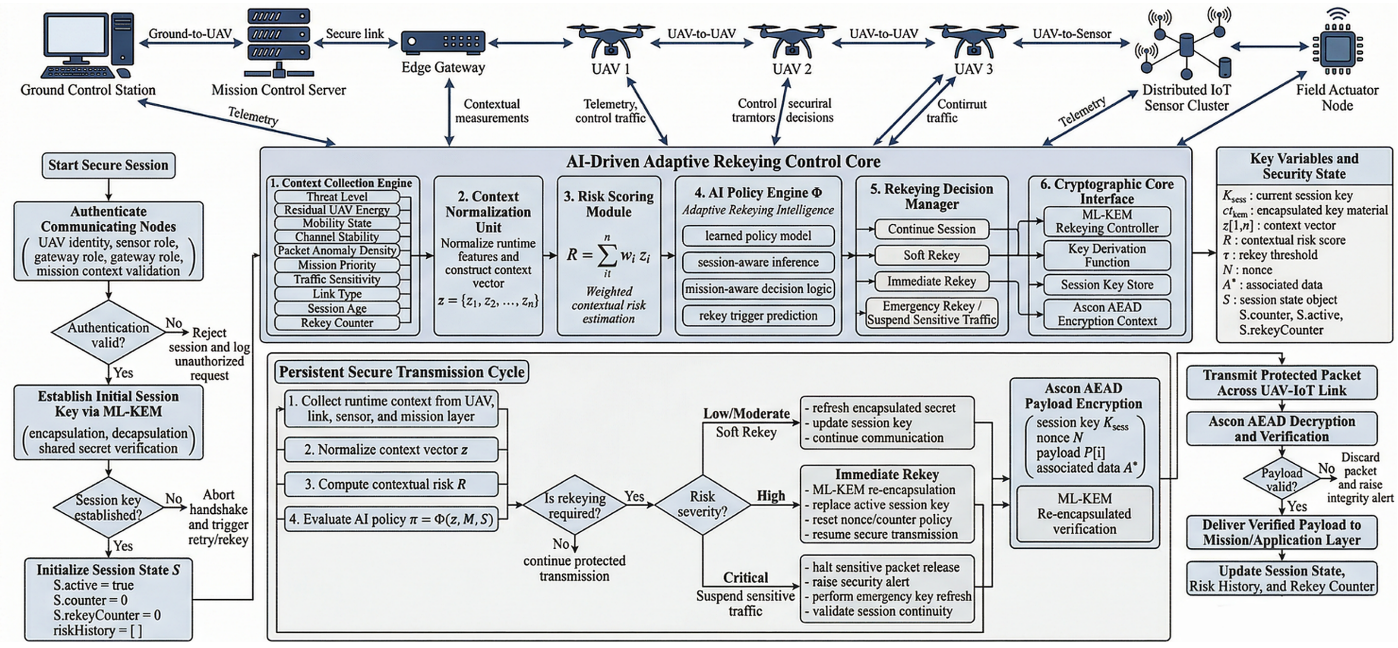


Figure 4. Cross-layer secure communication protocol and AI-Driven adaptive rekeying operation in the proposed UAV–IoT framework.

3.5. Experimental Design and Evaluation Protocol

The experimental design and evaluation protocol were adopted to validate the proposed UAV–IoT secure communication framework under realistic mission-oriented operating conditions. The evaluation methodology was structured to assess not only the cryptographic correctness of the hybrid Ascon–ML-KEM protection scheme but also the

operational effectiveness of the AI-driven adaptive rekeying mechanism when exposed to varying communication states, mobility conditions, and threat intensities. To achieve this, the framework was examined through a combination of simulated mission scenarios, generated secure communication traces, and attack-aware validation settings that reflect UAV-to-UAV, UAV-to-sensor, and UAV-to-ground interactions. The protocol specifies the system topology, implementation environment, parameter settings, evaluation datasets or generated traces, attack scenarios, and comparison baselines while also defining the main performance dimensions used for analysis, including security effectiveness, authenticated delivery reliability, end-to-end latency, throughput behavior, energy overhead, rekeying cost, and resilience under dynamically changing threat conditions. In this way, the experimental protocol provides a rigorous and reproducible foundation for quantifying both the security benefits and the practical deployment feasibility of the proposed architecture in resource-constrained and mission-critical UAV–IoT environments.

The energy-overhead values reported in this study were obtained using a simulation-based embedded-platform energy model rather than direct physical power measurements from a deployed UAV prototype. The assumed target platform represents a resource-constrained ARM Cortex-class UAV–IoT processing unit, which is commonly used as a practical reference profile for lightweight aerial sensing and field communication nodes. For each secure communication session, the energy overhead was estimated from the simulated execution time of the main cryptographic and adaptive-security operations and the corresponding active processing power assumed for the embedded platform. The session-level energy value includes ML-KEM encapsulation and decapsulation, key derivation, Ascon-authenticated encryption and decryption, authentication-tag verification, session-state management, and the additional cost of adaptive rekeying when triggered. The total session energy was computed as $E_{\text{session}} = \sum_i P_i t_i$, where P_i denotes the assumed active power associated with operation i and t_i denotes the corresponding simulated execution time. Therefore, the reported mJ/session values should be interpreted as platform-aware simulation estimates for an ARM Cortex-class constrained UAV communication node rather than as direct FPGA, GPU, or laboratory power-meter measurements.

Table 3 demonstrates that the experimental campaign was deliberately organized as a structured progression of twenty increasingly demanding validation conditions rather than as a set of isolated parameter trials so that the proposed framework can be examined under controlled escalation in mission scale, communication pressure, policy-network capacity, and adaptive rekeying sensitivity. The policy function (Φ) was implemented as a lightweight feed-forward deep neural network that receives a 10-dimensional normalized context vector and outputs one of four rekeying decisions: normal continuation, soft rekeying, immediate rekeying, or critical traffic suspension. Therefore, the hidden-layer configurations reported in Table 3, such as 64-32-16, 128-64-32, and 256-128-64, define the architecture of Φ rather than a generic unspecified learning module. In the first configuration block (E1–E4), the network remains at a compact scale of 3 UAVs and 20 sensors, with low-to-medium threat exposure; payload sizes increasing from 128 bytes in E1 to 512 bytes in E4; and a lightweight Φ architecture of 64-32-16 hidden units trained with learning rates of 1.0×10^{-3} in E1–E2 and 8.0×10^{-4} in E3–E4, a batch size of 64, dropout of between 0.20 and 0.25, and 50–60 epochs. This initial group defines the baseline operating envelope in which the soft, immediate, and critical rekeying thresholds remain relatively relaxed, ranging from $(0.35, 0.60, 0.85)$ in E1–E2 to $(0.32, 0.58, 0.84)$ in E3–E4, which indicates that rekeying is reserved for more pronounced security-state deviations. The second block (E5–E10) increases both operational and learning complexity by moving to a larger 128-64-32 Φ policy network, payload sizes of up to 1024 bytes in E6 and E7, and learning rates reduced from 7.0×10^{-4} in E5–E6 to 5.0×10^{-4} in E9–E10, while the

epoch budget expands to 60–70 and dropout rises to 0.30 in E6–E10. At the same time, the threshold triplets contract from $(0.30, 0.56, 0.82)$ in E5 to $(0.28, 0.53, 0.78)$ in E7–E8, then partially recover to $(0.33, 0.57, 0.83)$ in E9 and $(0.31, 0.56, 0.82)$ in E10, showing that the framework was tested not only under greater traffic and threat stress but also under different policy-aggressiveness settings to examine the responsiveness of adaptive rekeying across U2U, U2S, and U2G communication modes. A third escalation phase appears in E11–E16, where the topology expands to 4 UAVs and 30 sensors, training depth rises to 75–80 epochs, batch size grows from 128 in E11–E15 to 256 in E16, and the Φ network capacity reaches 256-128-64 in E12–E16. During this stage, the learning rate is reduced further from 5.0×10^{-4} in E11 to 4.0×10^{-4} in E12–E13, then to 3.0×10^{-4} in E14–E16, while the threshold bands narrow from $(0.31, 0.55, 0.81)$ in E11 to $(0.29, 0.54, 0.79)$ in E12–E13, $(0.27, 0.50, 0.75)$ in E14–E15, and $(0.26, 0.49, 0.74)$ in E16. This indicates a progressively more sensitive rekeying policy as mission conditions shift from medium and high risk toward critical-risk operation. The final block (E17–E20) constitutes the most severe validation regime, where the mission scale reaches 5 UAVs and 40 sensors, payload sizes remain at 512–1024 bytes, the batch size is fixed at 256, epochs are fixed at 80, and the learning rate decreases to 2.5×10^{-4} in E17-E18 and 2.0×10^{-4} in E19–E20 to stabilize learning under maximum threat and maximum system scale. In parallel, the rekeying thresholds are tightened to $(0.28, 0.52, 0.77)$ in E17, $(0.25, 0.48, 0.72)$ in E18, $(0.25, 0.47, 0.71)$ in E19, and $(0.24, 0.46, 0.70)$ in E20, representing the most aggressive threshold configuration in this study and, therefore, the setting most sensitive to contextual risk fluctuations. For reproducibility, Φ was trained offline using the generated 120,000-record UAV–IoT cryptographic benchmarking dataset. Each training record contains the secure-session context, risk score, threshold values, cryptographic validation outcome, and corresponding rekeying class. The target labels were generated from the combined threshold-based decision logic and validation-event outcomes, with low-risk sessions corresponding to normal continuation, moderate-risk sessions corresponding to soft rekeying, high-risk sessions corresponding to immediate rekeying, and critical-risk or integrity-failure cases corresponding to critical suspension. The model was optimized using categorical cross-entropy loss with the Adam optimizer, while the learning rate, batch size, dropout ratio, and number of epochs were varied according to Table 3. During online mission execution, Φ is not fully retrained onboard the UAV. Instead, online adaptation is achieved through lightweight inference using the current context vector, followed by continuous updates of the session state, risk score, rekey counter, nonce counter, and threshold comparisons. In summary, the table reveals a carefully engineered validation strategy in which network size increases from 3 to 5 UAVs and from 20 to 40 sensors, payload load increases from 128 to 1024 bytes, learning rates decrease from 1.0×10^{-3} to 2.0×10^{-4}, hidden-layer capacity grows from 64-32-16 to 256-128-64, batch size expands from 64 to 256, and critical-risk thresholds contract from 0.85 in E1–E2 to 0.70 in E20. This systematic progression is important because it confirms that the proposed framework was evaluated across a broad spectrum of mission realities, ranging from lightweight, low-risk communication to large-scale, high-throughput, critical-threat UAV–IoT operation, thereby allowing the subsequent performance results to be interpreted as evidence of robustness, scalability, policy sensitivity, and reproducible adaptive-rekeying behavior rather than as outcomes tied to a single favorable parameter setting.

The evaluated baselines were configured using explicitly defined cryptographic primitives, key sizes, and rekeying policies. Table 4 summarizes the baseline settings used in the comparative evaluation. The conventional symmetric baseline represents a lightweight classical configuration using AES-128-GCM without post-quantum key establishment. The static hybrid PQC baseline uses ML-KEM-based session-key establishment with Ascon-authenticated encryption, but it keeps the session key fixed during the session unless a

session failure occurs. The fixed-rekey hybrid baseline uses the same ML-KEM–Ascon cryptographic stack but refreshes the session key at a fixed interval, independent of threat level, residual energy, mobility state, channel condition, and anomaly density. The proposed framework differs from these baselines by using AI-driven adaptive rekeying, where key refresh is triggered according to the joint evolution of mission context, security risk, and communication state.

Table 3. Experimental configurations and parameter settings across 20 evaluation experiments. Abbreviations U2G, U2U, and U2S denote UAV-to-ground, UAV-to-UAV, and UAV-to-sensor communication links, respectively. The "Φ Hidden" column reports the fully connected hidden-layer architecture of the lightweight feed-forward DNN policy function (Φ) used for adaptive rekeying decisions. LR denotes the learning rate used during offline training of Φ, while τ_{soft}, τ_{imm}, and τ_{crit} denote the soft, immediate, and critical rekeying thresholds, respectively.

Exp.	UAVs	Sensors	Payload (B)	Link	Threat	Ctx Dim	Φ Hidden	LR	Batch	Dropout	Epochs	τ_{soft}	τ_{imm}	τ_{crit}
E1	3	20	128	U2G	Low	10	64-32-16	1.0×10^{-3}	64	0.20	50	0.35	0.60	0.85
E2	3	20	256	U2U	Low	10	64-32-16	1.0×10^{-3}	64	0.20	50	0.35	0.60	0.85
E3	3	20	256	U2S	Medium	10	64-32-16	8.0×10^{-4}	64	0.25	60	0.32	0.58	0.84
E4	3	20	512	U2G	Medium	10	64-32-16	8.0×10^{-4}	64	0.25	60	0.32	0.58	0.84
E5	3	20	512	U2U	Medium	10	128-64-32	7.0×10^{-4}	64	0.25	60	0.30	0.56	0.82
E6	3	20	1024	U2S	High	10	128-64-32	7.0×10^{-4}	64	0.30	70	0.30	0.55	0.80
E7	3	20	1024	U2G	High	10	128-64-32	6.0×10^{-4}	64	0.30	70	0.28	0.53	0.78
E8	3	20	256	U2U	High	10	128-64-32	6.0×10^{-4}	128	0.30	70	0.28	0.53	0.78
E9	3	20	128	U2S	Low	10	128-64-32	5.0×10^{-4}	128	0.30	70	0.33	0.57	0.83
E10	3	20	256	U2G	Medium	10	128-64-32	5.0×10^{-4}	128	0.30	70	0.31	0.56	0.82
E11	4	30	256	U2U	Medium	10	128-64-32	5.0×10^{-4}	128	0.25	75	0.31	0.55	0.81
E12	4	30	512	U2S	High	10	256-128-64	4.0×10^{-4}	128	0.25	75	0.29	0.54	0.79
E13	4	30	512	U2G	High	10	256-128-64	4.0×10^{-4}	128	0.25	75	0.29	0.54	0.79
E14	4	30	1024	U2U	Critical	10	256-128-64	3.0×10^{-4}	128	0.25	80	0.27	0.50	0.75
E15	4	30	1024	U2S	Critical	10	256-128-64	3.0×10^{-4}	128	0.20	80	0.27	0.50	0.75
E16	4	30	256	U2G	Critical	10	256-128-64	3.0×10^{-4}	256	0.20	80	0.26	0.49	0.74
E17	5	40	512	U2U	High	10	256-128-64	2.5×10^{-4}	256	0.20	80	0.28	0.52	0.77
E18	5	40	512	U2S	Critical	10	256-128-64	2.5×10^{-4}	256	0.20	80	0.25	0.48	0.72
E19	5	40	1024	U2G	Critical	10	256-128-64	2.0×10^{-4}	256	0.20	80	0.25	0.47	0.71
E20	5	40	1024	U2U	Critical	10	256-128-64	2.0×10^{-4}	256	0.15	80	0.24	0.46	0.70

Table 4. Baseline configurations used for comparative evaluation.

Baseline	Payload Protection	Key Establishment	Rekeying Policy	Main Purpose
Conventional Symmetric	AES-128-GCM	Pre-shared symmetric key	No periodic rekeying	Classical low-overhead encryption reference
Static Hybrid PQC	Ascon AEAD	ML-KEM session establishment	Static per-session key	Post-quantum key establishment without adaptive refresh
Hybrid with Fixed Rekeying	Ascon AEAD	ML-KEM session establishment	Fixed interval: 60 s or 100 packets	Hybrid PQC protection with non-adaptive key refresh
Mahdi et al.—Aligned Hybrid	ASCON AEAD	Kyber-512	Static/session-based refresh	Literature-aligned hybrid PQC–AEAD IoT reference
Hoque et al.—Aligned PQC Wireless	Protocol-level protected channel	ML-KEM-based PQC handshake	Handshake/session dependent	Literature-aligned PQC wireless performance reference
Proposed Framework	Ascon AEAD	ML-KEM session establishment	AI-driven adaptive rekeying	Energy-aware, risk-aware, and mission-adaptive UAV–IoT security

The main evaluation metrics were formally defined to improve comparability across all baselines. The secure delivery rate measures the proportion of transmitted packets that are successfully delivered, authenticated, and accepted by the receiver:

$$SDR = \frac{N_{\text{secure}}}{N_{\text{total}}} \times 100\%, \tag{9}$$

where N_{secure} denotes the number of packets that are successfully decrypted and pass authentication-tag verification and N_{total} denotes the total number of transmitted packets.

Attack detection and mitigation effectiveness is defined as the percentage of attack events that are either detected, blocked, mitigated through rekeying, or prevented from reaching the mission layer:

$$ADME = \frac{N_{\text{detected}} + N_{\text{mitigated}}}{N_{\text{attack}}} \times 100\%, \tag{10}$$

where N_{attack} is the total number of injected or simulated attack events; N_{detected} is the number of attacks flagged by the security logic; and $N_{\text{mitigated}}$ is the number of attacks neutralized through packet rejection, integrity-failure handling, session suspension, or rekeying. The average end-to-end encryption latency is computed as

$$L_{\text{e2e}} = \frac{1}{N} \sum_{i=1}^{N} \left(t_{\text{verified}}^{(i)} - t_{\text{generated}}^{(i)} \right), \tag{11}$$

where $t_{\text{generated}}^{(i)}$ and $t_{\text{verified}}^{(i)}$ denote the generation and successful verification times of packet i, respectively. Throughput is defined as

$$T = \frac{\sum_{i=1}^{N_{\text{secure}}} B_i}{\Delta t}, \tag{12}$$

where B_i is the size of securely delivered packet i, and Δt is the observation interval. Energy overhead per session and rekeying overhead per event are computed as

$$E_{\text{session}} = \frac{\sum_{i=1}^{N} E_i}{N_{\text{sessions}}}, \qquad E_{\text{rekey}} = \frac{\sum_{j=1}^{N_{\text{rekey}}} E_{\text{rekey}}^{(j)}}{N_{\text{rekey}}}. \tag{13}$$

Finally, session resilience is measured as the percentage of sessions that remain secure and operational after attacks, channel degradation, integrity failures, and rekeying events:

$$SR = \frac{N_{\text{resilient}}}{N_{\text{sessions}}} \times 100\%. \tag{14}$$

4. Discussion, Results, and Comparison

Table 5 demonstrates that the proposed Ascon–ML-KEM + AI-driven rekeying framework achieves the strongest and most balanced performance across all evaluation criteria, with the reported values computed from the generated UAV–IoT secure communication traces produced by the Python-based benchmarking framework. In this comparison, security-related metrics were derived from successfully protected, verified, and resilient communication events, whereas latency, throughput, energy overhead, and rekeying overhead were estimated from simulated cryptographic execution, transmission behavior, and the embedded-platform energy model. These results confirm the practical advantage of integrating lightweight authenticated encryption, post-quantum key establishment, and adaptive session protection within a unified UAV–IoT security architecture. In particular, the proposed method attains the highest secure delivery rate of 99.2%, outperforming the conventional symmetric scheme (94.1%), the static hybrid PQC scheme (96.3%), and the hybrid scheme with fixed rekeying (97.4%), which indicates superior communication reliability under protected mission exchange. A similar pattern is observed in attack detection and mitigation effectiveness, where the proposed framework reaches 98.9%, compared with 90.8%, 94.6%, and 96.1% for the competing baselines, showing that the adaptive security logic enhances the system's ability to respond to hostile communication conditions more effectively. Despite providing stronger protection, the proposed framework also records the lowest end-to-end encryption latency of 8.7 ms, improving on 11.9 ms, 10.8 ms, and

9.9 ms, respectively, while simultaneously achieving the highest throughput of 5.03 Mbps, whereas the baseline methods remain limited to 4.82 Mbps, 4.57 Mbps, and 4.41 Mbps. From an efficiency perspective, the proposed approach yields the lowest energy overhead of 11.6 mJ/session and the smallest rekeying overhead of 2.9 mJ/event, clearly below the conventional symmetric baseline (16.8 mJ/session and 4.9 mJ/event), the static hybrid PQC scheme (15.1 mJ/session and 4.3 mJ/event), and the fixed-rekey hybrid method (14.2 mJ/session and 3.8 mJ/event), which confirms that the intelligence-driven rekeying strategy reduces unnecessary cryptographic burden rather than adding excessive control cost. Moreover, the proposed framework delivers the highest session resilience of 96.4% and integrity verification success of 99.1%, compared with only 84.7% and 95.3% for the conventional symmetric scheme, 88.9% and 97.1% for the static hybrid PQC method, and 91.6% and 98.0% for the fixed-rekey hybrid baseline.

Table 5. Comparative performance of the proposed framework against baseline schemes.

Method	Secure Delivery Rate (%)	Attack Detection/ Mitigation Effective-ness (%)	End-to-End Encryption Latency (ms)	Throughput (Mbps)	Energy Overhead (mJ/Session)	Rekeying Overhead (mJ/Event)	Session Resilience (%)	Integrity Verification Success (%)
Conventional Symmetric Scheme	94.1	90.8	11.9	4.82	16.8	4.9	84.7	95.3
Static Hybrid PQC Scheme	96.3	94.6	10.8	4.57	15.1	4.3	88.9	97.1
Hybrid Scheme with Fixed Rekeying	97.4	96.1	9.9	4.41	14.2	3.8	91.6	98.0
Proposed Ascon–ML-KEM + AI-Driven Rekeying Framework	99.2	98.9	8.7	5.03	11.6	2.9	96.4	99.1

Figure 5 provides a multi-perspective comparative interpretation of the overall results and clearly confirms the dominance of the proposed Ascon–ML-KEM + AI-driven rekeying framework across security, efficiency, and resilience dimensions. In the parallel-coordinates view, the proposed method consistently attains the highest normalized score across all metrics, indicating simultaneous superiority in secure delivery, attack detection, latency efficiency, throughput, energy behavior, rekeying cost, session resilience, and integrity verification, whereas the conventional symmetric scheme performs weakest overall and only shows relative strength in throughput. The Pareto-front panel further reinforces this conclusion by placing the proposed method at the top-right corner, with the best combined efficiency and security score, while the conventional, static PQC, and fixed-rekey baselines occupy progressively weaker positions. The directional heatmap shows the same trend numerically, with the proposed framework maintaining the strongest metric profile across all categories, while the baselines exhibit uneven behavior and visible weaknesses in security robustness and adaptive efficiency. This pattern is also reflected in the deviation-from-baseline profile, where the proposed scheme produces the largest improvement margins over the weakest baseline across nearly all metrics, with strong gains in latency-sensitive protection, energy-aware operation, rekeying efficiency, and resilience preservation. The composite-score lollipop plot summarizes the overall ranking in a highly interpretable manner, showing that the proposed framework achieves the highest weighted composite score while also maintaining superior headline values, including 99.2% secure delivery and 98.9% attack-detection effectiveness with only 8.7 ms end-to-end latency.

Table 6 confirms that the proposed framework maintains consistently strong security and communication efficiency across all twenty validation scenarios while also revealing a clear and technically meaningful performance transition as mission scale, payload burden, and threat severity increase. The values in this table were obtained from the generated scenario-level secure communication traces, with each experiment recording the simulated

delivery outcome, attack-mitigation response, latency, energy overhead, rekeying behavior, and session-resilience status under its corresponding UAV count, payload size, link type, and threat setting. In the early low-risk configurations, the framework delivers its strongest behavior, with secure delivery reaching 99.6% in E1 and 99.5% in E2; latency remaining very low, at 7.4 ms and 7.7 ms; energy overhead limited to 9.8 and 10.1 mJ/session; and the rekey count fixed at only one event, which indicates that the framework operates with minimal cryptographic disturbance under stable conditions. As the experiments move into medium-risk operation in E3–E5 and E10–E11, performance remains highly robust, with secure delivery still ranging from 98.8% to 99.2%, latency increasing only moderately to 8.0–8.5 ms, and attack mitigation remaining between 98.2% and 98.9%, despite the increase in payload size to 512 B and the transition across U2S, U2G, and U2U communication modes. Under high-risk conditions, represented by E6–E8, E12–E13, and E17, the framework still preserves strong reliability, with secure delivery between 98.2% and 98.7%, session resilience between 96.4% and 97.4%, and attack mitigation between 97.4% and 98.1%, although latency rises to 8.6–9.2 ms, energy overhead increases to 11.3–12.4 mJ/session, and rekey count grows to 3–4, which directly reflects the additional cryptographic effort required to preserve security under harsher conditions. The most demanding evidence appears in the critical scenarios (E14–E16 and E18–E20), where the system is exposed to tighter thresholds, larger network scale, and heavier operational stress; even in these cases, secure delivery remains between 97.3% and 98.0%, attack mitigation stays within 96.2–97.1%, and session resilience remains above 94.8%, while latency increases in a controlled manner from 9.4 ms in E16 to 10.2 ms in E20, energy overhead rises from 12.6 to 13.8 mJ/session, and rekey count reaches 5–6 events.

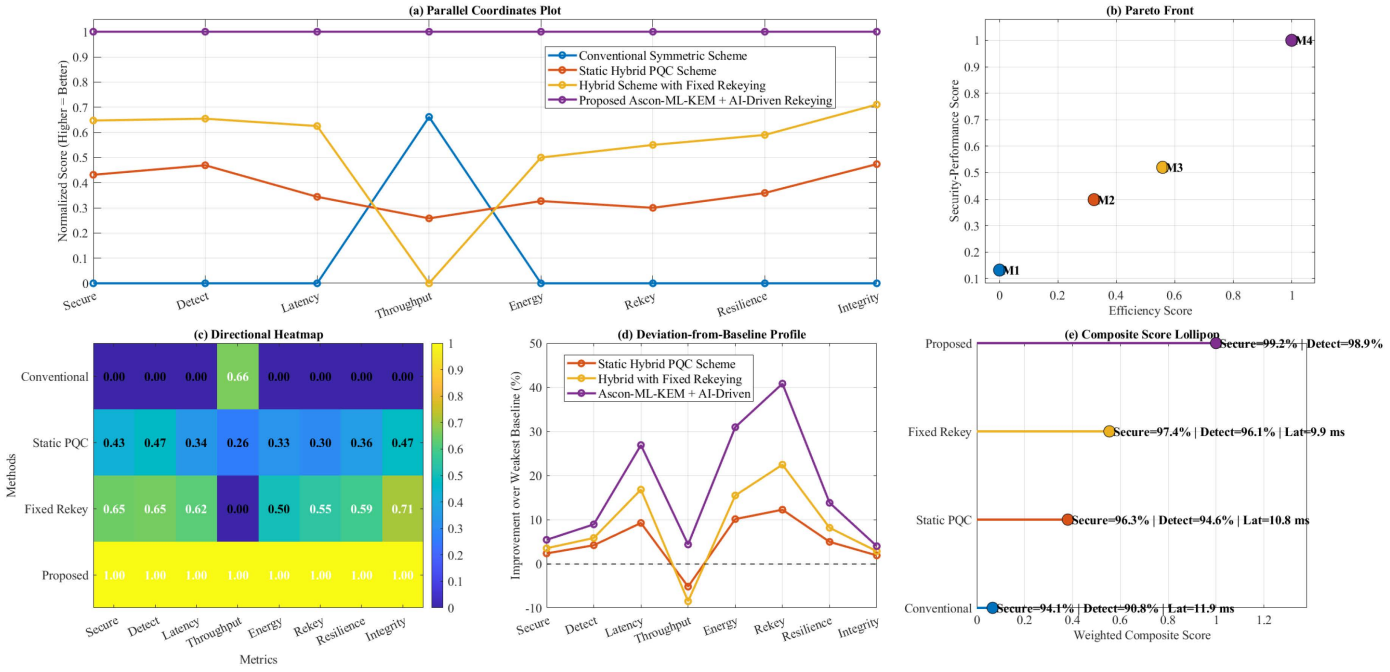


Figure 5. Security–efficiency trade-off analysis of the proposed Ascon–ML-KEM UAV–IoT framework: (**a**) parallel-coordinates profile, (**b**) pareto front, (**c**) directional heatmap, (**d**) baseline-deviation profile, and (**e**) composite-score lollipop plot.

Figure 6 provides a compact yet highly informative experiment-wise interpretation of the behavior of the proposed framework across the full E1–E20 validation trajectory and clearly shows that the system degrades in a gradual, controlled, and structurally meaningful manner as mission difficulty increases. In the clustered heatmap, the strongest normalized performance is concentrated in the early low-risk experiments, particularly

E1, E2, and E9, where delivery, resilience, and mitigation remain near the top of the scale, while the most demanding critical scenarios, especially E19 and E20, occupy the lowest region, confirming that larger payloads, tighter thresholds, and harsher threat conditions impose measurable stress on the framework. The parallel-coordinates panel reinforces this pattern by showing a progressive downward shift from early experiments toward later ones across delivery, latency efficiency, energy efficiency, resilience, and mitigation dimensions, while the rekey axis remains relatively high in more difficult scenarios, indicating that adaptive key refresh acts as an active compensatory protection mechanism rather than a passive overhead source. The bubble-matrix view further clarifies the relationship between the experiment index and threat category, showing a clear transition from low-threat cases with the highest secure-delivery percentages, such as E1 at 99.6%, E2 at 99.5%, and E9 at 99.4%, through medium- and high-threat regions and, finally, toward critical experiments such as E19 and E20, where secure delivery remains strong at 97.5% and 97.3%, despite the substantially harsher operating regime. The latent-space multi-metric trajectory is particularly important because it visualizes the experiments as an ordered progression rather than isolated points, revealing that the framework moves through a structured performance manifold as conditions intensify instead of exhibiting unstable or erratic transitions.

Table 6. Experiment-wise performance across validation scenarios E1–E20.

Exp. ID	UAVs	Sensors	Payload (B)	Link	Threat Level	τ_{soft}	τ_{imm}	τ_{crit}	Secure Delivery (%)	Latency (ms)	Energy Overhead (mJ/Session)	Rekey Count	Packet Discard (%)	Session Resilience (%)	Attack Mitigation (%)
E1	3	20	128	U2G	Low	0.35	0.60	0.85	99.6	7.4	9.8	1	0.4	98.7	99.3
E2	3	20	256	U2U	Low	0.35	0.60	0.85	99.5	7.7	10.1	1	0.5	98.5	99.1
E3	3	20	256	U2S	Medium	0.32	0.58	0.84	99.2	8.0	10.4	2	0.6	98.1	98.8
E4	3	20	512	U2G	Medium	0.32	0.58	0.84	99.1	8.2	10.8	2	0.7	97.9	98.6
E5	3	20	512	U2U	Medium	0.30	0.56	0.82	98.9	8.4	11.1	2	0.8	97.6	98.4
E6	3	20	1024	U2S	High	0.30	0.55	0.80	98.7	8.8	11.6	3	0.9	97.2	98.1
E7	3	20	1024	U2G	High	0.28	0.53	0.78	98.5	9.0	11.9	3	1.0	96.9	97.8
E8	3	20	256	U2U	High	0.28	0.53	0.78	98.8	8.6	11.3	3	0.8	97.4	98.0
E9	3	20	128	U2S	Low	0.33	0.57	0.83	99.4	7.8	10.0	1	0.5	98.4	99.0
E10	3	20	256	U2G	Medium	0.31	0.56	0.82	99.2	8.1	10.6	2	0.6	98.0	98.9
E11	4	30	256	U2U	Medium	0.31	0.55	0.81	98.8	8.5	11.4	3	0.8	97.5	98.2
E12	4	30	512	U2S	High	0.29	0.54	0.79	98.4	8.9	12.0	4	1.0	96.8	97.7
E13	4	30	512	U2G	High	0.29	0.54	0.79	98.3	9.1	12.2	4	1.1	96.6	97.5
E14	4	30	1024	U2U	Critical	0.27	0.50	0.75	97.9	9.6	12.9	5	1.4	95.8	97.0
E15	4	30	1024	U2S	Critical	0.27	0.50	0.75	97.7	9.8	13.2	5	1.5	95.5	96.8
E16	4	30	256	U2G	Critical	0.26	0.49	0.74	98.0	9.4	12.6	5	1.3	95.9	97.1
E17	5	40	512	U2U	High	0.28	0.52	0.77	98.2	9.2	12.4	4	1.1	96.4	97.4
E18	5	40	512	U2S	Critical	0.25	0.48	0.72	97.8	9.7	13.0	5	1.4	95.7	96.9
E19	5	40	1024	U2G	Critical	0.25	0.47	0.71	97.5	10.0	13.5	6	1.6	95.1	96.5
E20	5	40	1024	U2U	Critical	0.24	0.46	0.70	97.3	10.2	13.8	6	1.8	94.8	96.2

Figure 7 provides a complementary structural view of how the proposed framework behaves as these validation scenarios evolve from lighter and safer operating conditions toward larger, heavier, and more critical mission settings. In panel (a), the scenario-progression plots show that the early experiments, especially E1 and E10, were positioned in low-to-medium threat regions with smaller scale and lighter payload burden, and the same experiments remain associated with the strongest performance region, whereas later experiments, such as E14 and, in particular, E20, move toward higher threat, larger scale, heavier payload, and weaker relative performance positions. This confirms that these reductions in framework performance are not random but closely tied to the coordinated escalation of scenario difficulty across multiple dimensions. Panel (b) reinforces this interpretation through response-surface slices, where secure delivery remains highest in the low-threat region, reaching approximately 99.6% near the lighter-payload condition represented by E1 while gradually decreasing as payload size increases and threat intensity moves from medium and high toward critical conditions. Even in the most demanding region, around the critical-threat and 1024 B payload configuration associated with E20, secure delivery remains close to 97.3%, which indicates controlled degradation rather than abrupt security collapse. The surface also shows that threat escalation has stronger negative effect than payload increase alone, since delivery drops more sharply along the vertical threat axis than along the horizontal payload axis.

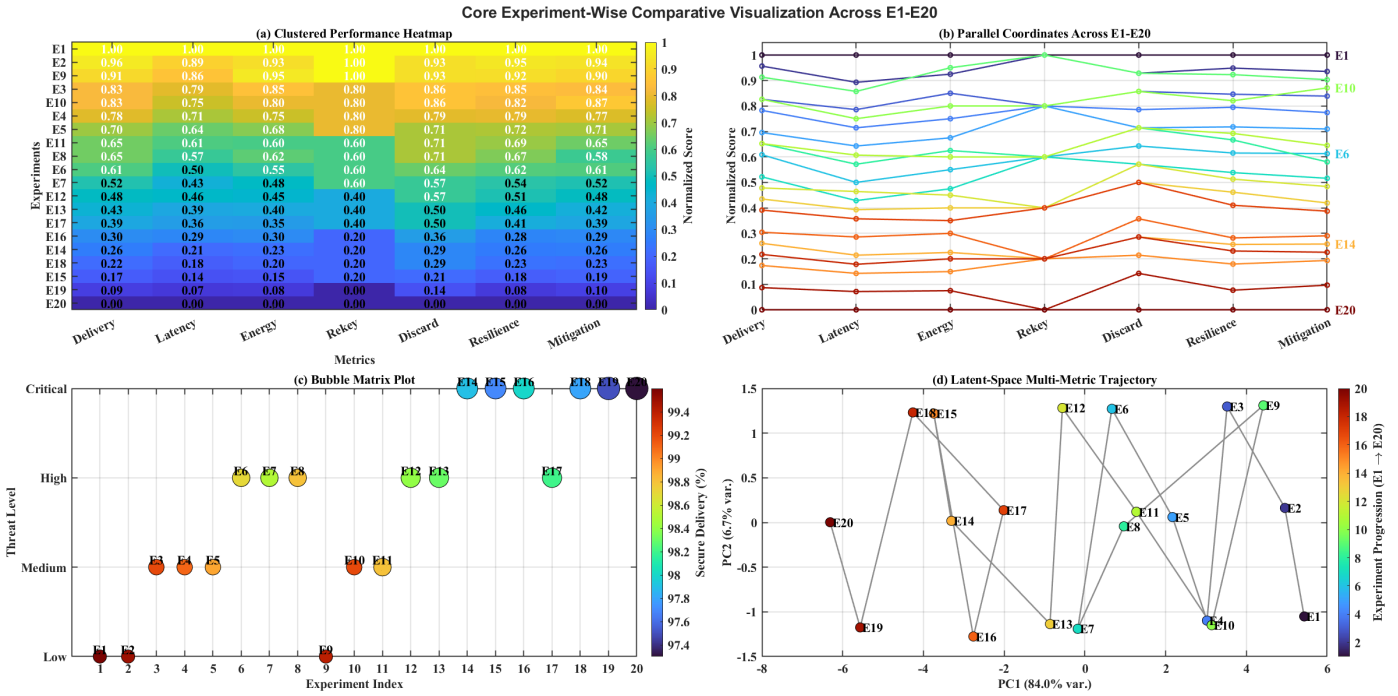


Figure 6. Experiment-wise security–performance evaluation of the proposed Ascon–ML-KEM UAV–IoT framework: (**a**) clustered performance heatmap, (**b**) parallel-coordinates profile, (**c**) threat-level bubble matrix, and (**d**) latent-space multi-metric trajectory.

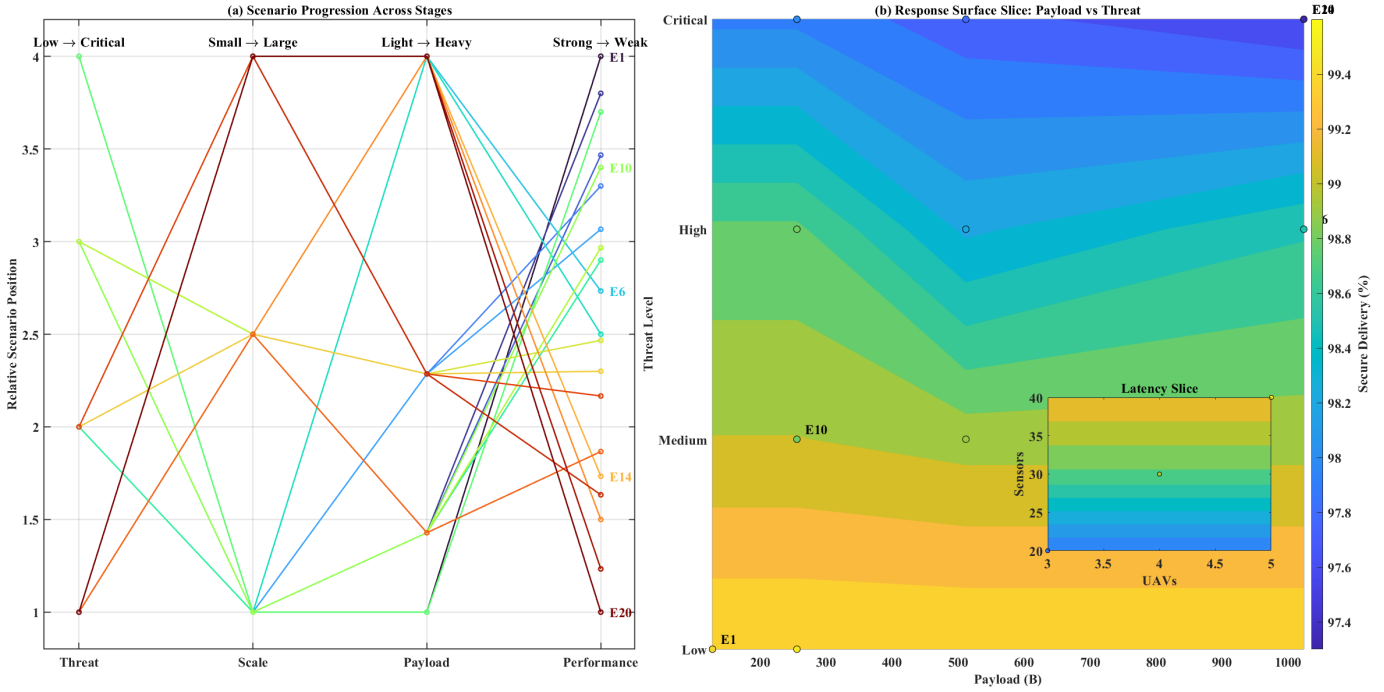


Figure 7. Scenario-Level Security–performance sensitivity analysis of the proposed Ascon–ML-KEM UAV–IoT framework: (**a**) stage-wise progression across threat, scale, payload, and performance; (**b**) payload–threat secure-delivery response surface and inset latency slice.

Table 7 shows that the proposed framework maintains a highly consistent level of secure communication performance across all three UAV–IoT link categories while also revealing meaningful differences that reflect the practical difficulty of each communication mode. The values in this table were obtained by grouping the generated secure communication traces according to link type—namely, U2G, U2U, and U2S—then computing the mean

delivery, latency, energy, rekeying, discard, resilience, and integrity-verification outcomes for each group. Among the evaluated links, U2G achieves the strongest overall performance, with the highest mean secure delivery rate of 98.53%, the lowest latency of 8.76 ms, the lowest energy overhead of 11.63 mJ/session, the smallest packet discard rate of 0.96%, the highest session resilience of 96.61%, and the highest integrity-verification success of 98.74%. This indicates that ground-connected communication benefits from relatively more stable coordination and lower communication volatility. U2U communication remains similarly strong, with a secure delivery rate of 98.44%, latency of 8.84 ms, energy overhead of 11.86 mJ/session, rekey frequency of 3.43, session resilience of 96.43%, and integrity-verification success of 98.61%, showing that the framework preserves robust protection, even under cooperative aerial exchange, where node mobility and swarm interaction introduce greater synchronization pressure than U2G links. By contrast, U2S represents the most demanding communication case, as reflected by the lowest secure delivery rate of 98.20%, the highest latency of 8.87 ms, the highest energy overhead of 12.03 mJ/session, the highest mean rekey frequency of 3.57, the highest packet discard rate of 1.03%, the lowest session resilience of 96.10%, and the lowest integrity-verification success of 98.46%. Although U2S is slightly more challenging because of field-device constraints, more variable edge conditions, and tighter security adaptation demands, the observed performance reduction remains very limited.

Table 7. Link-type-based performance analysis for U2G, U2U, and U2S communication.

Link Type	Mean Secure Delivery Rate (%)	Mean Latency (ms)	Mean Energy Overhead (mJ/Session)	Mean Rekey Frequency	Mean Packet Discard Rate (%)	Mean Session Resilience (%)	Mean Integrity-Verification Success (%)
U2G	98.53	8.76	11.63	3.29	0.96	96.61	98.74
U2U	98.44	8.84	11.86	3.43	1.00	96.43	98.61
U2S	98.20	8.87	12.03	3.57	1.03	96.10	98.46

Figure 8 presents a deep parameter-outcome interpretation of the proposed framework across the three communication-link types and shows that the observed performance differences are strongly aligned with the underlying methodological and control-state structure rather than arising from isolated metric variation. The heatmap indicates that U2S is associated with the highest normalized methodological pressure across several contextual factors, including threat, energy burden, channel volatility, anomaly exposure, traffic sensitivity, and aggressive control response, which is consistent with its role as the most operationally demanding link type. This is reflected in its outcome profile, where secure delivery reaches 98.20%, latency rises to 8.87 ms, energy overhead reaches 12.03 mJ/session, rekey frequency increases to 3.57, packet discard reaches 1.03%, resilience is 96.10%, and integrity-verification success remains strong at 98.46%. By contrast, U2G exhibits the most favorable outcome pattern, which coincides with stronger values in lightweight security adaptation, mission continuity control, and cross-layer robustness; accordingly, it achieves the highest secure delivery of 98.53%, the lowest latency of 8.76 ms, the lowest energy overhead of 11.63 mJ/session, the lowestrekey frequency of 3.29, the lowest packet discard rate of 0.96%, the highest resilience of 96.61%, and the highest integrity-verification success of 98.74%. U2U occupies an intermediate position, with secure delivery of 98.44%, latency of 8.84 ms, energy overhead of 11.86 mJ/session, rekey frequency of 3.43, packet discard of 1.00%, resilience of 96.43%, and integrity-verification success of 98.61%, which suggests that the framework sustains strong protection under cooperative aerial interaction but still experiences more control pressure than ground-linked communication.

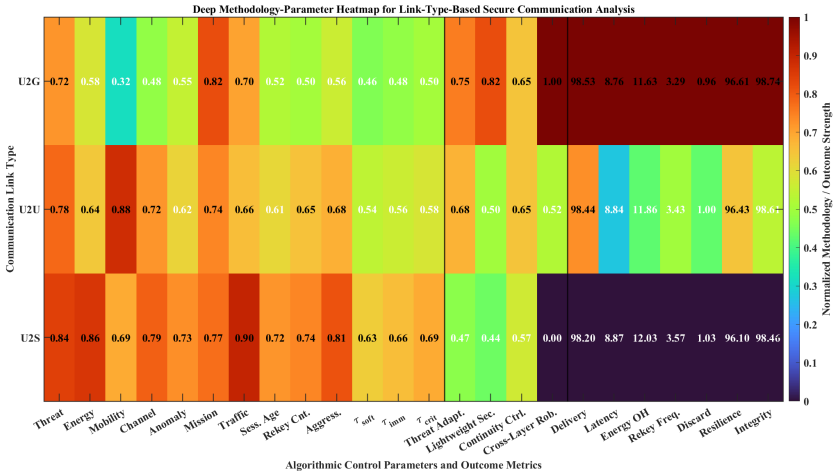


Figure 8. Deep methodology–parameter heatmap for link-type-aware secure communication performance in the proposed UAV–IoT framework.

Table 8 clearly demonstrates that the proposed framework preserves strong security and communication stability across all threat regimes while also exhibiting a gradual and controlled degradation pattern as the operational environment becomes more hostile. Under low-threat conditions, the framework achieves its best overall performance, with a mean secure delivery rate of 99.50%, mean attack mitigation effectiveness of 99.13%, latency of only 7.63 ms, energy overhead of 9.97 mJ/session, a mean rekey count of 1.00, zero emergency rekeying events, a very low session disruption rate of 0.50%, and a high resilience of 98.53%, indicating that the system can sustain secure communication with minimal cryptographic intervention when exposure is limited. As the threat level increases to medium, secure delivery decreases only slightly to 99.00%, attack mitigation remains high at 98.58%, latency rises moderately to 8.24 ms, and energy overhead increases to 10.86 mJ/session, while the mean rekey count more than doubles to 2.20 and emergency rekeying begins to appear at 0.20, showing that the framework responds adaptively rather than passively to growing risk. In the high-threat regime, the system still maintains 98.48% secure delivery, 97.70% attack mitigation effectiveness, and 96.72% resilience, despite the increases in latency to 8.93 ms, energy overhead to 11.90 mJ/session, mean rekey count to 3.40, and emergency rekey count to 0.80, which confirms that stronger protection is activated to preserve communication integrity under harsher attack pressure. Even in the most demanding critical-threat setting, the framework continues to deliver 97.70% secure delivery, 96.75% attack mitigation effectiveness, and 95.47% resilience, while latency reaches 9.78 ms, energy overhead increases to 13.17 mJ/session, mean rekey count rises sharply to 5.40, and emergency rekey count reaches 2.20; although the session disruption rate grows to 1.50%, this value remains low relative to the severity of the operating condition.

Table 8. Threat-level sensitivity and robustness analysis.

Threat Level	Mean Secure Delivery Rate (%)	Mean Latency (ms)	Mean Attack Mitigation Effectiveness (%)	Mean Rekey Count	Mean Emergency Rekey Count	Mean Energy Overhead (mJ/Session)	Mean Session Disruption Rate (%)	Mean Resilience (%)
Low	99.50	7.63	99.13	1.00	0.00	9.97	0.50	98.53
Medium	99.00	8.24	98.58	2.20	0.20	10.86	0.70	97.82
High	98.48	8.93	97.70	3.40	0.80	11.90	1.00	96.72
Critical	97.70	9.78	96.75	5.40	2.20	13.17	1.50	95.47

Figure 9 provides a comprehensive threat-aware interpretation of how the proposed framework reorganizes its security behavior as operating conditions evolve from low to critical severity, and it clearly shows that the observed performance degradation is tightly controlled by adaptive methodological responses rather than by uncontrolled instability.

In panel (a), secure continuity and cross-layer robustness begin at 100% under low-threat conditions, then decrease progressively to approximately 76% and 74% under medium threat; 43% and 41% under high threat; and, finally, to 0 at the normalized critical endpoint, while context pressure simultaneously rises from 8% to 33%, 62%, and 100% and adaptive burden increases from 0% to 22%, 51%, and 100%, confirming that escalating threat directly activates heavier defensive control behavior. Panel (b) reinforces this structural transition by showing that secure continuity, cross-layer robustness, burden efficiency, and latency efficiency dominate the low-threat regime, whereas threshold tightness and context-pressure-linked control become much stronger under high and critical conditions, indicating a systematic shift from efficiency-oriented operation toward protection-oriented enforcement. The same pattern is visible in panel (c), where mean resilience declines from 98.53% under low threat to 97.82% under medium threat, 96.72% at high and 95.47% at under critical threat, while mean energy overhead increases from 9.97 to 10.86, 11.90, and 13.17 mJ/session, demonstrating a clear security–efficiency tradeoff that remains gradual rather than abrupt. The methodology-linked transition heatmap in panel (d) makes this especially explicit by showing that delivery, mitigation, resilience, latency efficiency, and energy efficiency are strongest in the low-threat regime, all normalized at 1.00, but contract progressively as the environment moves toward high and critical states, whereas threshold-tightness dimensions, adaptive burden, and context pressure move in the opposite direction and peak at the critical stage. Panel (e) further quantifies this contraction by showing that mean energy overhead increases from 9.97 to 13.17 mJ/session, the mean rekey count rises from 1.00 to 5.40, and the mean emergency rekey count increases from 0.00 to 2.20 as the framework transitions from low to critical threat, while the threshold parameters tighten from approximately 0.35, 0.60, and 0.85 to 0.24, 0.46, and 0.70, thereby compressing the tolerance margins for adaptive response. The threshold–burden–quality overlay in panel (f) shows that increasing rekey activity and tighter thresholds are accompanied by gradual reductions in delivery, resilience, and mitigation, but these declines remain limited, with delivery still near 97.70%, resilience at 95.47%, and mitigation at 96.75% in the critical regime.

Table 9 provides strong evidence that the proposed AI-driven adaptive rekeying mechanism responds coherently and progressively to the escalation of contextual risk across the twenty validation scenarios, confirming that key refresh behavior is governed by communication-state severity rather than by rigid periodic scheduling. In the earliest low-risk experiments, such as E1, E2, and E9, the mean risk score remains very low, at 0.20, 0.22, and 0.23, respectively, and the framework triggers only one soft rekey event, with no immediate or critical rekeying, while maintaining very large mean rekey intervals of 18.8, 18.1, and 17.8; extremely high rekey success rates of 99.8%, 99.7%, and 99.7%; and minimal rekey-induced latency and energy overhead within 0.31–0.34 ms and 0.41–0.43 mJ/event. As the operating conditions move toward medium and high stress, represented by E3–E11, the mean risk score rises from 0.30 to 0.47, the total rekey count increases from 2 to 3 events, and the framework begins to combine soft and immediate rekeying decisions, while the mean rekey interval contracts from 14.9 in E3 to 11.6 in E7 and 12.9 in E11, indicating that the controller accelerates key refresh in response to mounting exposure. At the same time, rekey success remains very strong, staying between 99.0% and 99.5%, whereas rekey-induced latency increases only moderately from 0.40 to 0.56 ms and energy overhead increases from 0.50 to 0.70 mJ/event, which shows that the adaptation cost remains well controlled. A more pronounced transition appears in E12–E18, where mean risk scores rise to 0.53–0.70 and critical rekeying begins to emerge, with E12 and E13 each showing one critical rekey and E14, E15, E16, and E18 each reaching total rekey counts of five. In this regime, the mean rekey interval shrinks further to 10.7, 10.3, 8.8, 8.4, 9.1, and 8.6, while rekey-induced

latency grows to 0.61–0.82 ms and energy overhead reaches 0.76–1.00 mJ/event, reflecting the expected cost of more aggressive protection under sustained elevated risk. The most demanding scenarios, E19 and E20, represent the peak adaptive-response condition, with the highest mean risk scores of 0.74 and 0.77 and the highest total rekey counts of six and representing the only cases with two critical rekey events, while the mean rekey interval drops to 7.7 and 7.3, respectively, indicating that the framework compresses key refresh timing substantially when exposure becomes severe. Even under this maximum pressure, the rekey success rate remains high, at 98.1% in E19 and 97.9% in E20, while rekey-induced latency and energy overhead rise only to 0.91–0.96 ms and 1.10–1.16 mJ/event.

Table 9. AI-driven adaptive rekeying decision analysis.

Experiment	Mean Risk Score	Soft Rekey Count	Immediate Rekey Count	Critical Rekey Count	Total Rekey Count	Mean Rekey Interval	Rekey Success Rate (%)	Rekey-Induced Latency (ms)	Rekey-Induced Energy Overhead (mJ/Event)
E1	0.20	1	0	0	1	18.8	99.8	0.31	0.41
E2	0.22	1	0	0	1	18.1	99.7	0.34	0.43
E3	0.30	1	1	0	2	14.9	99.5	0.40	0.50
E4	0.32	1	1	0	2	14.4	99.4	0.43	0.53
E5	0.35	2	0	0	2	13.9	99.3	0.45	0.56
E6	0.44	2	1	0	3	12.1	99.1	0.52	0.65
E7	0.47	2	1	0	3	11.6	99.0	0.56	0.70
E8	0.42	2	1	0	3	12.4	99.1	0.50	0.63
E9	0.23	1	0	0	1	17.8	99.7	0.33	0.42
E10	0.34	1	1	0	2	14.2	99.4	0.42	0.52
E11	0.40	2	1	0	3	12.9	99.2	0.48	0.60
E12	0.53	2	1	1	4	10.7	98.9	0.61	0.76
E13	0.55	2	1	1	4	10.3	98.8	0.64	0.80
E14	0.67	2	2	1	5	8.8	98.5	0.78	0.95
E15	0.70	2	2	1	5	8.4	98.4	0.82	1.00
E16	0.62	2	2	1	5	9.1	98.6	0.74	0.91
E17	0.58	2	1	1	4	9.9	98.7	0.67	0.83
E18	0.69	2	2	1	5	8.6	98.4	0.80	0.98
E19	0.74	2	2	2	6	7.7	98.1	0.91	1.10
E20	0.77	2	2	2	6	7.3	97.9	0.96	1.16

Figure 10 provides a comprehensive experiment-wise view of how the proposed AI-driven rekeying controller transforms rising contextual risk into progressively stronger and more frequent security actions across E1–E20. In panel (a), the stacked streamgraph shows a clear escalation in rekey-state composition, with the earliest experiments, such as E1, E2, and E9, dominated by a single soft rekey action, while medium- and high-pressure scenarios introduce immediate rekeying and the most demanding cases, especially E12–E20, begin to accumulate critical rekey events. The total rekey curve confirms this transition quantitatively, increasing from one event in E1, E2, and E9 to two in E3, E4, E5, and E10, then to three in E6, E7, E8, and E11 before reaching four in E12, E13, and E17; five in E14, E15, E16, and E18; and, finally, six in E19 and E20. Panel (b) shows that this action growth is tightly aligned with the rising mean risk score, which increases from 0.20 in E1 and 0.22 in E2 to 0.53 in E12, 0.70 in E15, 0.74 in E19, and 0.77 in E20, while the rekey success rate remains consistently high, ranging from 99.8% in E1 to 97.9% in E20. This is an important result because it indicates that more aggressive adaptive control does not destabilize key-refresh execution reliability, even under severe operating pressure. Panel (c) further clarifies the decision logic by showing the staircase-like movement of dominant rekey severity from soft-only behavior in the earliest experiments toward immediately active states under medium- and high-threat conditions, then to critically activebehavior in the later scenarios, especially from E12 onward, where the controller increasingly operates in a high-alert mode. At the same time, the total rekey count rises in parallel from 1 to 6, confirming that

severity escalation and action frequency are coupled rather than independent. Panel (d) adds another important layer by showing interval compression, where the mean rekey interval drops from 18.8 in E1 and 18.1 in E2 to 10.7 in E12, 8.4 in E15, 7.7 in E19, and 7.3 in E20, meaning that the controller progressively shortens the secure-session refresh window as risk intensifies. This compression is accompanied by a rise in the mean risk score from 0.20 to 0.77, while the weighted severity index also shifts toward the upper end of the scale, confirming that the framework not only rekeys more often but also does so with more severe intervention logic as conditions worsen.

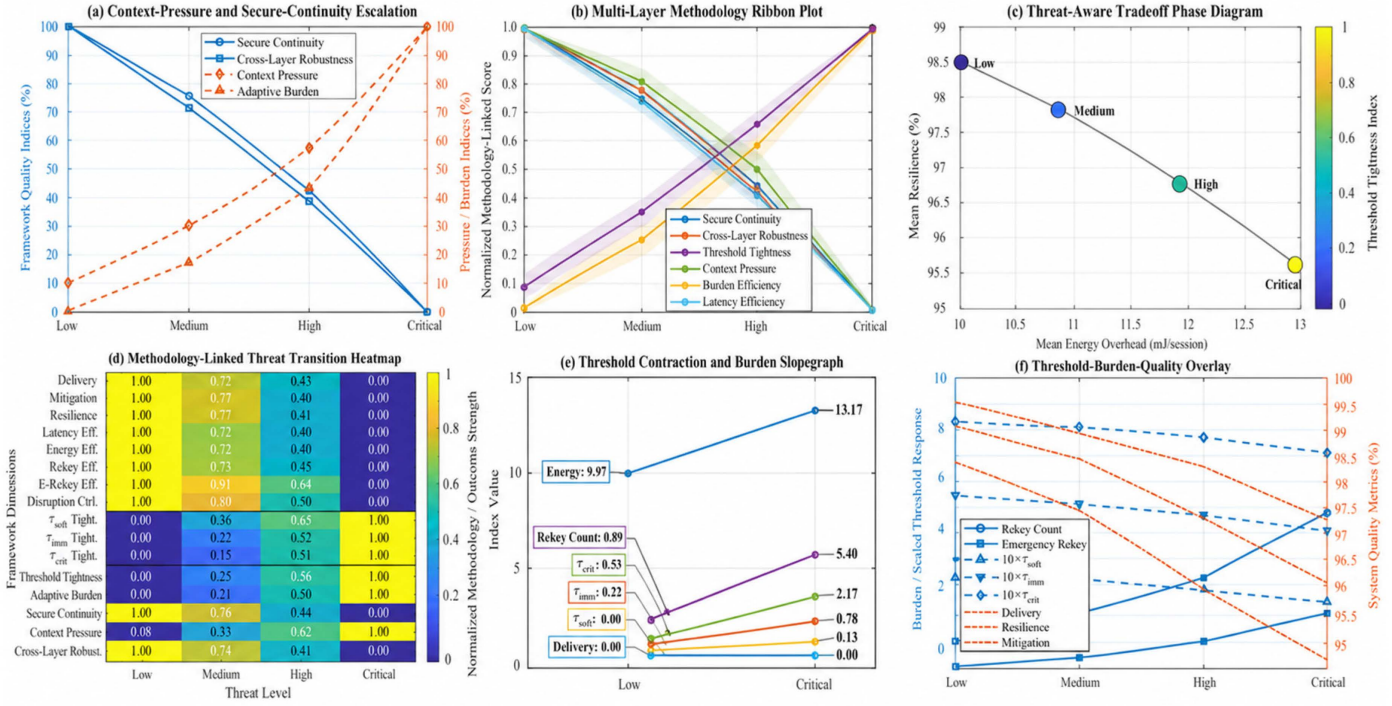


Figure 9. Threat-aware security–continuity evaluation of the proposed Ascon–ML-KEM UAV–IoT framework: (**a**) context-pressure and secure-continuity escalation, (**b**) multi-layer methodology ribbon plot, (**c**) security–energy trade-off phase diagram, (**d**) threat transition heatmap, (**e**) threshold–burden slopegraph, and (**f**) threshold–burden–quality overlay.

Figure 11 provides a focused interpretation of how the adaptive rekeying mechanism increases its intervention burden as experimental difficulty escalates while also showing that this growth in burden is accompanied by a structured transition in dominant decision severity. In panel (a), the latency-energy burden bubble plot shows a strong monotonic relationship between rekey-induced latency and rekey-induced energy overhead, indicating that the cost of adaptive protection rises in a highly coherent manner with contextual risk. The earliest experiments, such as E1, E2, and E10, occupy the lower-left region, where rekey-induced latency remains within approximately 0.31–0.42 ms and rekey-induced energy overhead remains between 0.41 and 0.52 mJ/event, corresponding to low mean risk scores around 0.20–0.34. As the experiments move toward higher-risk conditions, the burden increases progressively, with intermediate cases such as E6 and E17 reaching 0.52 and 0.67 ms latency and 0.65 and 0.83 mJ/event energy overhead, respectively, while the most demanding late-stage scenarios, especially E14, E19, and E20, rise to 0.78–0.96 ms latency and 0.95–1.16 mJ/event energy overhead. The color gradient further confirms that this increase in burden is directly associated with the rising mean risk score, progressing from approximately 0.20 in E1 to 0.77 in E20. Panel (b) complements this quantitative trend by revealing the structural evolution of dominant rekey severity across grouped experimental stages. In the earliest stages (E1–E5), the decision profile is still strongly

influenced by soft-only behavior, with a limited transition toward immediately active control. In E6–E10, immediately active behavior becomes more prominent, although a residual soft-only component remains present. By E11–E15, the balance shifts further toward critically active control, and in the final stage (E16–E20), critically active severity becomes clearly dominant, while soft-only behavior disappears and immediately active influence is reduced to a secondary role. This progression is important because it shows that the controller does not merely increase rekey cost numerically but also reorganizes its decision structure qualitatively as mission pressure intensifies.

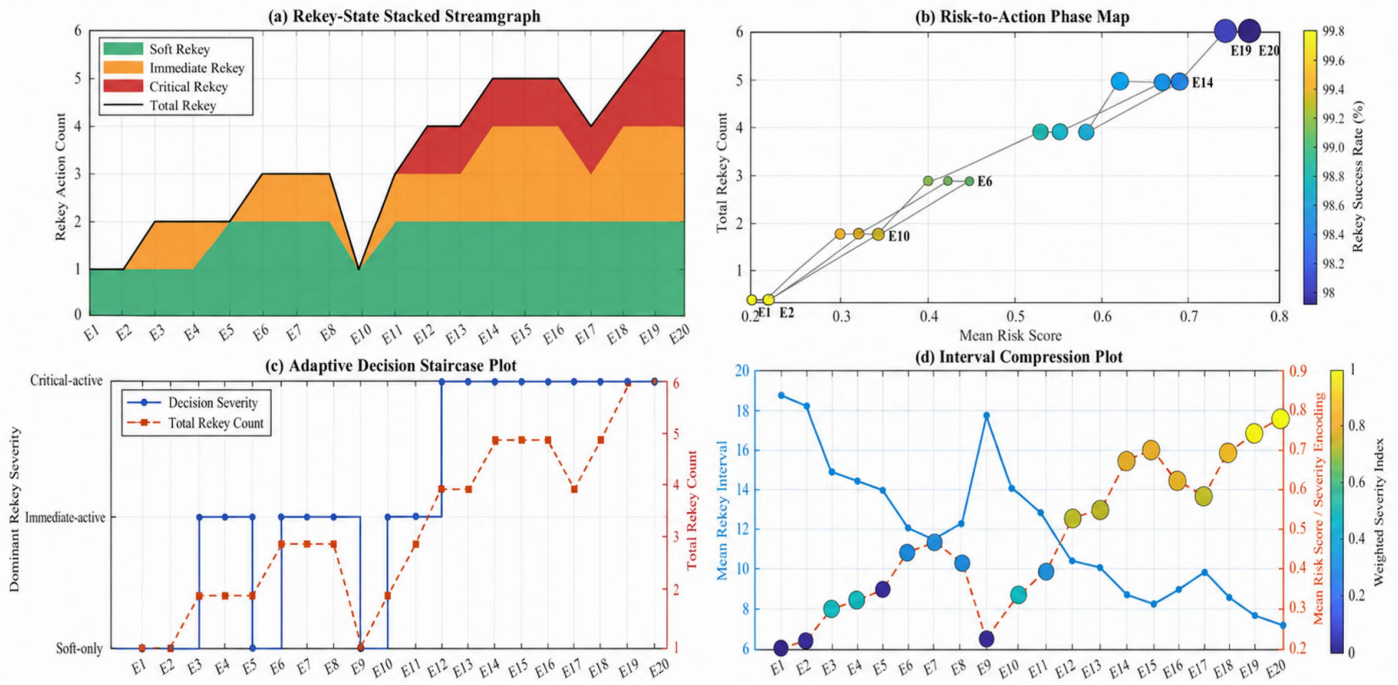


Figure 10. Risk-aware adaptive rekeying evaluation of the proposed Ascon–ML-KEM UAV–IoT framework: (**a**) rekey-state streamgraph, (**b**) risk-to-action phase map, (**c**) decision staircase Plot, and (**d**) rekey-interval compression plot.

Table 10 demonstrates that the proposed Ascon–ML-KEM + AI-driven rekeying framework achieves the lowest overall cryptographic session cost while preserving the full hybrid security pipeline, which confirms that its performance advantage is not limited to one isolated stage but is distributed across the complete communication lifecycle. In particular, the proposed method records the smallest total session overhead of 8.92 ms, clearly outperforming the conventional symmetric scheme at 11.51 ms, the static hybrid PQC scheme at 13.26 ms, and the hybrid scheme with fixed rekeying at 11.49 ms. This reduction is mainly driven by the lower execution time of the lightweight authenticated protection stages, with Ascon encryption and decryption requiring only 2.01 ms and 1.90 ms, compared with 4.02 ms and 3.79 ms for the conventional symmetric scheme, 3.34 ms and 3.18 ms for the static hybrid PQC baseline, and 2.81 ms and 2.67 ms for the fixed-rekey hybrid method. The proposed framework also achieves the lowest authentication time of 0.78 ms, the lowest key derivation time of 0.18 ms, the lowest verification time of 0.81 ms, and the lowest rekeying time of 0.69 ms, whereas the corresponding values remain higher, at 0.84–0.93 ms, 0.19–0.25 ms, 0.96–1.15 ms, and 1.01–1.52 ms for the baseline schemes. Although the ML-KEM encapsulation and decapsulation stages remain naturally present in the proposed hybrid design, at 1.21 ms and 1.34 ms, they are still lower than those of the static hybrid PQC scheme, which requires 1.52 ms and 1.66 ms, and the fixed-rekey

hybrid scheme, which requires 1.39 ms and 1.53 ms, indicating that the post-quantum key establishment component is integrated in a more computationally efficient manner.

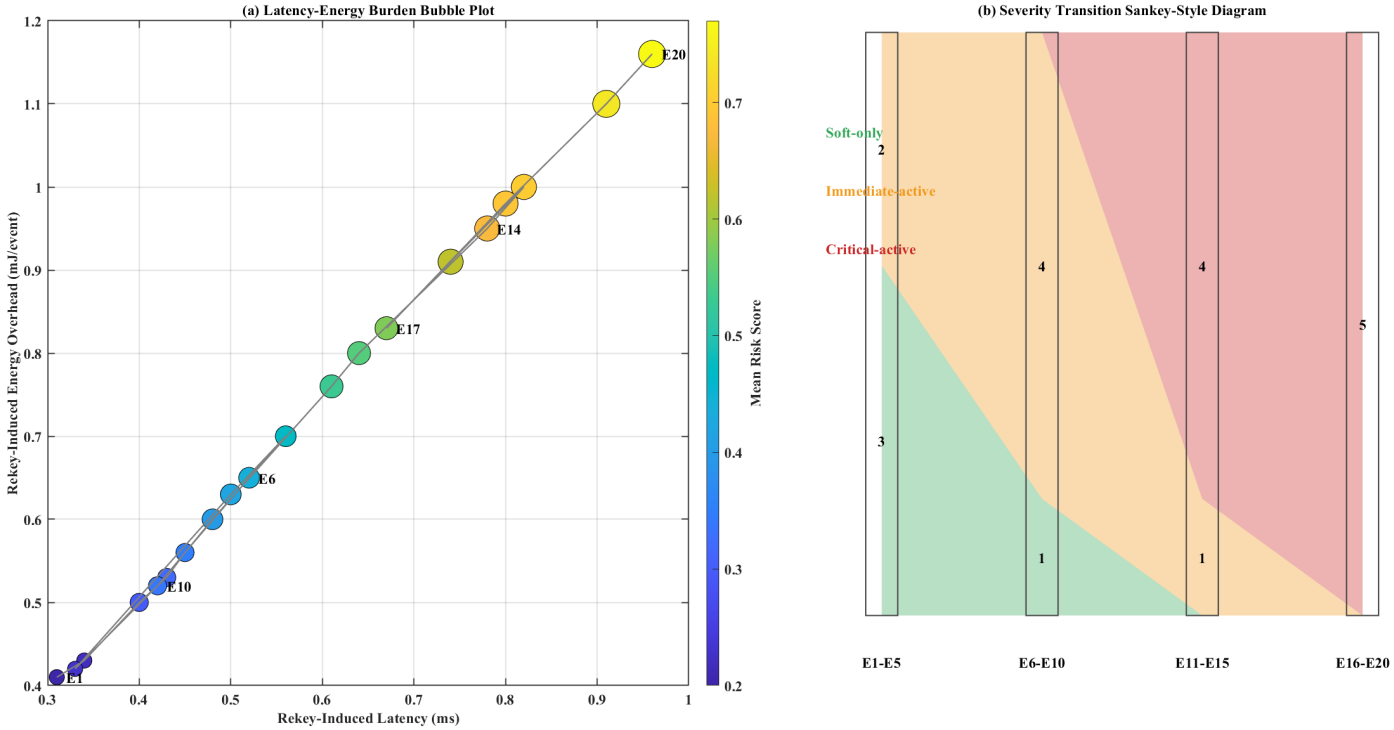


Figure 11. Analysis of the risk-aware rekeying burden of the proposed Ascon–ML-KEM UAV–IoT framework: (**a**) latency–energy burden bubble plot and (**b**) Sankey-style severity-transition diagram.

Table 10. Communication-stage cryptographic overhead decomposition.

Scenario/Method	Authentication Time (ms)	ML-KEM Encapsulation Time (ms)	ML-KEM Decapsulation Time (ms)	Key Derivation Time (ms)	Ascon Encryption Time (ms)	Ascon Decryption Time (ms)	Verification Time (ms)	Rekeying Time (ms)	Total Session Overhead (ms)
Conventional Symmetric Scheme	0.84	0.00	0.00	0.19	4.02	3.79	1.15	1.52	11.51
Static Hybrid PQC Scheme	0.93	1.52	1.66	0.25	3.34	3.18	1.05	1.33	13.26
Hybrid Scheme with Fixed Rekeying	0.89	1.39	1.53	0.23	2.81	2.67	0.96	1.01	11.49
Proposed Ascon–ML-KEM + AI-Driven Rekeying Framework	0.78	1.21	1.34	0.18	2.01	1.90	0.81	0.69	8.92

Figure 12 provides a focused view of how the proposed framework retains its core security and communication qualities as the operating condition shifts from low to critical threat, clearly showing that the degradation pattern remains gradual, structured, and operationally manageable rather than abrupt. In panel (a), the dumbbell comparison indicates that, relative to the low-threat reference state fixed at 100%, the framework preserves 98.2% of secure delivery, 97.6% of mitigation effectiveness, and 96.9% of resilience under critical conditions, which confirms that the most important protection-oriented metrics remain very high, even under maximum stress. By contrast, latency retention drops to 78.0%, and energy retention drops to 75.7%, showing that the main penalties of escalation are borne by efficiency-related dimensions rather than by security collapse, while disruption-related burden and rekey-related burden move fully toward the critical-response side, reflecting the activation of stronger protective control. The same tendency is reinforced in panel (b), where the diverging-bar view shows that the performance loss from the low-threat state increases progressively from medium to high, then to critical threat across all dimensions, but the largest contractions occur in latency, energy, rekey burden, and disruption control, whereas secure delivery, mitigation, and resilience remain comparatively less affected. Panel (c) makes this transition especially clear by tracing the

threat trajectory in the latency–resilience plane, where the framework moves from the low-threat point at approximately 7.63 ms latency and 98.53% resilience to the medium-threat point at 8.24 ms and 97.82%, then to the high-threat point at 8.93 ms and 96.72%, and, finally, to the critical-threat point at 9.78 ms and 95.47%. This connected progression shows a smooth and nearly monotonic tradeoff path, meaning that each escalation stage imposes a measured increase in delay, together with a moderate reduction in resilience, rather than producing unstable behavior.

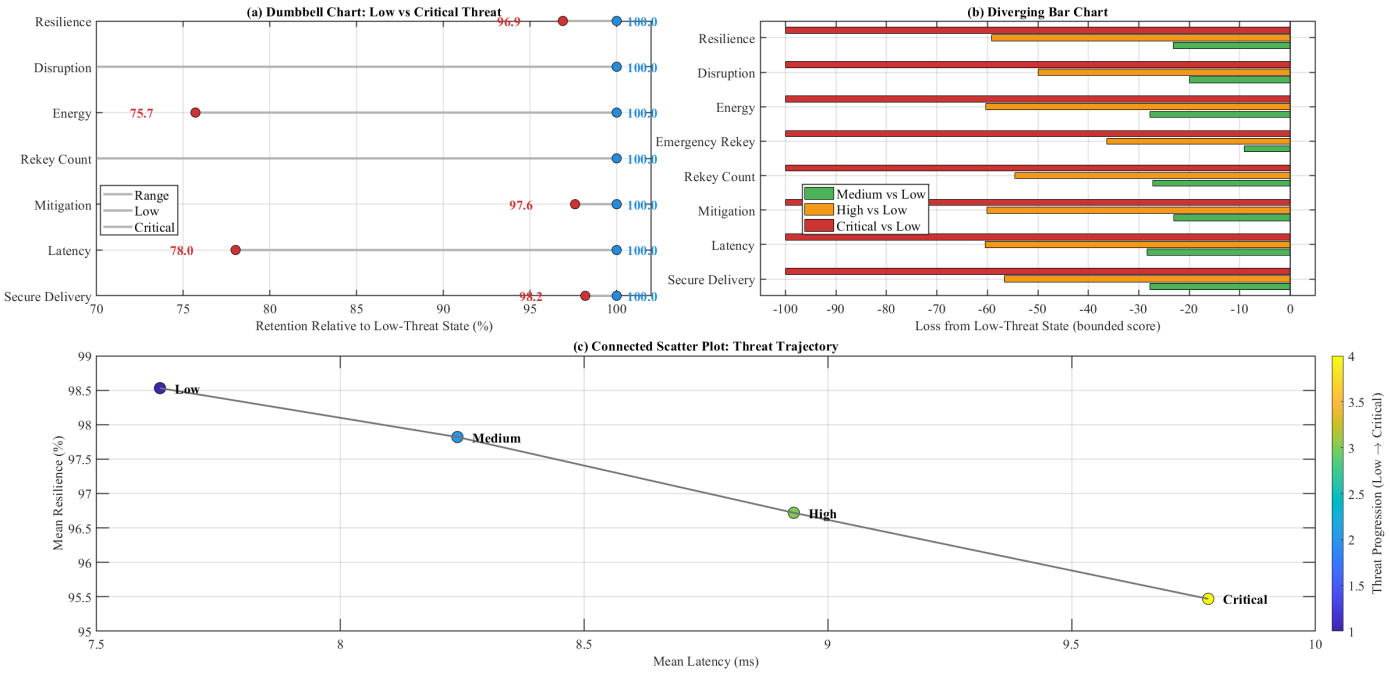


Figure 12. Threat-driven resilience and performance degradation analysis of the proposed Ascon–ML-KEM UAV–IoT framework: (**a**) low-vs-critical threat dumbbell chart, (**b**) diverging metric-loss bar chart, and (**c**) latency–resilience threat-trajectory scatter plot.

Figure 13 presents a detailed stage-wise trend analysis of how the proposed framework reorganizes its control behavior and system quality as threat severity progresses from low to critical, and it shows a highly coherent pattern in which defensive burden increases while communication quality degrades in a gradual and interpretable manner. In the first row, the security-control burden rises steadily with escalation: the mean rekey count increases from 1.00 under low threat to 2.20 under medium threat, 3.40 under high threat, and 5.40 under critical threat, while emergency rekeying grows from 0.00 to 0.20, 0.80, and 2.20, confirming that more urgent protection is activated only as the environment becomes substantially more hostile. This increase is accompanied by a corresponding rises in energy overhead from 9.97 to 10.86, 11.90, and 13.17 mJ/session and in session the disruption rate from 0.50% to 0.70%, 1.00%, and 1.50%, indicating that the framework absorbs escalating risk primarily through controlled cryptographic effort and moderate continuity cost. The second row further clarifies the adaptive control mechanism by showing progressive contraction of the rekey thresholds, with τ_{soft} decreasing from 0.34 to 0.31, 0.29, and 0.26; τ_{imm} declining from 0.59 to 0.57, 0.54, and 0.48; and τ_{crit} tightening from 0.84 to 0.83, 0.79, and 0.73, while the overall threshold-tightness index increases from 0.00 under low threat to 0.23 under medium threat, 0.56 under high threat, and 1.00 under critical threat. This means that the controller becomes progressively less tolerant of risk as threat conditions intensify, allowing rekey intervention to be triggered earlier and more aggressively. The third row shows the resulting quality tradeoff, with secure continuity decreasing from 1.00 under low threat to 0.76 under medium threat, 0.44 under high threat, and 0.00 at the normalized

critical endpoint; adaptive burden rising in parallel from 0.00 to 0.21, 0.50, and 1.00; cross-layer robustness contracting from 1.00 to 0.74, 0.41, and 0.00; and latency efficiency falling from 1.00 to 0.72, 0.40, and 0.00. These trends are particularly important because they show that the proposed framework does not react to escalating threat in a random or unstable way; instead, it follows a structured control policy in which tighter thresholds, more frequent rekeying, and higher adaptive burden are used to preserve security under harsher conditions, even though this inevitably reduces efficiency-oriented indicators.

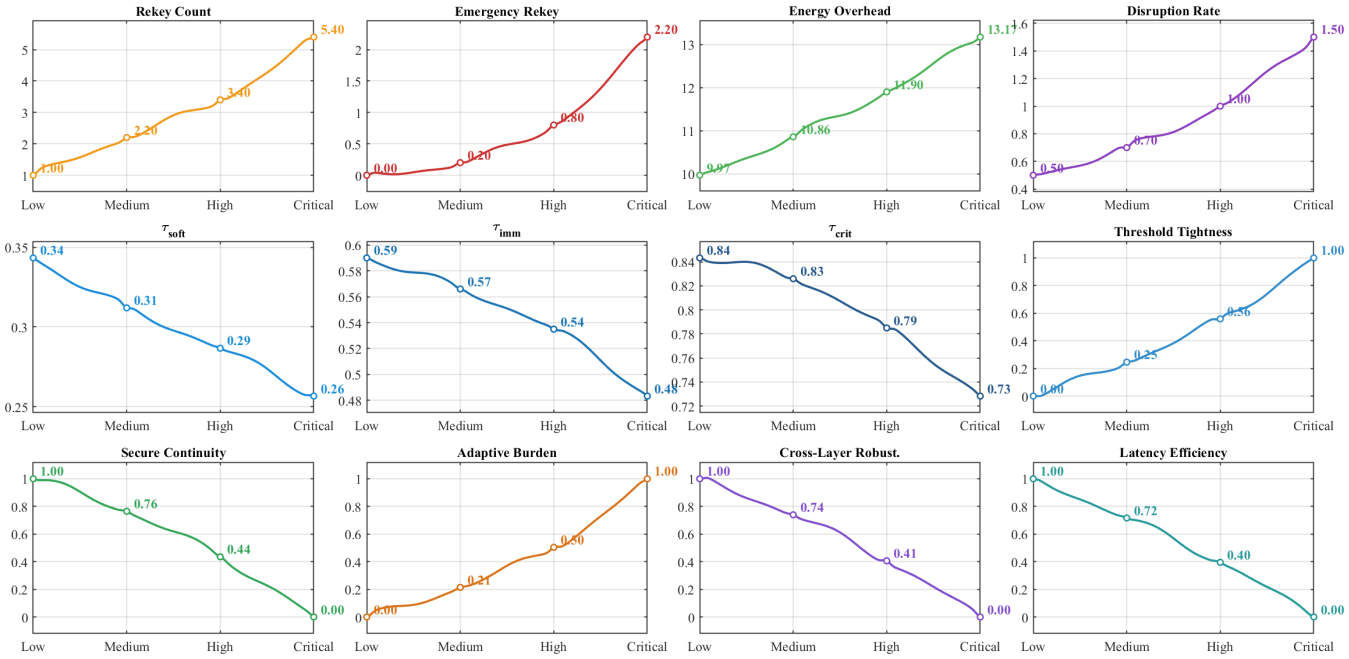


Figure 13. Threat-level trend analysis of rekeying, threshold contraction, burden escalation, and secure-continuity degradation.

5. Conclusions and Future Work

This paper presents an energy-aware hybrid cryptographic architecture for secure and low-latency UAV–IoT mission communications, designed to address the growing need for lightweight yet quantum-resilient protection in dynamic aerial–terrestrial environments. The proposed framework unifies three tightly coupled capabilities within one cross-layer security design: Ascon-based authenticated encryption for efficient payload protection, ML-KEM-based post-quantum session-key establishment for long-term cryptographic resilience, and an AI-driven adaptive rekeying mechanism for context-aware security control. Unlike conventional approaches that rely on static protection policies or fixed rekeying schedules, the proposed method continuously interprets the threat level, residual energy, mobility state, channel stability, anomaly density, traffic sensitivity, and mission urgency to adapt security behavior in real time. Experimental evaluation across twenty progressively demanding scenarios confirmed that the framework maintains strong secure-delivery performance, high attack mitigation effectiveness, low end-to-end latency, reduced energy and rekeying overhead, and robust session resilience under heterogeneous UAV-to-ground, UAV-to-UAV, and UAV-to-sensor communication conditions. These results demonstrate that the proposed architecture can balance lightweight operation, adaptive defense, and post-quantum security in simulation-based mission-critical UAV–IoT environments. Although the obtained results provide useful comparative evidence, the present evaluation remains simulation-based and does not yet include real UAV hardware, physical radio-channel measurements, or embedded cryptographic testbeds. Therefore, future

work will prioritize hardware-in-the-loop validation using representative UAV communication modules, embedded processors, low-power radio transceivers, and external power-measurement equipment to quantify real encryption latency, ML-KEM key-establishment delay, rekeying cost, energy consumption, packet-delivery behavior, and battery-level impact under realistic channel conditions. The hardware-oriented UAV and post-quantum communication studies discussed in the literature will be used as calibration references for realistic energy and latency ranges during this deployment-oriented validation stage. In addition, the current simulator adopts an idealized channel abstraction and does not explicitly capture hardware interruption latency, operating-system scheduling jitter, cache behavior, memory-bus contention, radio-transceiver startup delay, or nonlinear battery-discharge dynamics. It also represents UAV mobility at the scenario level rather than through full three-dimensional flight trajectories with wind disturbances, aerodynamic effects, and trajectory-dependent fading. Future validation will therefore calibrate the simulation model using real UAV wireless-channel traces and flight logs, incorporate 3D mobility and wind-aware trajectory models, and compare simulation-level latency, throughput, energy, and rekeying indicators against hardware-based measurements from UAV-class embedded platforms. Future work may extend the framework in several additional directions. First, more advanced learning models can be incorporated into the adaptive rekeying engine to support predictive threat anticipation and self-optimizing policy adaptation. Second, future studies may investigate federated or distributed secure coordination across larger UAV swarms, as well as integration with routing, trust management, and edge intelligence layers. Finally, broader benchmarking under additional post-quantum schemes, mobility regimes, and mission domains would further strengthen the generalizability of the proposed framework.

Author Contributions: Conceptualization, N.Y.A.-T., M.A. and M.Q.A.-J.; methodology, M.A., M.Q.A.-J. and A.A.; software, M.A. and M.Q.A.-J.; validation, N.Y.A.-T., A.A., S.A.A. and N.H.A.; formal analysis, M.A., M.Q.A.-J. and K.H.A.; investigation, N.Y.A.-T., M.A., A.A. and M.K.A.; resources, S.A.A., N.H.A., K.H.A. and M.K.A.; data curation, M.A., M.Q.A.-J. and A.A.; writing—original draft preparation, N.Y.A.-T., M.A. and M.Q.A.-J.; writing—review and editing, A.A., S.A.A., N.H.A., K.H.A. and M.K.A.; visualization, M.A. and M.Q.A.-J.; supervision, M.Q.A.-J., A.A. and S.A.A.; project administration, M.Q.A.-J. and S.A.A.; funding acquisition, S.A.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Deanship of Scientific Research at Northern Border University, Arar, KSA, under project number NBU-FFR-2026-2119-06.

Data Availability Statement: The generated cryptographic benchmarking dataset supporting the findings of this study is available from the corresponding author upon reasonable request.

Acknowledgments: The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA, for funding this research work.

Conflicts of Interest: The authors declare no competing interests.

References

1. Viradia, V.; Jain, A.; Ogety, S.S.; Donvir, A. Resilient Cloud Computing Systems for Mission-Critical Applications. In *Proceedings of the 2025 IEEE International Conference on Electro Information Technology (eIT)*; IEEE: Piscataway, NJ, USA, 2025; pp. 311–315.
2. Granelli, F.; Lu, Y.-P.; Wu, Q.; Yuan, Z.; Abdalla, A.S.; Marojevic, V.; Jiang, Y.; Afghah, F.; Geraci, G.; Mukherjee, A.; et al. A Survey on Unmanned Aerial Vehicles (UAVs) Communications: State-of-the-Art, Existing Standards and Future Directions. *IEEE Open J. Commun. Soc.* **2026**, *7*, 3000–3045. [CrossRef]
3. Al-Kamali, F.; Chan, F.; Ammar, H.A.; Bayes, J.H.; D'Amours, C. UAV-Mounted Aerial Relays in Military Communications: A Comprehensive Survey. *IEEE Open J. Commun. Soc.* **2026**, *7*, 1096–1136. [CrossRef]

4. Ahmed, M.; Nasir, A.A.; Masood, M.; Memon, K.A.; Qureshi, K.K.; Khan, F.; Khan, W.U.; Xu, F.; Han, Z. Advancements in UAV-Based Integrated Sensing and Communication: A Comprehensive Survey. *arXiv* **2025**, arXiv:2501.06526.
5. Pradhan, A.; Das, S.; Piran, M.J.; Han, Z. A Survey on Security of Ultra/Hyper Reliable Low Latency Communication: Recent Advancements, Challenges, and Future Directions. *arXiv* **2024**, arXiv:2404.08160.
6. Atebawone, E.; Akromond, R. Communication-Efficient Protocol Designs for Wireless Federated Learning: A PRISMA-Guided Systematic Review. *Wirel. Pers. Commun.* **2026**, *146*, 2019–2060. [CrossRef]
7. Gao, W.; Liu, C.; Shu, F. Security Capacity Analysis of Wireless Sensor Data Transmission in UAV-Aided IoT Systems. *IEEE J. Sel. Areas Commun.* **2026**, *44*, 4011–4022. [CrossRef]
8. Alsulieman, R.; Escobar, E.H.; Swilley, R.; Sherif, A.; Khalil, K.; Elsersy, M.; Abdelfattah, R. Hardware Implementation-Based Lightweight Privacy-Preserving Authentication Scheme for Internet of Drones Using Physically Unclonable Function. *Sensors* **2026**, *26*, 2224. [CrossRef] [PubMed]
9. Aljamal, M.; Khassawneh, B.S.; Alsarhan, A.; Okour, S.; Almusfar, L.A.; AlThani, B.F.; Aldossary, W. A Novel Dual-Layer Quantum-Resilient Encryption Strategy for UAV-Cloud Communication Using Adaptive Lightweight Ciphers and Hybrid ECC-PQC. *Computers* **2026**, *15*, 101. [CrossRef]
10. Gușiță, B.; Anton, A.A.; Stângaciu, C.S.; Stănescu, D.; Găină, L.I.; Micea, M.V. Securing IoT Edge: A Survey on Lightweight Cryptography, Anonymous Routing and Communication Protocol Enhancements. *Int. J. Inf. Secur.* **2025**, *24*, 149. [CrossRef]
11. AL Ajmi, N.A.; Shoaib, M. A Comparative Review of Quantum Neural Networks and Classical Machine Learning for Cardiovascular Disease Risk Prediction. *Computers* **2026**, *15*, 102. [CrossRef]
12. Awan, K.A.; Uddin, M.; Althobaiti, M.M.; Alaidaros, H.; Alsalman, D.; Farouk, A. TUB-IoT: Quantum Trust-Based Big Data UAV Architecture for Security-Centric Internet of Things. *IEEE Open J. Commun. Soc.* **2026**, *7*, 1235–1248. [CrossRef]
13. Nagy, N.; Alnemer, S.; Alshuhail, L.M.; Alobiad, H.; Almulla, T.; Alrumaihi, F.A.; Ghadra, N.; Nagy, M. Module-Lattice-Based Key-Encapsulation Mechanism Performance Measurements. *Sci* **2025**, *7*, 91. [CrossRef]
14. Kempf, M.; Gauder, N.; Jaeger, B.; Zirngibl, J.; Carle, G. A Quantum of QUIC: Dissecting Cryptography with Post-Quantum Insights. *arXiv* **2024**, arXiv:2405.09264.
15. Zheng, J.; Zhu, H.; Dong, Y.; Song, Z.; Zhang, Z.; Yang, Y.; Zhao, Y. Faster Post-Quantum TLS 1.3 Based on ML-KEM: Implementation and Assessment. *arXiv* **2024**, arXiv:2404.13544.
16. Zhang, Q.; He, Y.; Xiao, Y.; Zhang, X.; Song, C. OTA-Key: Over the Air Key Management for Flexible and Reliable IoT Device Provision. *arXiv* **2024**, arXiv:2412.11564.
17. Rahmati, M.; Rahmati, N. Lightweight Post-Quantum Cryptographic Frameworks for Real-Time Secure Communications in IoT Edge Networks. *Telecommun. Syst.* **2025**, *88*, 22. [CrossRef]
18. Turan, M.S.; McKay, K.; Kang, J.; Kelsey, J.; Chang, D. *Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions*; NIST Special Publication 800-232; National Institute of Standards and Technology: Gaithersburg, MA, USA, 2025.
19. Kaur, J.; Cintas Canto, A.; Mozaffari Kermani, M.; Azarderakhsh, R. A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Cryptography Standard. *arXiv* **2023**, arXiv:2304.06222.
20. Martalò, M.; Pettorru, G.; Atzori, L. A cross-layer Survey on Secure and Low-Latency Communications in Next-Generation IoT. *IEEE Trans. Netw. Serv. Manag.* **2024**, *21*, 4669–4685. [CrossRef]
21. Banerjee, A. Securing the Future: AI-Driven Data Transmission in IoT-Powered Smart Cities. *Soft Comput. Fusion Appl.* **2025**, *2*, 33–53.
22. Zhaxygulova, D.; Iavich, M.; Rakhmetullina, S.; Alipbayev, K. Secure and Energy-Aware Cryptographic Framework for IoT-Enabled UAV Systems. *Symmetry* **2025**, *17*, 1987.
23. Sarkar, S.; Shafaei, S.; Jones, T.S.; Totaro, M.W. Secure Communication in Drone Networks: A Comprehensive Survey of Lightweight Encryption and Key Management Techniques. *Drones* **2025**, *9*, 583. [CrossRef]
24. Hafeez, S.; Abro, G.E.M.; Mustafa, H. Quantum-Resilient Threat Modelling for Secure RIS-Assisted ISAC in 6G UAV Corridors. *arXiv* **2025**, arXiv:2510.25411.
25. Aissaoui, R.; Deneuville, J.-C.; Guerber, C.; Pirovano, A. Evaluating Post-Quantum Key Exchange Mechanisms for UAV Communication Security. In *2024 AIAA DATC/IEEE 43rd Digital Avionics Systems Conference (DASC)*; IEEE: Piscataway, NJ, USA, 2024; pp. 1–10.
26. Khan, M.A.; Javaid, S.; Mohsan, S.A.H.; Tanveer, M.; Ullah, I. Future-Proofing Security for UAVs with Post-Quantum Cryptography: A Review. *IEEE Open J. Commun. Soc.* **2024**, *5*, 6849–6871. [CrossRef]
27. Hoque, S.; Aydeger, A.; Zeydan, E.; Liyanage, M. Analysis of Post-Quantum Cryptography in User Equipment in 5G and Beyond. In *2025 IEEE 50th Conference on Local Computer Networks (LCN)*; IEEE: Piscataway, NJ, USA, 2025; pp. 1–9.
28. Mahdi, L.H.; Abdullah, A.A. A Hybrid Post-Quantum Cryptographic Framework Integrating Kyber-512 and ASCON for Secure IoT Communications. *Eng. Technol. Appl. Sci. Res.* **2025**, *15*, 26527–26533. [CrossRef]

29. Rakshit, H.; Bhandari, R.; Banerjee, S. Lightweight Session-Key Rekeying Framework for Secure IoT-Edge Communication. *arXiv* **2025**, arXiv:2511.02924.
30. Mondal, M.S.; Ramasamy, S.; Rownak, R.; Russo, L.; Humann, J.D.; Dotterweich, J.M.; Bhounsule, P. Risk-Aware Energy-Constrained UAV-UGV Cooperative Routing Using Attention-Guided Reinforcement Learning. In *2025 IEEE International Conference on Robotics and Automation (ICRA)*; IEEE: Piscataway, NJ, USA, 2025; pp. 13000–13006.
31. Zhang, C.; Liu, D.; Liu, X.; Zou, X.; Niu, G.; Liu, B.; Jiang, Q. Towards Efficient Hardware Implementation of NTT for Kyber on FPGAs. In *Proceedings of the 2021 IEEE International Symposium on Circuits and Systems (ISCAS), Daegu, Korea, 22–28 May 2021*; IEEE: Piscataway, NJ, USA, 2021. [CrossRef]
32. Di Matteo, S.; Sarno, I.; Valea, E.; Saponara, S. KEM-22: An Efficient Post-Quantum ML-KEM Hardware Accelerator on 22-nm ASIC. *IEEE Internet Things J.* **2026**, *13*, 4715–4726. [CrossRef]
33. Xing, Y.; Li, S. A Compact Hardware Implementation of CCA-Secure Key Exchange Mechanism CRYSTALS-KYBER on FPGA. *Cryptogr. Hardw. Embed. Syst.* **2021**, *2021*, 328–356. [CrossRef]
34. Louzi, N.; AlJamal, M.; Al-Jamal, M.Q. Learning the City's Hidden Danger: A Continuous Hazard Field Intelligence Framework for Traffic Accident Emergence and Urban Safety Prediction. *Urban Sci.* **2026**, *10*, 300. [CrossRef]
35. Hayajneh, M.T.; AL-Oqla, F.M.; AL-Jamal, M.Q. Statistical modeling and optimization of the mechanical performance of natural fiber-reinforced polyolefin composites by applying response surface methodology. *J. Compos. Mater.* **2026**, 1–24. [CrossRef]
36. Al-Jamal, M.Q.; Alsarhan, A.; AlJamal, M.; Aljamal, Q.; Khassawneh, B.S.; Salhi, A.; Hayat, H. Integrating Generative Design and Artificial Intelligence for Optimized Energy-Efficient Composite Facades in Next-Generation Smart Buildings. *Sustainability* **2026**, *18*, 2379. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.