Poster: From Earth to Orbit: A Quantum-Secure Authentication Key-Establishment Mechanism to Defend Satellite Communications in the Quantum Age

Salman Shamshad
University of Bristol,
Bristol, United Kingdom.
salman.shamshad@bristol.ac.uk

Waqas Bin Abbas
University of Bristol,
Bristol, United Kingdom.
waqas.abbas@bristol.ac.uk

Sana Belguith
University of Bristol,
Bristol, United Kingdom.
sana.belguith@bristol.ac.uk

Lucy Berthoud
University of Bristol,
Bristol, United Kingdom.
Lucy.Berthoud@bristol.ac.uk

***Abstract*—The inherent broadcast characteristics of satellite communication systems make them vulnerable to interception and manipulation threats. Stringent Authentication and Key-Establishment (AKE) mechanisms play a vital role in securing satellite communication links by verifying legitimate participants and establishing a secret session for protected communication. Nevertheless, the existing AKE mechanisms based on classical cryptographic methods are not sufficient to guarantee the security of these systems in the forthcoming post-quantum era. Recognizing these flaws, we propose a quantum-secure robust AKE mechanism that fortifies these communications systems against emerging cyber and quantum threats. To the best of our knowledge, this is the first study to integrate NIST-approved quantum-safe cryptography primitives, coupled with a hardware fingerprinting-based key generation mechanism.**

I. Introduction

The continuous advancements in satellite technology and onboard processing equipment have made space-based systems a vital element of modern communication infrastructure. Their extensive information exchange capabilities play a significant role in facilitating services for a wide range of applications, including telecommunication networks, humanitarian operations, maritime surveillance, military operations, and global Internet services [1]. Over the years, satellite communications has witnessed a transition from simple analog transmission to advanced digital and broadband communication networks. In contrast to terrestrial networks, satellite communication constellations can offer reliable connectivity with up to 99.99% availability, even in remote and inaccessible regions of the world. They facilitate the transmission of multimedia signals and data across long distances through satellites, functioning as an intermediate node (or 'bent pipe' rep) in space.

This rising reliance also carries substantial risks, as any failure can disrupt essential communication and affect national and economic stability. For example, space infrastructure lacks default security measures and is inherently vulnerable to threats, which can target its communication links, user interfaces, ground infrastructure, and spacecraft. Notably, most of these attacks exploit weaknesses in authentication and data integrity; so adopting robust cryptographic protections is vital to secure these systems [2]. Otherwise, attacks can lead to serious consequences that may include altering trajectories or even causing collisions. All the aforementioned vulnerabilities emphasize the crucial need for cybersecurity in space infrastructure to protect sensitive data and ensure its smooth operations. To address such limitations, AKE mechanisms offer a more robust alternative to existing countermeasures in establishing dynamic and authenticated keys across space networks.

However, the use of weak encryption and cryptographic primitives may render AKE ineffective. For example, recently developed quantum algorithms (i.e., Shor's algorithm [3]) threaten the robustness of classical cryptographic primitives (e.g., elliptic curve cryptography). As existing AKE mechanisms continue to rely on classical cryptography, these techniques are not sufficient to guarantee the foolproof security of satellite communication systems in the post-quantum era. In line with this objective, the European Space Agency (ESA) has launched an initiative to advance quantum-safe satellite communication systems, positioning cybersecurity as a fundamental asset of the space industry [4]. This aims to develop a qualified commercial space system comprising space and ground components that provides end-to-end quantum-safe security for all satellite data. Therefore, we propose a provably secure AKE mechanism by integrating the NIST-approved Module Learning-Key Encapsulation Mechanism, coupled with SHA-256 and AES-256 cryptographic primitives, to make our protocol resilient against both classical and quantum-capable adversarial threats.

Figure 1 demonstrates a high-level system architecture of our target satellite communication systems. Typically, these systems include three core segments: ground, space, and end-user, which together form a complete system. It begins with the ground segment that encompasses the ground operations center, the ground station server, and the supporting ground network located on Earth. This part is responsible for sending the commands to the spacecraft and receiving telemetry and sometimes payload data in response. The Space Link

Workshop on Security of Space and Satellite Systems (SpaceSec) 2026
23 February 2026, San Diego, CA, USA
ISBN 978-1-970672-02-2
https://dx.doi.org/10.14722/spacesec.2026.23095
www.ndss-symposium.org

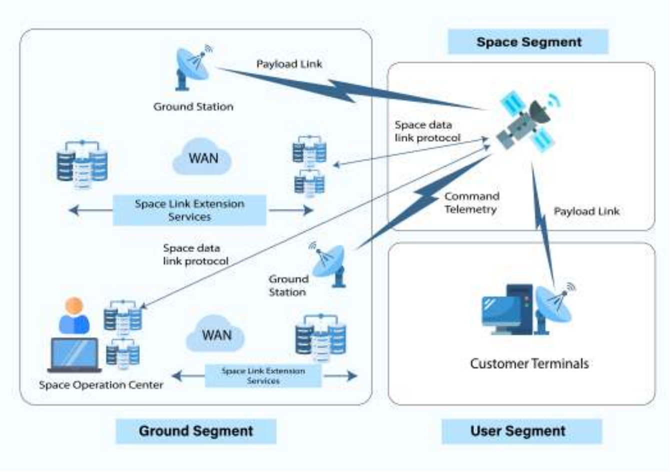

Figure 1: Satellite Communication System Architecture

Extension (SLE) services enable ground stations to connect with both space operation and data centers. Above the ground is the space segment, which encompasses all in-orbit assets, including spacecraft and orbital stations (e.g., the International Space Station). The last part is the user segment, comprising the equipment and terminals used by end-users. Communication primarily occurs through Radio Frequency (RF) channels, where the space segment serves as a payload platform and sometimes as a communication node for forwarding signals between the end-user and the ground segments.

II. Proposed Protocol

This section presents our proposed quantum-safe authentication mechanism explicitly designed for securing satellite communications networks. It primarily involves three entities, including a Space Operations Center ($\mathbb{SOC}_k$), $\mathbb{GSS}_j$, and $\mathbb{SAT}_i$.

A. System Initialization

This phase initializes the authentication system by establishing trusted and consistent cryptographic parameters, creating a secure foundation for all subsequent authentication and key establishment operations.

B. Registration Phase

Each satellite is securely registered by the $\mathbb{GSS}_j$ before launch by assigning secure identities and generating hardware-bound secrets using PUFs with error correction support. The registration data is encrypted, securely stored at the ground station, and essential credentials are embedded in the satellite's memory to enable secure and privacy-preserving future communications.

C. Authentication and Key-Establishment Phase

A step-by-step process of the designed AKE mechanism detailed as below:

Step-1: Initially, $\mathbb{SAT}_i$ automatically initiates the AKE procedure upon its first RF contact with $\mathbb{GSS}_j$ or when a previously established session key expires. During this step, $\mathbb{SAT}_i$ reconstructs its internal security parameters using its hardware-bound identity and generates fresh random values along with a current timestamp to ensure message freshness. Based on these parameters, $\mathbb{SAT}_i$ constructs an authentication request that conceals sensitive identity information and guarantees unlinkability. The authentication request message is then transmitted to $\mathbb{GSS}_j$ over the insecure RF channel.

Step-2: Upon receiving the request, $\mathbb{GSS}_j$ first validates the freshness of the message by checking the included timestamp, thereby mitigating replay attacks. Afterward, $\mathbb{GSS}_j$ retrieves the corresponding registration record of $\mathbb{SAT}_i$ from its secure verification table and validates the authenticity of the received message using the stored credentials. Once the verification succeeds, $\mathbb{GSS}_j$ generates fresh challenge values and derives a session key bound to the satellite's identity and hardware-specific secrets. Subsequently, $\mathbb{GSS}_j$ constructs an authentication response message that proves its legitimacy and forwards it to $\mathbb{SAT}_i$.

Step-3: After receiving the response, $\mathbb{SAT}_i$ verifies the freshness and authenticity of $\mathbb{GSS}_j$ by validating the received challenge information. Upon successful verification, $\mathbb{SAT}_i$ independently derives the same session key and accepts it as the shared symmetric key. This session key is finally used to encrypt and secure all subsequent telemetry, command, and data exchanges between $\mathbb{SAT}_i$ and $\mathbb{GSS}_j$, ensuring confidentiality, integrity, and mutual trust within the satellite communication system.

III. Conclusion

This work leverages the security strength of NIST-approved quantum-safe cryptographic primitives to propose a quantum-secure AKE mechanism that enhances satellite communication's resilience against emerging cyber and quantum threats. It further integrates a hardware-rooted fingerprinting process that generates unique and tamper-resistant keys to provide a robust foundation for robust of trust in resource-constrained satellite communication systems.

References

[1] N. H. S. Suhaimi, N. H. Kamarudin, M. N. A. Khalid, I. Tahir, and M. A. A. Mohamed, "State-of-the-art authentication measures in satellite communication networks: a comprehensive analysis," *IEEE Access*, 2024.

[2] S. Salim, N. Moustafa, and M. Reisslein, "Cybersecurity of satellite communications systems: A comprehensive survey of the space, ground, and links segments," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 1, pp. 372–425, 2024.

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[4] European Commission, "Quantum europe strategy: Quantum europe in a changing world," Communication from the Commission to the European Parliament and the Council, Brussels, July 2025, cOM(2025) 363 final. [Online]. Available: https://commission.europa.eu/