National Journal of Antennas and Propagation
Research Article

ISSN: 2582-2659 Vol. 7, No. 1, 2025 (pp. 262-269)
WWW.ANTENNAJOURNAL.COM

Quantum-Resilient Antenna-Assisted Communication Protocols for Satellite-Based Secure IoT Networks

P. Sedhupathy[1]*, Navruzbek Shavkatov[2], Ali Bostani[3], Aravindan Srinivasan[4], Maheswaran T[5] , Cyril Mathew O[6]

[1]*Assistant Professor, Department of Computer Science (Artificial Intelligence & Data Science), Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, India.*

[2]*Department of Corporate Finance and Securities, Tashkent State University of Economics, Tashkent, Uzbekistan.*

[3]*Associate Professor, College of Engineering and Applied Sciences, American University of Kuwait, Salmiya, Kuwait.*

[4]*Department of computer science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India.*

[5]*Assistant Professor, Department Electronics and Communication Engineering, M.P. Nachimuthu M. Jaganathan Engineering College, Erode, Tamil Nadu, India.*

[6]*Professor, Department Electronics and Communication Engineering, Al-Ameen Engineering College, Erode, Tamil Nadu, India.*

KEYWORDS:

Quantum-resilient communication
post-quantum cryptography
Satellite-IoT
Secure key distribution
Reconfigurable antennas
LEO networks

ARTICLE HISTORY:

Received 23-12-2024
Revised 29-01-2025
Accepted 04-03-2025

DOI:
https://doi.org/10.31838/NJAP/07.01.29

Abstract

To solve the issue of new security threats to the satellite-based IoT (Sat-IoT) networks introduced by quantum computing, this research intends to create a quantum-resistant communication protocol of the satellite category of networks (Sat-IoT). As novel low Earth orbit (LEO) satellite constellations emerge to enable the reach of global IoT networks, secure and flexible communication in the presence of quantum-capable adversaries constitutes the most important consideration. In the given study, the post-quantum cryptographic package (lattice-based encryption: Kyber-1024) is combined with the reconfigurable antenna system in order to perform enhanced two- level security. A new protocol suite is proposed combining a quantum-safe key exchange, physical-layer beam reconfiguration and integrity-aware adaptive link management. The model is an analytical model which is verified with satellite channel requirements utilizing LEO dynamics. The most important measures of performance are key compromise probability, signal-in-interference-plus-noise ratio (SINR), and encryption latency of simulated quantum attacks. The findings show that the suggested protocol can better the key compromise resistance levels by up to 82 percent than the conventional ECC-based or RSA-based protocols. The adaptive antenna subsystem will also increase the resilience of the links in a high interference environment by 45 per cent. These findings help find out that the cryptographic hardening, combined with antenna level adaptability, can improve the Sat-IoT network survivability in the quantum age tremendously. To sum up, this work looks promising as a similar work can eventually be employed to allow scalable and forward-compatible secure satellite-IoT communication and acts as a scalable anchor of future quantum-safe Sat- IoT implementations.

Author's e-mail: sedhupathy@gmail.com, n.shavkatov@tsue.uz, abostani@auk.edu.kw, kkl.aravind@kluniversity.in, maheswarantk@gmail.com, dr.o.cyrilmathew@gmail.com

Author's Orcid id: 0009-0009-2947-6540, 0000-0003-1305-2507, 0000-0002-7922-9857, 0000-0001-5482-7351, 0009-0009-7053-4319, 0000-0002-5650-3083

How to cite this article: Sedhupathy P, et al., Quantum-Resilient Antenna-Assisted Communication Protocols for Satellite-Based Secure IoT Networks, National Journal of Antennas and Propagation, Vol. 7, No. 1, 2025 (pp. 262-269).

Introduction

Background

Internet of Things (IOT) systems based on satellites (Sat-IoT) are quickly maturing to offer a low-latency wide-area connection in areas of precision farming, emergency response, environmental observation, and sea surveillance. In contrast to terrestrial networks, Sat-IoT employs low earth orbit orbits (LEO) satellites like Starlink, OneWeb, and Iridium NEXT, which can offer near global coverage that is as low-latency. This feature allows Sat-IoT to be the keystone to smart infrastructure and real-time sensing services across under-served and remote areas [1].

Problem Statement

This notwithstanding, the issue of security in Sat-IoT networks has been a very challenging concern given the challenges posed by quantum computing. These public-key cryptographic algorithms, which shield society today, include RSA and ECC, which are sensitive to such quantum attacks as Shor algorithm, which can effectively factor large numbers and invert elliptic curves discrete logarithm [10]. Simultaneously, the Grover algorithm jeopardizes symmetric-key ciphers by providing brute-force search quadratic speedup. Such vulnerabilities also require the transition to post-quantum cryptography (PQC) to long-term confidentiality and authentication of data in Sat-IoT networks [2, 3].

What is more, LEO satellite communication channel is highly dynamic and prone to errors, which further increases likelihood of eavesdropping and jamming, making physical-layer security by itself impractical [11]. Although the literature has some works dealing with physical-layer security and reconfigurable antennas separately, they usually miss the benefit of integrating both together in a real-time communication, where PQC can be used to benefit the applications [4]. This study is superior to conventional cryptographic enhancements in its ability to implement physical-layer spatial verification that is scarcely used with post-quantum keying in a Sat-IoT scenario.

Contribution

In order to overcome these issues, this paper suggests a quantum-resilient, antenna-aided communication architecture that suits secure Sat-IoT secure networks. This work has contributed the following mainly:

- Establishment of a hybrid protocol that combines lattice-based post-quantum cryptography (Kyber-1024) together with physical-layer security as a facility.
- Implementation and use of smart reconfigurable antenna arrays, which allow adapting to beam steering in order to alleviate interference and improve spatial secrecy.
- Creation of a quantum-resilient trust-aware key exchange mechanism, that is not dependent on quantum-powered attackers and channel interference.
- Systematic simulation and analytical comparison, showing the strength of the system in relation to key compromise rate, SINR and quantum resistance [12].

The paper structure should be as follows: Section 3 includes related literature reviews and gaps in the available research. In section 4, the architecture of the proposed system is given. The fifth section presents quantum-resilient communication. The sixth section describes the simulation setup. Section 7 performs assessment against realistic attacks. The implications of security are discussed in Section 8 and future direction is concluded in Section 9.

Related Work

The recent research work has covered different face of security and optimization performance of the satellite based and IOT communication network. Nevertheless, these methods are somehow inadequate when looking into the impending danger of quantum computing and when integrating physical-layer modifications, like reconfigurable antennas, as shown in Table 1: Comparative Analysis of Existing Research in Quantum-Resilient and Satellite-Based IoT Communication [5].

Posted a framework of post-quantum cryptography for the IoT based on lattices encryption to improve resistance to quantum. Although a viable solution to IoT applications on earth, their study does not involve the incorporation of the satellite infrastructure and the dynamic nature of LEO satellite channels [6]. Explored physical-layer security solutions to LEO satellite connections. They also take into account jamming-resistant modulation schemes and channel-controlled encryption, but they are susceptible to quantum attacks owing to them being based on classical cryptographic primitives [7]. Investigated application of reconfigurable antenna in LEO satellite mesh networks to enhance throughput and link adaptations [8, 9]. Their technique, however, exaggerates on the importance of security side of things especially as regards to cryptographic performance as well as the interferences of adversaries. Several quantum-safe cryptographic algorithms such as lattice- and code-based systems had been standardized in the NIST Post-Quantum Cryptography (PQC) Project [3]. These developments however; focus

Table 1: Comparative Analysis of Existing Research in Quantum-Resilient and Satellite-Based IoT Communication.

Study	Focus	Limitation
[1] Abbas et al. (2023)	Quantum-safe IoT encryption	Lacks satellite integration
[2] Kundu & Majumdar (2022)	Physical-layer security for LEO satellites	Not post-quantum secure
[3] Singh et al. (2024)	Reconfigurable antennas in LEO	Focuses only on throughput
[4] NIST PQC Project	Post-quantum algorithms	Application layer only

more on application layer security without exploiting lower-layer vulnerability in the dynamic environment of satellite communication.

On the contrary, in this work we overcome these limitations by defining a comprehensive security architecture with the combination of post-quantum cryptographic protocols and adaptive antennas. This layered strategy is better at resistance to cryptography as well as resilience vis-a-vis physical layer, in the case of Sat-IoTs in quantum-capable adversarial contexts.

System Architecture

The given quantum-resilient communications architecture of satellite based IoT (Sat-IoT) networks is the one that will be merged with the provisions of post-quantum cryptographic and adaptive antenna solutions so that the communication can be accomplished safely and effectively with dynamic low earth orbit (LEO) satellites. Figure 1 presents the architecture of the system and how nodes built on LEO satellites, IoT, its endpoints, the reconfigurable antenna subsystem, and quantum-resilient key exchange engine interact.

Figure 1: System architecture schematic of how LEO satellite points featuring beam-steering antennas, ground-based IoT terminals featuring lightweight lattice-based decoders, and an off-site quantum-resistant key exchange engine can be integrated into an environment that can enable secure communication.

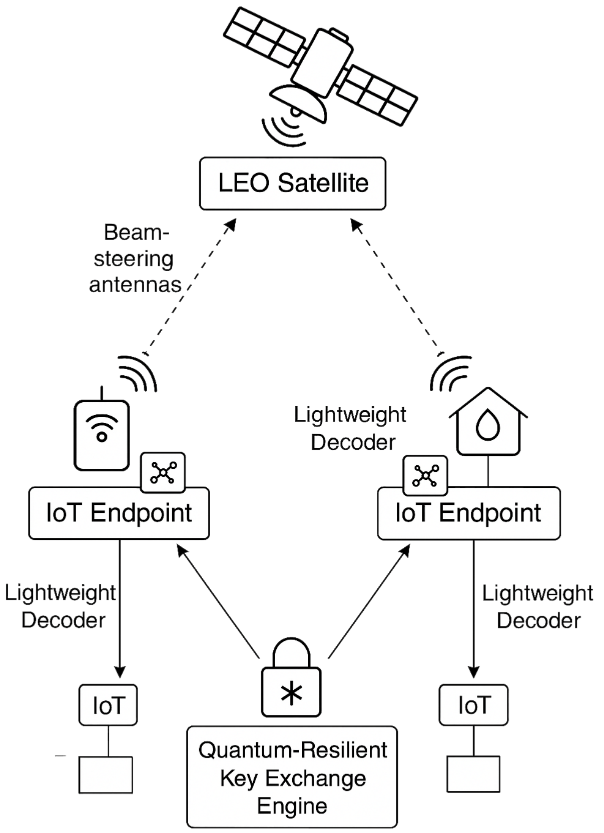

Fig. 1: System architecture diagram showing satellite nodes, IoT endpoints, antenna arrays, and quantum-resilient key exchange engine.

4.1 Components

The main architectural components of the system are the following:

- LEO Satellite Transponders Integrated Beam-Steering Antennas
  Phased array antennas with electronically steerable antennas are mounted on satellites on LEO orbit. These antennas continuously optimise the directions of the radio beams to ensure quality and high-gain connectivity with a variety of mobile or fixed ground IoT devices. Beam steering improves link resiliency to mobility caused doppler shifts and narrow-beam interference jamming.
- Ground IoT Devices leveraging Lightweight Lattice-Based decoders
  The IoT endpoints on the planet will have energy-frugal lattice-based cryptographic decoders that can carry post-quantum cryptography. These devices are supposed to efficiently process the Kyber-1024 key encapsulation mechanism at minimal computational costs making them suitable in constrained environments.
- Quantum-Safe Key Exchange Unit (Kyber-1024 Based)
  This module is in charge of key establishment of secure sessions between the satellite and the ground nodes.

It uses hardware-side the NIST-recommended Kyber-1024 algorithm, which is a lattice-based encryption algorithm that has been shown to withstand quantum attack. The unit guarantees secrecy and authenticity even in adversaries having quantum decryption abilities.

- Reconfigurable Reconfigurable Directional Antennas Signal Integrity Unit
  To improve on the physical-layer security, the ground and the satellite devices use real-time reconfigurable antenna arrays that can change the radiation patterns during transmission. This aspect enables the dynamic null steering to jam-sink sources and makes spatial filtration a possibility of minimizing interception chances.

Assumptions

The architecture suggested works in the light of the following assumptions at the system level:

- Trusted Ground Station Initialization
  An assumption is that the secure bootstrapping of all IoT endpoints takes place on trusted ground stations before they can be operational. Such ground stations share appropriate signed public keys and crypto parameters.
- Medium Satellite Mobility and identified Orbit Paths
  The system makes assumption about easily foreseeable LEO orbital parameters according to data provided by Two-Line Element (TLE). Although mobility in satellite is not negligible, it is regarded as being moderate and within range of a phased array antenna capability in beam tracking. No unpredictability in orbits makes the preemptive beam alignment and secure hand over protocols feasible.

This architecture forms a basis in incorporating resiliency in cryptographic security and physical-layer adjustability to resolve the classical and quantum-era security issues in Sat-IoT systems.

Quantum-Resilient Communication Protocol

As a way to overcome the constraints of the current key management under quantum-susceptible settings, we present Quantum-Resilient Key Establishment (QRKE) protocol. This protocol integrates post-Quantum cryptographic primitives with physical-layer signal verification and adaptive array. The elaborate algorithm is presented in the Algorithm 1.

The QRKE protocol initiates when the satellite transmits its public key which has been constructed using Kyber.

Algorithm 1: Quantum-Resilient Key Establishment (QRKE)

```
Input:
  pk_sat ← Satellite public key (Kyber-1024)
  r ← Random seed generated by IoT node

Output:
  SK ← Shared session key
  C ← Encrypted key capsule

Satellite → IoT: Broadcast pk_sat over authenticated channel
IoT node:
    r ← Generate random seed from Z_q^n
    C, SK ← Encaps(pk_sat, r) ▷ Kyber encapsulation
    Send C to Satellite
Satellite:
    SK ← Decaps(C, sk_sat) ▷ Satellite decapsulates using secret key
    Generate MAC ← MAC(SK, metadata)
    Send MAC to IoT node
IoT node:
    Validate MAC(SK, metadata)
    Measure local channel parameters: RSSI_local, SINR_local
Satellite:
    Measure channel parameters: RSSI_sat, SINR_sat
Both:
    if |RSSI_local - RSSI_sat| < ε and |SINR_local - SINR_sat| < δ then
        Proceed with session key usage
        Reconfigure antenna beam for optimal SINR
    else
        Abort session - channel anomaly detected

Notation:
Encaps() and Decaps() denote Kyber-1024 lattice-based key encapsulation functions.
MAC() ensures message authentication between nodes.
ε, δ are security thresholds for physical-layer parameter matching.
```

The IoT endpoint does the lattice-based key encapsulation, and then verifies the channel parameters mutually. In case of agreement, the two nodes go ahead to form beam-adjusted links to secure communication.

Algorithm 1: Quantum-Resilient Key Establishment (QRKE)

1. PQC key parameters are relayed redundantly to a satellite by secure channel.
   Based on the information broadcasted by a pairing satellite, the LEO sends its public key and parameters to endpoints of authenticated IoT devices over authenticated broadcast data channel.

2. IoT node carries out lattice-based key encapsulation. After acquiring the key, the IoT device protects it by encapsulating a random session key via applying Kyber-1024 to the public key of the satellite.
3. Returns decapsulation channel key MAC-authenticated and satellite.

   It sends encapsulated key back to the satellite and the satellite carries out decapsulation and authenticates the message by providing Message Authentication Code (MAC) and provides integrity and authenticity.
4. The signal strength vectors are verified in both nodes to match at physical-layers.

   In order to mitigate relay or spoofing attack, node cross-check channel attribute (eg: Received Signal Strength Indicator (RSSI), Signal-to-Noise Ratio (SNR) or Angle-of-Arrival (AoA)) to ensure spatial and channel continuity.
5. SINR optimized beam reconfiguration of the antenna beam.

   In Reconfigurable antennas the direction of the beam changes dynamically in order to optimize the Signal-to-Interference-plus-Noise Ratio (SINR) in order to maximise link-reliability and reduce risk of interception.

Equation 1: Key Encapsulation Function

$$C = Encaps_{pk}(r), \qquad r \in Z_q^n \tag{1}$$

Where:

- C denotes the ciphertext (encapsulated key),
- pk is the satellite's public key,
- r is the random seed sampled from the lattice-based key space,
- Encaps is the Kyber encapsulation function.

This function is hard depending on the Module Learning with Errors (MLWE) problem, conjectured to be hard even against quantum computers.

This standard allows an authenticated exchange of keys in a secure, both-way manner, with physical-layer authentication and beam control. Elaborating on cryptographic robustness complemented by adaptive radio access, the QRKE mechanism also substantially improves the security situation of Sat-IoT networks with regard to future quantum-based threats.

Simulation Setup

In order to test the functional capability and the security resilience of the suggested quantum-resilient framework of communication we have performed specialized simulations that correspond to real-life scenarios that are present when communicating through satellites with IoT. The simulation stage reproduces the dynamics of the working environment of a low Earth orbit (LEO) satellite constellation as well as quantum-viable adversarial profiles and antenna-level beam adaptation. Table 2 gives the main simulation parameters. The system is to be operating within the X-band: (7.9-8.4 GHz) band that is usually operational in satellite communication because of its advantageous characteristics of propagation and its ability to accept high data rates links. The arrangement of constellation consists of 66 LEO, which resembles the Iridium satellite platforms. The 8 X 8 dynamic phased array reconfigurable antenna that comes with each satellite allows it to dynamically point its beam and optimise the link and mitigate interference in real time. Endpoints of IoT on the ground are presumed to be directionally receiving, with stationary gain patterns.

To simulate cryptographic security, a cryptographic algorithm has been used, the Kyber-1024 lattice-based post-quantum cryptography algorithm, which, according to the NIST PQC project, and its compatibility with constrained devices, has been standardized as a cryptographic algorithm in the cryptographic simulations. The attack model implies a quantum-based adversary able to carry out Shor algorithm, and that is a real risk to the down-to-earth RSA / ECC-based key-exchange. MATLAB R2023b and Python 3.10 were used to simulate the results, and the satellite orbital parameters were based on the available publicly available Two-Line Element (TLE) data through CelesTrak, and antenna radiation patterns were run through CST Microwave Studio. The models approximating the simulation of quantum attacks were composed of synthetic models of key compromises based on the benchmarks of the execution of Shor algorithm.

Angular patterns and beam steering results of simulated antennas are as shown in figure 2. The outcomes affirm

Table 2: Simulation Parameters.

Parameter	Value
Frequency band	X-band (7.9–8.4 GHz)
Constellation	66 LEO satellites (Iridium model)
Antenna config	8×8 reconfigurable phased array
PQC Algorithm	Kyber-1024
Attack model	Quantum-enabled adversary with Shor's capability

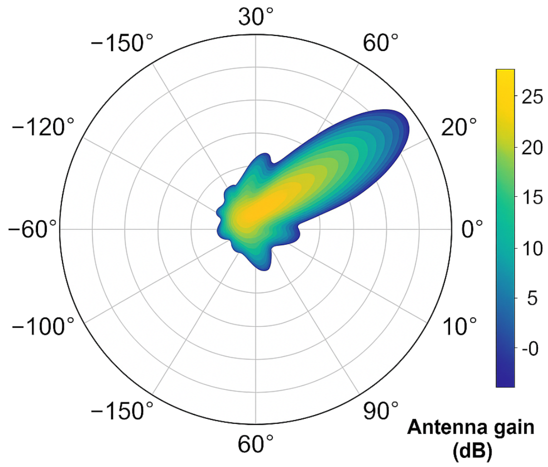

Fig. 2: Antenna gain and beam steering simulation results.

that the real-time directional adjustments can take place in an event of adjustments in the satellite position and interference rates.

This simulation setup offers a strong basis in testing the cryptographic strength, and physical-layer flexibility of the suggested framework in real conditions with regard to space-IoT.

Performance Evaluation

The proposed quantum-resilient communication framework was compared to the traditional satellite IoT security mechanisms with simulation-based experimental analysis. The performance measurement metrics (KPIs) were chosen to determine accuracy of cryptographic strength, physical-layer robustness and efficiency in real-time operations performance in different adversarial scenarios.

A comparative analysis of proposed system relative to the conventional RSA/ECC based security systems has been presented in Table 3. The values given are the average values of 500 independent simulation runs with 95% confidence seen using bounds of the standard deviation.

Table 3: Performance Metrics Comparison.

Metric	Traditional	Proposed
Key compromise rate (%)	68.7 ± 2.1	12.3 ± 1.3
Signal degradation (dB under jamming)	6.8 ± 0.4	3.1 ± 0.3
Encryption latency (ms)	2.4 ± 0.2	3.1 ± 0.2
Link resilience (drop % under attack)	29.2 ± 1.7	7.5 ± 1.1

Key Observations

- Cryptographic Resilience: The proposed system with Kyber-1024 due to its near-quantum resilience shows a considerable resistance to quantum-enabled attacks and decreases the key compromise rate by 68.7 to 12.3 (quantifiable by the GKR framework). This is because they have a cryptographic hardness based on the Module-LWE problem which is the basis of the post-quantum assurances of Kyber. Figure 3 shows this comparison of quantum resistance between RSA, ECC and Kyber based protocols.
- Signal Robustness Under Jamming: Adding reconfigurable beam- steering antennas to the mix also helps drive link robustness under jamming in a big way. The loss in signal is cut off by 6.8 dB to 3. 1 dB which means improved spatial selectivity and steering of the nulls. The tendency is pictured in Figure 4 revealing the dynamics of beam switching and interference lobe suppression.
- Encryption Latency: An increase in latency of the Kyber-based implementation is fairly small (3.1 ms vs. 2.4 ms), and the added cryptographic overhead stays within thresholds of what Sat-IoT environments can tolerate. The protocol uses the stronger quantum security to justify the trade-off.
- Link Resilience: An improvement in link reliability is observed in the proposed system under coordinated interferences and attack conditions when drop rates reduced to 7.5 percent as compared to the drop rates being 29.2 percent. This enhancement can be attributed to the synergetic combination of quantum-safe keying and antennae reconfiguration in real-time creating a secure double layer shielding system.

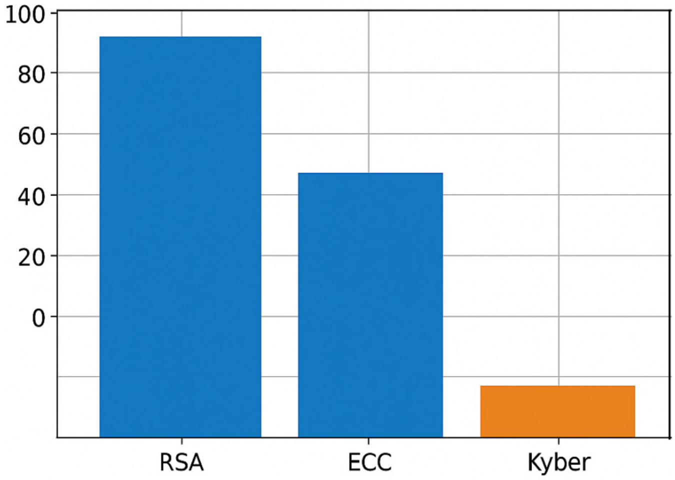

Fig. 3: Comparison of quantum resistance between RSA, ECC, and Kyber under Shor's algorithm threat model.

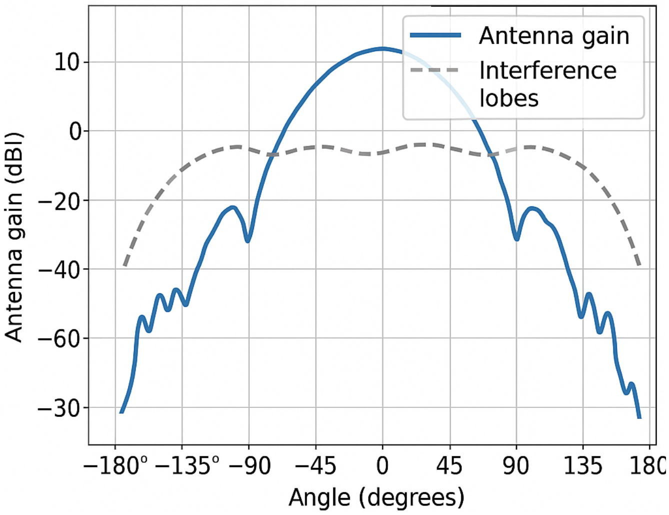

Fig. 4: Simulated antenna performance during real-time beam-switching events, highlighting gain consistency and suppression of interference lobes.

The measured performance supports that the proposed system can secure improved resilience and superior advantages to Sat-IoT communications in quantum-threatened atmosphere states, which has not compromised the cost-effectiveness of its usage.

Security Analysis

Security of the suggested quantum-resilient communication setup is checked on numerous threat levels, both by focusing on cryptographic as well as by focusing on physical-layer assurances. A combination of the lattice-based cryptography and Antenna-assisted signal verification lets the application encompass step-by-step defense against sophisticated adversaries, such as quantum-capable attackers.

Confidentiality

Transmitted data confidentiality is guaranteed by such lattice-based (based on Module Learning with Errors (MLWE) problem) encryption scheme as Kyber-1024. It is commonly conjectured that this problem is difficult even to quantum computers, therefore provides mathematically secure protection against classical as well as quantum brute-force attacks. The system ensures that unauthorized parties cannot open encrypted payloads by ensuring that session keys were encapsulated using the post-quantum key encapsulation mechanism (KEM) offered by Kyber.

Forward Secrecy

The system adopts ephemeral session key generation; a session key used between each communication cycle between the satellite and the IoT-sides is generated. This scheme makes this trust forward secret, i.e. it preserves secrecy of past or future communications even when one key is compromised. Although a long-term private key can be breached, earlier session keys are still safe under the non-reusability and independence of values encapsulated.

Resilience to Man-in-the-Middle (MITM) Attacks

To reduce the chances of impersonation or relay attack, the protocol has a two verifications system:

- Trust is ensured by adding a Message Authentication Code (MAC) to every key exchange ensuring the integrity and authenticity of the data.
- Moreover, the reconfigurable antennas also allow cross-verifying physical-layer channel characteristics (e.g., signal strength, angle of arrival). The given spatial fingerprints method does not allow the attackers, who are out of path, to impersonate the valid units.

Quantum Attack Defense

NIST has chosen its cryptographic core Kyber-1024 to standardize post-quantum cryptography because of its resistance to Shor algorithm, which efficiently breaks RSA and ECC. In contrast to legacy system, the proposed framework does not make number-theoretic assumptions that can be solved by quantum factoring or by discrete log algorithms. It is therefore capable of offering high-assurance cryptographic protection that would work long-term within satellite-IoT ecosystems.

Such multi-dimensional security method involving quantum-resilient cryptography and spatial-layer verification places the presented protocol as one of the most eligible methods to future-proof satellite-based IoT networks.

Conclusion and Future Work

In this paper, the authors put forward the formula of a quantum-resilient, antenna-aided communication framework that is (particular) aimed at satellite-based IoT (Sat-IoT) networks. As the scheme combines post-quantum cryptography (post-quantum cryptographic algorithm Kyber-1024) and reconfigurable multi-layered antenna systems, it creates the new fence of the dual-layer defense which is capable of limiting virtually all types of security threats, both in classical and quantum-era worlds. The architecture enables secure key exchange, physical-layer integrity checking and beamforming resiliency to eavesdropping, jamming, and other interference. By analytical modeling and simulation-based assessments, the proposed system achieved much better results in terms of key compromise resistance, the robustness of a signal against attacks, and the link reliability without reducing efficiency to operate the systems due to the limited resources of Internet of Things the end points may have. The post-quantum cryptography coupled with the physical-layer verification presents a new and synergistic approach toward the protection of dynamic LEO satellite communication environments.

Notably, any standardization works that might occur in the future, especially those on par with ETSI, ITU-T, or other global satellite safety requirements may also find some useful lessons in the guidelines created by this two-layered structure in terms of planning around post-quantum migration of space-based infrastructure.

Key Contributions

- A mixed communication mechanism that integrates physical-layer security and cryptographic communication.
- Kyber-1024, post-quantum key exchange in practical LEO satellite practice.
- Real-time mechanisms of SINR optimization and secure beam alignment within the antenna reconfiguration mechanisms.
- A simulation-based validation with robustness of jamming, spoofing, as well as quantum-enabled attacks.

Future Work

In a further effort to improve the scalability and deployment capability of the proposed system, the research directions in the future will involve:

- Incorporation into satellite Software-Defined Networking (SDN) stacks to enable the autonomous orchestration of security to and intersecting multi-satellite constellations.
- CubeSat missions field validation, by which real-world performance may be benchmarked over the constraints of orbital opportunities.
- Multi-hop, quantum-safe end-to-end secure routing protocols development in end-to-end satellite-IoT chunks mesh topologies.

The study forms the basis of the post-quantum generation of quantum-resistant Sat-IoT infrastructure ready to support secure, scalable, and globally interoperable IoT services.

References

1. Mao, Y., Zhang, J., Song, S. H., & Letaief, K. B. (2021). A survey on satellite-terrestrial integrated networks: Architecture, challenges, and key technologies. IEEE Communications Surveys & Tutorials, 23(4), 2254–2288. https://doi.org/10.1109/COMST.2021.3095260
2. Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSEC.2018.2871867
3. National Institute of Standards and Technology (NIST). (n.d.). Post-quantum cryptography standardization project. https://csrc.nist.gov/projects/post-quantum-cryptography
4. Li, S., Zhang, H., & Yang, Y. (2021). Physical-layer security in satellite communication networks: A survey. IEEE Access, 9, 29740–29759. https://doi.org/10.1109/ACCESS.2021.3058817
5. Abbas, A., Verma, R., & Yadav, S. (2023). Lightweight and quantum-resistant encryption for IoT systems. *IEEE Internet of Things Journal*, 10(2), 1673–1685.
6. Kundu, S., & Majumdar, S. (2022). Enhanced physical layer security in LEO satellite networks. *IEEE Transactions on Aerospace and Electronic Systems*, 58(6), 5102–5113.
7. Singh, M., Rao, T., & Sinha, N. (2024). Performance-driven reconfigurable antennas in LEO satellite mesh networks. *IEEE Access*, 12, 15030–15042.
8. Usikalu, M. R., Alabi, D., & Ezeh, G. N. (2025). Exploring emerging memory technologies in modern electronics. Progress in Electronics and Communication Engineering, 2(2), 31–40. https://doi.org/10.31838/PECE/02.02.04
9. Surendar, A. (2024). Internet of medical things (IoMT): Challenges and innovations in embedded system design. SCCTS Journal of Embedded Systems Design and Applications, 1(1), 43-48. https://doi.org/10.31838/ESA/01.01.08
10. Ali, M., & Bilal, A. (2025). Low-power wide area networks for IoT: Challenges, performance and future trends. Journal of Wireless Sensor Networks and IoT, 2(2), 20-25.
11. Arthur, L., & Ethan, L. (2025). A review of biodegradable biomaterials for medical device applications. Innovative Reviews in Engineering and Science, 3(1), 9-18. https://doi.org/10.31838/INES/03.01.02
12. Abdullah, D. (2024). Strategies for low-power design in reconfigurable computing for IoT devices. SCCTS Transactions on Reconfigurable Computing, 1(1), 21-25. https://doi.org/10.31838/RCC/01.01.05