electronics

MDPI

Article

Mitigating Machine-in-the-Loop Drone Attacks on Satellite Links via Atmospheric Scintillation Analysis

Rajnish Kumar * and Shlomi Arnon

Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer-Sheva 8410501, Israel
* Correspondence: rajnish@post.bgu.ac.il

Abstract

The emergence of quantum computing poses a significant threat to the security of traditional encryption methods employed in satellite communication. To mitigate this vulnerability and enhance cybersecurity in the next generation of communication systems, a novel physical-layer solution is presented. This approach centers on enhancing satellite link security through the analysis of stochastic atmospheric scintillation, facilitated by machine learning (ML). The proposed method safeguards ground stations against Machine-in-the-Middle (MITM) attacks perpetrated from aerial platforms (AP) such as drones or Unmanned Aerial Vehicles (UAVs). The underlying principle leverages the distinct statistical parameters inherent to received signals. These parameters are contingent upon the specific propagation channel, which is influenced by rapid tropospheric scintillation. As signals from legitimate satellites and malicious drones traverse separate spatial paths within the dynamic atmosphere, they exhibit demonstrably divergent scintillation statistics. Wavelet filtering is employed to extract these statistics from the incoming signal. The extracted data is subsequently processed through an ML algorithm, enabling the differentiation between satellite signals and potential spoofing signals emanating from drones. Extensive simulations have been conducted, illustrating the efficacy and robustness of the proposed architecture, consistently achieving an authentication rate exceeding 98% across diverse scenarios. Additionally, experimental results obtained from measurement data collected from Nilesat and Eutelsat satellites at a ground station in Israel provide empirical validation for this innovative approach.

Keywords: atmospheric effects; LEO satellite; machine Learning; physical layer security; wavelets

Check for updates

Academic Editor: Silvia Liberata Ullo

Received: 12 February 2026
Accepted: 3 March 2026
Published: 4 March 2026

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.

1. Introduction

The proliferation of Low Earth Orbit (LEO) satellite constellations, exemplified by Starlink, OneWeb, and Telesat, signifies a growing reliance on space-based communication infrastructure [1]. This trend is driven by the need for wider coverage and higher data rates, necessitating a shift towards millimeter-wave (mmWave) bands for LEO communication systems [2]. Furthermore, these LEO constellations are poised for integration with terrestrial networks, providing a robust foundation for future 6G communication systems. However, a critical concern emerges: the inherent vulnerability of satellite communication due to its broadcast nature across vast geographic areas. This susceptibility is compounded by advancements in integrated circuits, readily available and affordable electronic equipment,

and the prevalence of open-source software, all of which potentially facilitate cyberattacks on these critical communication links [3,4].

Integrated space–terrestrial networks (ISTNs) are emerging as a key architectural enabler for future 6G communication systems, offering global coverage, enhanced reliability, and robust connectivity in challenging environments. These capabilities are particularly critical for application domains such as global navigation satellite systems (GNSS), military and tactical communication networks, disaster-response operations, and remote sensing. However, the broadcast and open-air nature of satellite links exposes ISTNs to severe security vulnerabilities, making physical layer security (PLS) an essential design consideration. Recent studies—such as the work presented in [5,6], highlight the growing relevance of PLS techniques in safeguarding link confidentiality against sophisticated threats.

Satellite communication faces a multitude of cybersecurity threats, including data interception/corruption, eavesdropping, spoofing, and jamming [7,8]. While traditional encryption offers protection, its scalability to high-bandwidth, ultra-low latency LEO systems is hindered by increased transmission overhead [9]. Additionally, advancements like Shor's algorithm in quantum computing threaten to render current encryption methods obsolete [10]. Consequently, a multifaceted approach encompassing cross-layer solutions is necessary to mitigate these threats. Physical Layer Security (PLS) emerges as a promising technique by exploiting the inherent properties of the communication channel and wave propagation for secure transceiver design [11]. Leveraging information theory, PLS offers lower computational complexity compared to traditional cryptography, translating to reduced code size and energy consumption by eliminating complex encryption computations [7]. By complementing existing encryption and upper-layer authentication protocols, PLS contributes to a more robust and trustworthy transceiver design for secure satellite communication networks.

The mmWavecommunication with satellites experiences greater signal attenuation due to both increased free-space path loss and enhanced molecular absorption within the atmosphere [12]. Mitigating these substantial losses necessitates communication link designs that incorporate high-gain, highly directional antennas with narrow beamwidths [13]. These directional antennas inherently offer improved security against cyberattacks by virtue of their focused transmission patterns directed towards the satellite in the sky [14]. However, it is conceivable that under specific circumstances, an AP could be strategically positioned within this narrow beam, enabling a potential MITM attack on the ground station.

Modern anti-spoofing efforts, particularly in the GNSS domain, often rely on cryptographic authentication of navigation data (e.g., Galileo OS-NMA) or signal quality metrics like power level, angle-of-arrival (AOA) measurements, and polarization analysis. However, AOA systems can be defeated by synchronized spoofers, and power-based detection is trivial to overcome. Furthermore, these techniques often require complex, multi-antenna arrays or high-precision sensors, adding significant cost and complexity to ground station deployment.

The physical-layer spoofing presents as a major threat due to the emergence of quantum computing and low-cost aerial platforms. In this paper, we consider a specific and realistic threat model in which a low-altitude aerial platform (AP) launches Machine-in-the-Middle (MITM) attacks. By transmitting a forged satellite-like signal, the AP, such as commercial drones, tries to impersonate a legitimate satellite at a ground station receiver. The attacker aims to lock into the ground station by replicating the satellite waveform and tuning its transmit power while it remains within the main beam of the ground station's antenna.

Although spoofing is traditionally considered a network/logical-layer attack, it can manifest at the physical layer through inconsistencies in channel characteristics and signal

statistics. A spoofer attempting to impersonate a legitimate node cannot simultaneously replicate its location-dependent fading and hardware-induced impairments. Physical-layer security exploits these non-forgeable properties to distinguish legitimate signals from spoofed transmissions.

Environmental randomness has been widely recognized as a valuable resource for enhancing wireless security, particularly in covert communication scenarios where random channel fluctuations can significantly degrade an adversary's detection capability. Prior theoretical studies have demonstrated that randomness arising from user activity or propagation conditions can enable positive covert communication rates and improve low-probability-of-detection performance in random wireless networks [15,16]. In the considered satellite communication context, atmospheric scintillation constitutes a naturally occurring and spatially varying source of environmental randomness that introduces rapid amplitude and phase fluctuations in the received signal [17]. In this work, such scintillation-induced randomness is primarily exploited for practical physical-layer authentication and attack detection, as it provides distinctive and difficult-to-replicate signal characteristics.

Beyond authentication, the same propagation-induced randomness may also play a complementary role in other security scenarios, including covert communication and secrecy enhancement under interference-limited conditions [18,19]. Although a rigorous analysis of covert rate optimization and adversary detection bounds is beyond the scope of this paper, the results suggest that environmental randomness introduced by tropospheric scintillation can serve as a beneficial physical-layer resource rather than a purely detrimental channel impairment. This observation aligns with existing theoretical insights on environment-assisted security and motivates future investigations into the joint exploitation of scintillation dynamics for authentication, secrecy, and covert communication in integrated satellite–terrestrial networks.

Our proposed system introduces a fundamental departure from conventional cryptographic paradigms by implementing a zero-trust physical-layer authentication (PLA) mechanism. This approach moves beyond traditional protocol-based security to exploit the intrinsic, natural characteristics of the propagation channel itself. The core innovation lies in the utilization of rapid tropospheric scintillation as a unique, non-clonable "atmospheric fingerprint."

The authentication barrier is rooted in the significant spatial and atmospheric divergence between legitimate and adversarial signal paths. A legitimate satellite signal undergoes complex scattering and refraction as it traverses the entire depth of the ionosphere and troposphere. Conversely, a malicious signal (e.g., from a low-altitude drone or terrestrial spoofing agent) traverses a radically different, shorter, and lower-altitude path. This results in stochastic parameters that, when extracted via wavelet filtering, are statistically divergent from the legitimate source. Because an earthbound attacker cannot physically replicate the cumulative atmospheric turbulence of a deep-space-to-ground link, the channel itself serves as a robust, low-cost authentication primitive.

This work specifically addresses the "quiet" yet realistic threat of a clandestine eavesdropper who attempts to blend into the network using a single-antenna system without interfering with legitimate components. By feeding the unique spatiotemporal fingerprints of the received signal into a machine learning model, the system learns to differentiate between true satellite transmissions and impostor signals. Ultimately, instead of relying on a digital handshake, we allow the physics of the atmosphere to reveal the true origin of the transmission.

1.1. Problem Formulation

Advancements in technology have facilitated the widespread adoption of AP in various civilian applications [20,21]. Regulations permit these commercial drones to operate at low altitudes, for example, 400 feet, as stipulated by the USA Federal Aviation Administration (FAA) [22]. Malicious actors can exploit these readily available consumer drones to position a spoofing transmitter within the line-of-sight of the ground station's receiver, specifically aligned with the main antenna beam pointed towards the satellite. Electronic spoofing attacks involve a fraudulent transmitter mimicking a legitimate radio frequency (RF) signal, effectively deceiving the receiver and causing it to lock onto the spoofed signal instead of the intended satellite transmission [23]. By strategically placing the transmitting antenna on an AP, the attacker can generate a stronger signal at the satellite downlink frequency, thereby manipulating the ground-based receiver to lock onto the spoofed signal. Once a successful lock is established, the drone can be used as a platform to launch various cyberattacks against the receiver, potentially causing significant disruption to critical communication infrastructure.

This work considers a passive eavesdropping threat where the eavesdropper (AP) attempts to impersonate as a legitimate satellite. The eavesdropper is assumed to be equipped with a single antenna and has no cooperation with legitimate nodes. This threat model is relevant for space–terrestrial networks, where covert interception is more likely than active attacks due to detectability constraints. The PLS technique employed in this work is based on the scintillation characteristics in the tropospheric paths along the channel. The channel from the satellite-to-GS and that from AP-to-GS have different inherent characteristics. As a result the spatiotemporal signature of the two channels differ by which is the fed as input to the ML model. The ML model then classifies whether the time-series signal belongs to the satellite or an AP.

Figure 1 depicts a worst-case scenario for a spoofing attack launched by a drone against a ground station in an LEO satellite communication system. In this scenario, the drone strategically positions itself within the main beam of the ground station antenna, directly aligned with the line-of-sight path to the satellite. This alignment maximizes the attacker's signal strength due to the narrow-beamwidth characteristic of the antenna, particularly in mmWavebands. Consequently, signals originating from the drone at off-axis angles experience a significant reduction in the signal-to-interference plus noise ratio (SINR), rendering them less effective for spoofing attempts. High-gain antennas with narrow beamwidths are a defining feature of mmWavecommunication systems. Therefore, spoofing attempts from directions outside the main beam are significantly less threatening. Off-axis attack angles result in a considerably lower SINR, rendering them less viable for disrupting communication. The most advantageous position for the drone, maximizing the efficacy of its spoofing attempt, is directly within the main beam of the ground station antenna.

1.2. Related Works and Contribution

Several studies have explored PLS techniques to enhance the security of satellite communication links, including beamforming, power allocation, secrecy capacity optimization, precoding, and relay selection schemes. For example, Yin et al. [24] proposed a joint optimization framework that maximizes secrecy capacity through coordinated satellite beamforming and UAV power allocation. However, this approach relies on accurate channel state information (CSI) and centralized optimization, assumptions that may be difficult to satisfy in highly dynamic UAV attack scenarios. Similarly, Schraml et al. [25] introduced a precoding algorithm for securing multi-user satellite downlinks by optimizing the minimum secrecy capacity. While effective in static or slowly varying environments,

the method assumes stable channel conditions and does not explicitly account for the fast mobility or intermittent presence of aerial attackers.

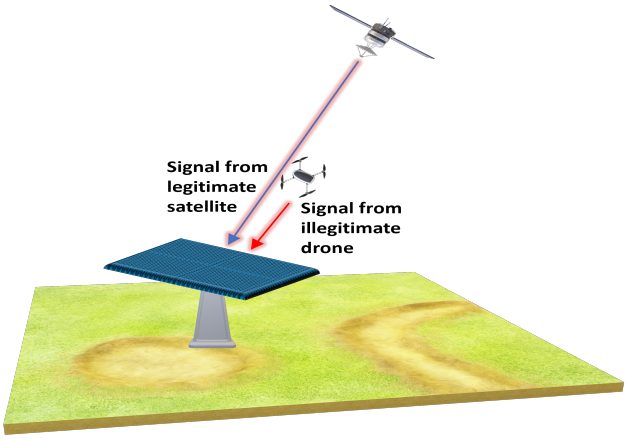


Figure 1. An aerial platform launching an MITM attack on a ground station antenna receiver with its main beam pointing to the sky towards the LEO satellite.

In ref. [26], the authors analyzed the secrecy performance of satellite links by deriving closed-form expressions for secrecy outage probability and average secrecy capacity. This work provides valuable theoretical insights, it focuses primarily on analytical performance evaluation rather than practical attack detection or mitigation mechanisms. Moreover, the considered eavesdropping models are largely static and may not fully capture the dynamic spatial behavior of UAV-based adversaries. Likewise, Li et al. [27] investigated cooperative interference relay selection and optimized power allocation to enhance satellite link security. Despite the performance gains, this approach depends on coordinated relaying and precise power control, which can introduce additional signaling overhead and limit scalability in real-world satellite–UAV–ground integrated networks.

In ref. [28], the authors employed low-density parity-check (LDPC) coding schemes while assuming the availability of CSI to enhance PLS. Although coding-based approaches can improve secrecy under controlled conditions, their effectiveness depends on accurate CSI acquisition and long codeword lengths, which may be impractical in fast-varying satellite–UAV channels and latency-sensitive applications. The work in [29] proposed an adaptive PLS technique based on Doppler shift and received power features using a support vector machine (SVM) classifier. While the method demonstrates promising detection capability, its performance relies on stable feature extraction and supervised learning, which may be sensitive to environmental variations and require extensive labeled training data.

In ref. [30], convolutional neural networks (CNNs) and autoencoders were employed for satellite transceiver authentication to detect spoofing attacks. Despite their strong classification performance, deep learning-based approaches often involve high computational complexity and large training datasets, which can limit their applicability in resource-constrained satellite or ground terminals. Furthermore, model generalization under rapidly changing channel and mobility conditions remains an open challenge. The study in [31] compared chirp spread spectrum (CSS)-based LoRa and direct sequence spread spectrum (DSSS)-based Ingenu schemes for IoT transmission over LEO satellites. While this work provides valuable insights into modulation robustness and link performance, it focuses primarily on physical-layer reliability and access efficiency rather than security or adversarial attack mitigation. Consequently, spoofing and eavesdropping threats are not explicitly addressed.

In ref. [32], a hypothesis-testing-based framework was proposed to differentiate between legitimate and illegitimate LEO satellites using Doppler spread and received power characteristics. Although effective for satellite identification, this approach assumes relatively stable statistical signatures and may suffer performance degradation in dense or highly dynamic UAV-assisted environments where attackers can partially mimic such features. The authors in [33] explored the use of statistical and spectral properties of rapid signal fluctuations to distinguish satellites at different elevation angles. While this method leverages naturally occurring channel variations, it is primarily tailored to classification and identification tasks rather than secrecy enhancement, and its robustness against sophisticated, adaptive spoofing attacks is not explicitly analyzed.

In ref. [34], the use of an aerial reconfigurable intelligent surface (RIS) for cooperative jamming was investigated by exploiting channel similarities among eavesdroppers. Although RIS-assisted jamming can significantly enhance secrecy, it requires precise coordination, additional aerial infrastructure, and accurate channel knowledge, which may increase deployment complexity and limit practicality in real-time UAV attack scenarios. The work in [35] presented a fast single-satellite positioning method for GNSS-denied environments using an LEO communication satellite, combining time–frequency Doppler analysis with beam switching. While the proposed approach enables real-time positioning, it is designed primarily for localization rather than security and does not explicitly address spoofing detection or confidentiality protection at the physical layer.

Finally, recent studies in [36,37] addressed hybrid-field channel estimation challenges in massive MIMO systems at mmWave and THz frequencies using sparse Bayesian learning (SBL) frameworks. These works significantly improve channel estimation accuracy and robustness; however, they focus on estimation performance rather than adversarial security. Moreover, their applicability to satellite–UAV scenarios is constrained by hardware complexity and the need for large antenna arrays, which may not be feasible in practical satellite payloads.

Modern anti-spoofing techniques often rely on intentional signal features, such as power, angle-of-arrival (AOA), or timing characteristics. However, these approaches are susceptible to replication or synchronization by sophisticated attackers and may require complex hardware (multi-antenna arrays, high-precision sensors) [14].

In contrast, our proposed approach leverages unintentional physical-layer features arising from the communication channel itself. Specifically, rapid tropospheric scintillation induces unique, spatially dependent fluctuations in the received signal that are extremely difficult for an AP attacker to replicate in practice. These naturally occurring variations serve as a practical fingerprint for signal authentication. Table 1 summarizes the key differences between traditional physical-layer authentication methods and the proposed channel-based, practical authentication approach.

This work presents a novel signal processing algorithm to improve the PLS of a ground station receiver communicating with an LEO satellite against MITM attacks launched from AP such as drones. The proposed technique leverages rapid signal variations primarily induced by atmospheric scintillation fading to differentiate between the legitimate satellite signal and spoofing signals originating from APs. At the ground station receiver, the algorithm first extracts these rapid fluctuations from the received signal and feeds them into a ML classifier for signal origin determination (satellite vs. drone). This work investigates the use of both a linear classifier (LC) and a neural network (NN) for classification, with the LC serving as a baseline and the NN anticipated to yield superior performance. The extraction of rapid variations is achieved through multi-resolution analysis using a maximum overlap discrete wavelet transform (MODWT) filter. The proposed algorithm

undergoes rigorous testing under diverse scenarios, employing both an extensive dataset and experimental data.

Table 1. Comparison of authentication paradigms.

Feature	Conventional Cryptographic Schemes.	Proposed Atmospheric PLA.
Authentication Source	Computational complexity (keys/hashes).	Natural channel stochasticity.
Primary Dependency	Secure key distribution and storage.	Atmospheric path length and turbulence.
Adversarial Resilience	Vulnerable to key theft or brute-force.	Physically impossible to forge path traits.
Computational Overhead	High (encryption/decryption cycles).	Low (passive signal analysis).
Detection Basis	Protocol handshake verification.	ML-driven statistical classification.

The GEO–GEO experimental framework employed in this work provides a controlled and repeatable environment that is well-suited for emulating several key characteristics of drone-based spoofing attacks. Although the geometry of drone spoofers differs from that of GEO satellites, the dominant signature features relevant to spoofing detection—such as prescribed power evolution, controlled carrier dynamics, and structured temporal behavior—can be accurately reproduced within a GEO–GEO configuration [38,39]. The inherent stability of GEO links enables precise parameter manipulation, facilitating systematic evaluation of spoofing-induced distortions that would be difficult to isolate in field trials involving airborne platforms. Consequently, GEO–GEO experimentation constitutes a practical and technically sound surrogate for drone spoofing during early-stage assessment and algorithm development. The interpretation of the observed "fast fluctuations" further benefits from the controlled nature of GEO–GEO measurements. While system-level impairments—including AGC transients, LNB frequency drift, multipath propagation, and replay-type echoes—may introduce additional amplitude or phase variability, such effects can be explicitly characterized and distinguished from the emulated spoofing signatures. Accounting for these impairments does not diminish the validity of the GEO–GEO approach; rather, it enhances confidence that the measured fluctuations originate from the intended emulation scenario rather than from receiver limitations or environmental artifacts. Overall, the results indicate that GEO–GEO experiments provide a credible and effective platform for spoofing-related research, enabling high-fidelity reproduction of relevant signal behaviors under well-defined conditions. With appropriate monitoring of potential system impairments, the GEO–GEO methodology faithfully captures the salient features required for spoofing detection analysis and offers a solid foundation for progression toward more complex drone-based or field-deployed validation studies.

The key contributions of this paper are outlined as follows:

- The work presents a comprehensive model for calculating the SINR that incorporates the influence of various atmospheric effects on the signal propagating from both the satellite and the drone to the ground station. This mathematical model, expressed as an SINR expression, serves as the statistical foundation for the authentication method. The rationale lies in the fact that atmospheric effects leave a distinct spatial signature on the received SINR at the ground station.

- To address the influence of atmospheric effects, particularly scintillation, on the received SINR, the work proposes a wavelet-based technique for their targeted removal. This process isolates the rapid fluctuations in the received SINR at the ground station antenna, which are attributed to the spatial atmospheric signature. These extracted fluctuations then serve as the key discriminant features for ML-based identification of the signal source (satellite or drone).
- The efficacy of the proposed algorithm is validated using a conceptual framework and experimental data collected at a ground station in Israel, involving communication with two distinct satellites. The results demonstrate the effectiveness of the proposed method in leveraging the spatiotemporal signature as a robust fingerprint for thwarting spoofing attacks.
- We establish an attack model for a drone positioned in the direct line-of-sight path between the satellite and the ground station receiver. This model informs the creation of a comprehensive dataset subsequently employed for training and evaluation of the LC and NN algorithms. The ML algorithms leverage the extracted spatial atmospheric signature as input features for source classification of the received signal. Ultimately, the algorithm determines whether the signal originated from the legitimate satellite or a spoofing drone.

This work presents a novel approach to PLS for satellite communication systems. To the best of our knowledge, it is the first to exploit the spatial characteristics of rapid signal fluctuations induced by scintillation fading in the satellite channel. This technique improves the security of the ground station receiver against MITM attacks launched from APs, even in the worst-case scenario of direct line-of-sight alignment.

The paper is organized as follows. Section 2 discusses the link design. Section 3 discusses the methodology with conceptual framework and the architecture of the proposed network to classify the signals as belonging to a legitimate satellite or spoofing drone. In Section 4, we show the experimental results using data obtained with two different satellites and numerical simulations using the SINR model. Section 5 concludes the paper.

2. SINR Modeling

This section establishes mathematical models for the SINR of the communication links. The models consider the respective links between a drone and the ground station (GS) receiver, and between a satellite and the GS receiver at an elevation angle of θ_0. Path losses and noise contributions within the atmospheric channel are incorporated into the models.

2.1. SINR: Drone to GS

The propagation through the atmospheric channel introduces attenuation to the transmitted signal from both the AP and the satellite. This attenuation stems from two primary mechanisms: free-space path loss and gaseous absorption loss. At mmWavefrequencies, oxygen and water vapor molecules become the dominant contributors to gaseous absorption. The magnitude of this absorption loss at a specific frequency depends on various atmospheric parameters, including pressure, temperature, water vapor density, and the total path length traversed by the signal within the channel. The following equation expresses the atmospheric absorption loss experienced by the communication link between the drone and the ground station antenna receiver: [40]

$$L_A^d(f, \theta_0) = \sum_{i=1}^{M_d} \gamma_i d_i(\theta_0) \quad (1)$$

Following the ITU recommendation [40], the atmospheric model considers the atmosphere to be comprised of multiple thin and homogeneous layers. We denote the specific attenuation (in dB) of the ith layer as γ_i, the path length traversed by the signal through this layer at an elevation angle θ_0 as $d_i(\theta_0)$, the total number of layers M_d is determined by the drone's altitude, and f is the frequency.

The free-space path loss experienced by the signal at an elevation angle θ_0 is given as

$$L_{FS}^{d}(f,\theta_0) = \left[\frac{4\pi}{\lambda}\left(-R_e\cos\theta_0 + \sqrt{(R_e+h_d)^2 - R_e^2\sin^2\theta_0}\right)\right]^2 \tag{2}$$

where R_e is the earth's radius and h_d is the altitude of the drone.

In addition to signal attenuation caused by the atmosphere, the communication channel also introduces thermal noise that disrupts the received signal at the ground station. This noise originates from various sources. The downwelling atmospheric gas temperature, influenced by the sky's brightness temperature, contributes to the overall antenna noise. Additionally, the upwelling ground surface temperature, arising from both ground emission and the reflected downwelling radiation from the ground surface, is another source of noise. The receiver electronics connected to the antenna port also generate noise, and the physical temperature of the receiving antenna itself plays a role. The brightness temperature of both the sky and ground, at a specific signal frequency, is determined by the physical temperature of the atmosphere. As outlined in [41], understanding these noise components is crucial for accurately modeling the SINR in satellite communication systems.

The downwelling atmospheric noise temperature experienced by the ground station receiver for a signal originating from the AP can be represented by [40]

$$T_{down}^{d}(f,\theta_0) = \sum_{n=M_d}^{1} T_B(f,T_j)(1-10^{-\gamma_n d_n(\theta_0)/10})10^{-\sum_{j=M_d-1}^{1}\gamma_i d_i(\theta_0)/10} \tag{3}$$

where T_j is the physical temperature of atmospheric layers, $T_B(f,T_j)$ is the brightness temperature of each atmospheric layer with its physical temperature T_j, and γ_i (dB) is the specific attenuation for the ith homogeneous layer.

The upwelling temperature at the antenna due to the ground surface can be written as [42]

$$T_{up}^{d}(f,\theta_0) = \epsilon T_g + \rho_g T_{down}^{d}(f,180-\theta_0) \tag{4}$$

where ϵ denotes the emissivity, ρ_g represents the ground surface reflection coefficient, and T_g signifies the ground surface temperature.

To model the antenna gains for both the transmitter and receiver in the communication link, the following equation representing the gain of a parabolic reflector antenna is employed [43]:

$$G(\text{dB}) = 10\log_{10}\left[(\frac{\pi D}{\lambda})^2\right] \tag{5}$$

where D represents the diameter of parabolic antenna.

Due to the high gain and narrow-beamwidth characteristics of parabolic reflector antennas, resembling a pencil beam, the antenna temperature attributed to the sky's downwelling temperature can be approximated as the downwelling temperature within the main beam's direction. However, the ground contributes antenna temperature through the sidelobes. Assuming roughly 10% of the radiated power falls within these sidelobes, the equivalent noise temperature at the receiver antenna output can be approximated as [3]

$$T_S^d(\theta_0) = \eta_R[T_{sky}(\theta_0) + 0.1\ T_{gnd}(\theta_0)] + (1-\eta_R)T_p + T_{rx} \tag{6}$$

where T_{rx} is the noise due to the low-noise block downconverter (LNB) connected to the antenna port, T_p is the physical temperature of the receiver antenna, and η_R is the radiation efficiency of the receiver antenna.

The SINR for the communication link between the drone and the ground station, at elevation angle θ_0 can be expressed as

$$SINR^d(f,\theta_0) = \frac{\eta_T^d \eta_R P_T^d G_T^d G_R}{L_{FS}^d(f,\theta_0) L_A^d(f,\theta_0) k_B T_A^d(f,\theta_0) B} \tag{7}$$

where P_T^d denotes the transmitted power, η_T^d represents radiation efficiency of the transmitting antenna, G_T^d signifies the gain of the transmitting antenna, G_R is the gain of the receiver antenna, $T_A^d(f,\theta_0)$ denotes the receiver antenna temperature due to the signal coming from drone at elevation angle θ_0 and frequency f, L_{FS}^d is the free-space path loss, L_A^d is the signal absorption loss in the atmospheric path, k_B denotes the Boltzmann constant, and B represents the bandwidth.

2.2. SINR: Satellite to GS

The link budget design for the satellite-to-ground station (GS) communication link adopts a similar approach to that established for the drone link. The free-space path loss calculation remains identical, with the substitution of the drone altitude h_d with the satellite's altitude h_s. However, the atmospheric absorption loss for the satellite link accounts for all atmospheric layers (M) as specified in the ITU recommendation. This recommendation typically suggests a value of $M = 922$, corresponding to a multi-layered atmospheric model. In this model, the thickness of each homogeneous layer exhibits an exponential decrease with increasing altitude. The downwelling atmospheric noise temperature experienced by the ground station receiver for a signal originating from the satellite can be expressed as [40]

$$T_{down}^s(f,\theta_0) = T_{mb} \times 10^{-\sum_{j=M}^{1} \gamma_i d_i(\theta_0)/10} + \sum_{n=M}^{1} T_B(f,T_j)(1 - 10^{-\gamma_n d_n(\theta_0)/10}) 10^{-\sum_{j=M-1}^{1} \gamma_i d_i(\theta_0)/10} \tag{8}$$

where $T_{mb} = 2.73$ K is the microwave background temperature, $M = 922$ the number of homogeneous layers, and γ_i and $d_i(\theta_0)$ are the specific attenuation (in dB) and the traversed path length through ith atmospheric layer at an elevation angle θ_0.

Leveraging the equation for upwelling temperature (4), we can determine the ground station receiver antenna temperature for the satellite-to-ground link using the same principles. Consequently, the total receiver antenna noise temperature, $T_A^s(f,\theta_0)$, for this scenario can be computed following an analogous approach as outlined in (6).

Tropospheric scintillation arises from spatial variations in the refractive index of the atmospheric channel. These variations induce random fluctuations in the received signal amplitude at the ground station, appearing as rapid intensity variations. Scintillation intensity depends on several atmospheric parameters, including pressure, temperature, water vapor content, the signal frequency, and the elevation angle of the signal path [44]. It becomes a critical factor in link design, particularly for frequencies exceeding 10 GHz. Tatarskii theory provides a framework to model this phenomenon. Within this framework, the variance of the log-amplitude scintillation is expressed as [45]

$$\sigma_x^2 = 23.17 C_n^2 (\frac{2\pi}{\lambda})^{7/6} L^{11/6} \quad \text{dB}^2 \tag{9}$$

where C_n^2 denotes the refractive index structure constant, which characterizes the intensity of turbulence within the atmospheric channel. L represents the path length traversed by the

signal through the turbulent layer. The effective slant path length, L through the turbulent layer at a specific elevation angle, θ_0, can be expressed as [44]

$$L = \frac{2h_l}{\sin\theta_0 + \sqrt{2.35 \times 10^{-4} + \sin^2\theta_0}} \tag{10}$$

where $h_l = 1000$ m is the height of turbulent layer.

The communication link between the satellite and the ground station receiver experiences signal losses and noise from common sources. However, tropospheric scintillation effects, induced by atmospheric turbulence, introduce an additional layer of complexity [46]. Consequently, the SINR for this link, at a specific elevation angle θ_0, can be expressed as

$$SINR^s(f,\theta_0) = \frac{\eta_T^s \eta_R P_T^s G_T^s G_R \sigma_x^2}{L_{FS}^s(f,\theta_0) L_A^s(f,\theta_0) k_B T_A^s(f,\theta_0) B} \tag{11}$$

where the symbols have the usual meaning as defined earlier, and we have used "s" to indicate the link design parameters for the satellite. η_T^s is the radiation efficiency of the transmitting antenna of the satellite, G_T^s is the gain of transmitting antenna of the satellite, G_R is the gain of receiver antenna at the ground, P_T^s is the transmitted power from satellite, $T_A^s(f,\theta_0)$ is the receiver antenna temperature due to the signal coming from the satellite at elevation angle θ_0 and frequency f, L_{FS}^s is the free-space path loss, L_A^s is the signal absorption loss in the atmospheric path, and σ_x^2 is the variance due to tropospheric scintillation fading.

3. Methodology

In this section, our aim is to first demonstrate the basic principle and motivation that has led to the conceptual framework that we have used to distinguish between two signals. Secondly, we discuss the proposed algorithm that is used to take SINR time-series signal as input to differentiate whether the incoming signal is a spoofing signal from an AP or a legitimate signal from a satellite. This work is limited to commercial drones that are more widely used, with a maximum height of 500 m. In case of high-altitude platforms and objects flying at thousands of km above the earth, they will have similar atmospheric effects and therefore the accuracy would be much lower.

3.1. Conceptual Framework

The data concerning ratio of energy per symbol to noise power spectral density E_S/N_0 (dB) has been obtained at the ground station located in Kfar Saba, Israel, with the help of Ayecka Communication Systems. The satellites under consideration are Nilesat 7° W and Eutelsat 33° E. The elevation angles at the receiving site for Nilesat and Eutelsat are 31.6° and 52.5°, respectively. The frequency of operation lies in Ku-bands, and data is obtained with a sampling time of 30 s. The receiver site's geographical coordinates are situated at a latitude of approximately 32.16 degrees North and a longitude of around 34.93 degrees East. The receiver equipment consists of a parabolic antenna with a diameter measuring 1.2 m. Two such antennas are positioned within a proximity of 5 m from each other and receive signals from Nilesat and Eutelsat. The demodulator employed for this setup is detailed in the reference document "TC1 pro" [47]. The signal strength for detection falls within the range of −35 dBm to −75 dBm. Data consisting of E_S/N_0 (dB) was collected over the period spanning from 16 November 2021 to 11 November 2022. During this period, a total of 712,413 samples of E_S/N_0 (dB) were gathered for Eutelsat and 922,004 samples for Nilesat.

In Figure 2, we show the extracted rapid variations extracted from the received SINR from the two satellites. The principle that is used to extract such rapid fluctuations will

follow in detail in Section 3.2. From the experimental data, we observe the differences in signal strength of the two fluctuations (dB) and therefore the spatial variations in the signal can be leveraged for PLS of the satellite communication networks. In the considered scenario, where the data belong to two satellites, the spatial differences are caused by the difference in elevation angles at the receiver. The scintillation fading depends on the elevation angle, antenna gain, season, latitude, and water vapor content.

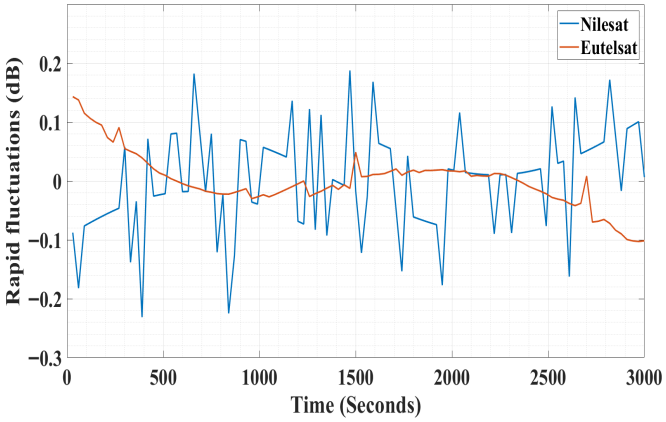


Figure 2. Rapid fluctuations extracted from the E_S/N_0 (dB) data received from two satellites—Nilesat and Eutelsat on 16 November 2022 at Kfar Saba, Israel.

Observing this conceptual framework showing that spatial variations can be utilized to identify the source of the transmitted signal from a satellite provides us motivation to dive deeper into the utility of this principle and its application to PLS. In the Section 4, we provide experimental results obtained with our proposed algorithm, which follows now.

3.2. Proposed Algorithm

Referring to Figure 1, the communication scenario involves a legitimate signal from a satellite and a potential spoofing signal from a drone (legitimate user) received at the ground station. Based on this configuration, we can establish the following observations:

- Since the received signals travel along distinct spatial paths through the atmosphere, the rapid fluctuations induced by scintillation will manifest as unique spatial signatures. The impact of tropospheric scintillation fading on the satellite-to-ground station link will be significant, whereas the effect on the drone-to-ground station link will be comparatively negligible [48,49].
- The downwelling atmospheric temperature experienced by the receiver antenna will exhibit a clear distinction between the drone-to-ground link and the satellite-to-ground link. This difference arises due to the distinct height of antenna placements within the atmosphere.
- Regarding the antenna temperature contributed by the upwelling brightness temperature, the noise temperature experienced by the antenna for both links will likely be similar. This can be attributed to the low reflection coefficient (approximately 0.05) and high emissivity (approximately 0.95) of the Earth's surface. These properties suggest that the majority of the upwelling radiation originates from the Earth itself, with minimal influence from the received signal [40].
- The noise temperature contribution from the receiver electronics connected to the antenna terminal is assumed to be identical for both communication links.

Several factors contribute to the overall signal variations experienced at the ground station receiver, including scintillation effects, sky and ground brightness temperatures, receiver noise temperature, and antenna temperature. To differentiate the legitimate satel-

lite signal from the potential drone-generated spoofing signal, we exploit the distinct characteristics of their rapid variations.

The first step involves isolating the rapid variations in the received SINR data. For this purpose, we employ multi-resolution analysis (MRA) utilizing the maximum overlap discrete wavelet transform (MODWT). MODWT decomposes the signal into various frequency bands using a set of low-pass and high-pass filter banks derived from the discrete wavelet transform. This decomposition enables the extraction of rapid, noise-like variations from the received signal.

A key advantage of MODWT lies in its ability to examine the signal across different frequency bands. This is particularly valuable when dealing with non-stationary signals, as it allows for the identification of features at distinct scales. Traditional methods, such as moving average filters, might smooth out the entire signal if its frequency content changes over time, leading to the loss of crucial details. In contrast, MODWT facilitates the independent analysis of specific frequency bands, offering a more nuanced approach.

The difference between the legitimate signal and eavesdropped signal mainly lies in the rapid signal variations in the received signal. With the real SINR data collected at the ground station, we extract the rapid signal variation using the MODWT and then pass this as a signal to NN. The schematic representation of the proposed architecture, designed to discriminate between the legitimate satellite signal and the spoofing signal from the drone, is illustrated in Figure 3.

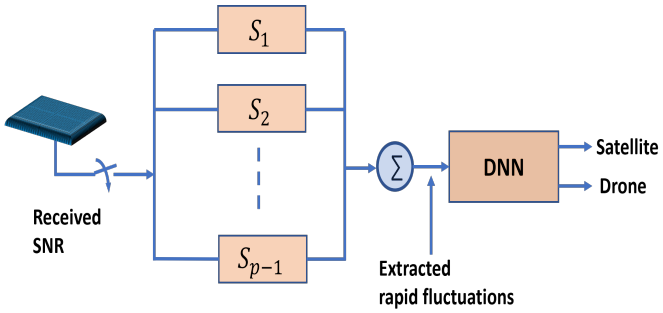


Figure 3. Block diagram of the proposed architecture for distinguishing the legitimate LEO satellite signal from the spoofing signal generated by an AP (where p represents the total number of transform levels).

To illustrate the decomposition of SINR into many high- and low-frequency components using multi-resolution analysis, we consider an example. We show the SINR plot using simulation in Figure 4 with a time-sequence length of 100. The number of transform levels can be taken as lower than $\lfloor \log_2 N \rfloor$, where N is the length of the signal vector. In this case, we have decomposed the signal in $p = 6$ different frequency levels. This same number of levels has been used in our dataset generation later on. The five highest frequency components are then summed up to get one composite signal representing the rapid fluctuations in the received SINR. It is the sum of the five highest frequency terms that is provided as input to NN, as shown in Figure 5. In Figure 6, the smoothest signal that will be discarded in the final computation is also shown. It is to be noted that the five highest frequency terms capture small, rapid fluctuations in the signal caused by the atmospheric effects primarily caused by scintillation.

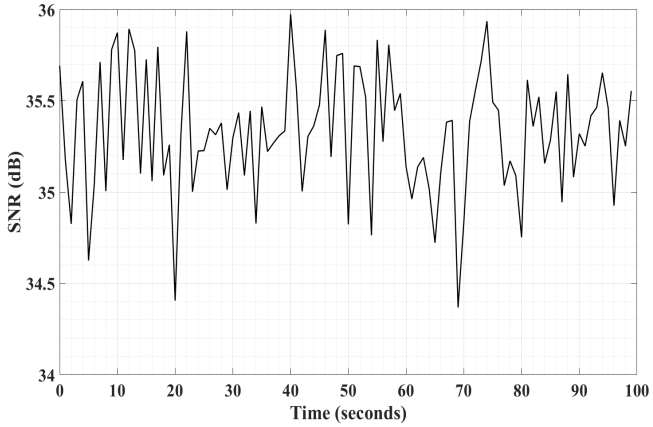


Figure 4. Simulated SINR at the ground station from an LEO satellite with the transmitted power of 1 W and a frequency of 80 GHz at an elevation angle of 10°.

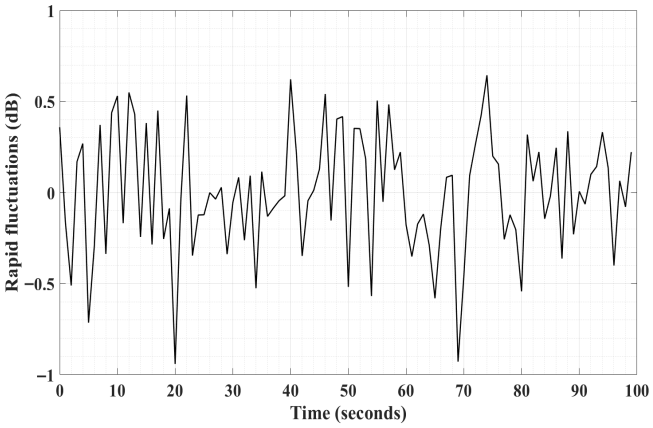


Figure 5. Rapid fluctuations (obtained by summing the five highest frequency components) extracted from the simulated SINR shown in Figure 4 using multi-resolution analysis.

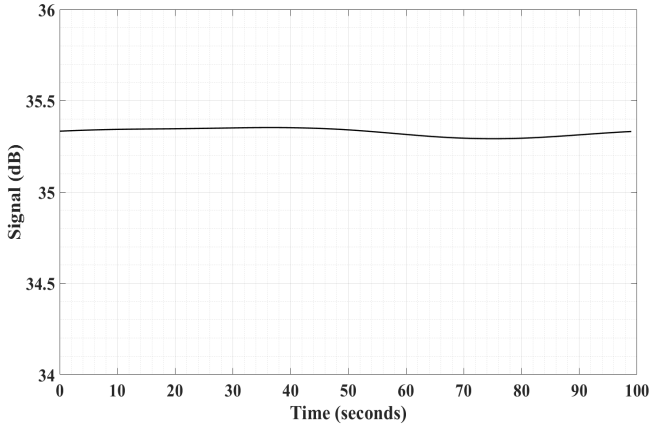


Figure 6. Signal component with the least frequency term extracted from simulated SINR, shown in Figure 4, finally discarded.

4. Results and Discussion

4.1. Experimental Results

We show the experimental validation of our proposed algorithm using the data from two geostationary (GEO) satellites. The model experiment will show how the spatiotemporal signatures can be utilized to help identify spoofing attacks by leveraging the spatial variations caused by atmospheric channels. This case can be considered an extreme exam-

ple of an AP launching a spoofing attack from another elevation angle and not being in the line-of-sight between the satellite and ground station receiver. In the scenario of drone and satellites, the spatial differences are caused by the difference in their altitudes.

The attack model is outlined as follows: Nilesat is regarded as the legitimate satellite, while Eutelsat takes on the role of an adversary attempting to execute electronic spoofing attacks by masquerading as Nilesat [33]. To attain this objective, we have maintained a constant E_S/N_0 (dB) value obtained from Nilesat while adjusting the E_S/N_0 (dB) from Eutelsat by the introduction of a variable, denoted as δ. This adjustment is made to mimic the tuning of signal power by Eutelsat in an attempt to emulate Nilesat. Consequently, the received E_S/N_0 (dB) for the signal originating from Eutelsat is expressed as $(E_S/N_0) + \delta$ (dB), where δ is allowed to vary within the range of 0 to 6 dB in increments of 0.1 dB. It is important to note that only positive values of δ are considered, as the E_S/N_0 (dB) obtained with Eutelsat is lower than that of Nilesat. The average E_S/N_0 (dB) values for Nilesat and Eutelsat are 9.5658 and 5.9116, respectively.

We employ the MODWT method to isolate the rapid fluctuations from the time-series E_S/N_0 data, as detailed in Section 3. The number of components in which the signal is decomposed is taken as six, as previously depicted. The resulting vector representing these rapid fluctuations will consist of 100 consecutive time samples. The vector consisting of the rapid fluctuations is provided to train the two ML algorithms. For this case, the number of examples extracted for the Nilesat and Eutelsat are 9220 and 7124, respectively. We will be considering an equal number of positive and negative examples, and therefore, the available dataset to train and test the NN will be 2×7124. For the training set, 70% of the dataset is used, while other 30% is used for the test set.

The linear classification model uses a support vector machine as the linear classification model. Specifically, the LC algorithm is selected as a representative traditional machine learning baseline due to its simplicity, interpretability, and widespread use in classification tasks under similar wireless sensing and channel-state scenarios. Including this baseline enables a clearer demonstration of the performance gains achieved by the proposed method over conventional linear decision models [50,51]. The classifier has the bias of 0.9645 and lambda as 6.6667×10^{-4}.

The neural network used in this work is composed of multiple fully connected (dense) layers designed to learn discriminative features from the input signals. The NN has the following specifications: three fully connected layers with 50, 20, and 10 neurons in each layer respectively, cross-entropy as the loss function, the activation function as the rectified linear unit (ReLU) function, the Xavier initializer to initialize the fully connected layer weights, and the loss function minimization technique as the limited-memory Broyden–Fletcher–Goldfarb–Shanno quasi-Newton algorithm (LBFGS). The specifications have been found heuristically to maintain high authentication rate.

With the help of the confusion matrix evaluated in each case, we compute the true positive (TP), true negative (TN), false positive (FP), and false negative (FN). We find the missed detection rate (MDR) and false alarm rate (FAR) as in [4]. Using the values of MDR and FAR, we define the authentication rate as [52]

$$\mathrm{AR} = \frac{1}{2}\left[(1 - \mathrm{FAR}) + (1 - \mathrm{MDR})\right] \tag{12}$$

We show the robustness and authenticity of the proposed method as δ is varied by providing the AR, MDR, and FAR. Observing Figure 7, the MDR is found to be below 1% NN in the case of all the considered scenarios of varying E_S/N_0 by Eutelsat while it is more than 2% for an LC. The results indicate that the system's ability to detect and classify potential spoofing attacks remains highly accurate. Figure 8 shows the FAR, and it is found

that FAR remains within a limit of 3% as δ is tuned over a wide range of values for NN. For LC, the FAR is more than 2% in all the cases. In Figure 9, the authentication rate is shown to achieve values higher than 99% for NN. For LC, it is lower than 98%. Overall, the performance metrics show that the rapid fluctuations can be utilized as a robust fingerprint for the identification of spoofing transmitters located in different spatial directions using NN with high authentication rate.

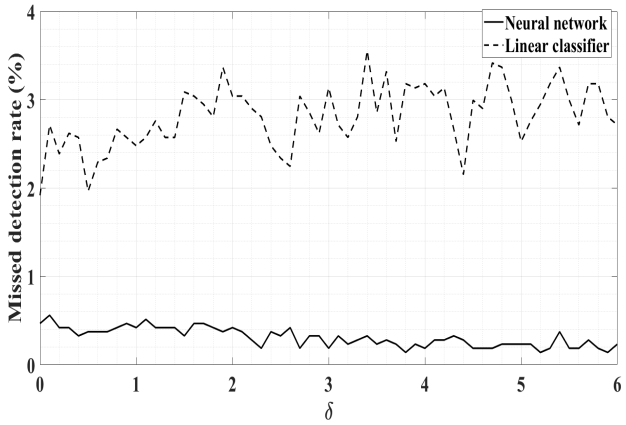


Figure 7. MDR with the proposed algorithm as Eutelsat tries to spoof Nilesat using experimental data.

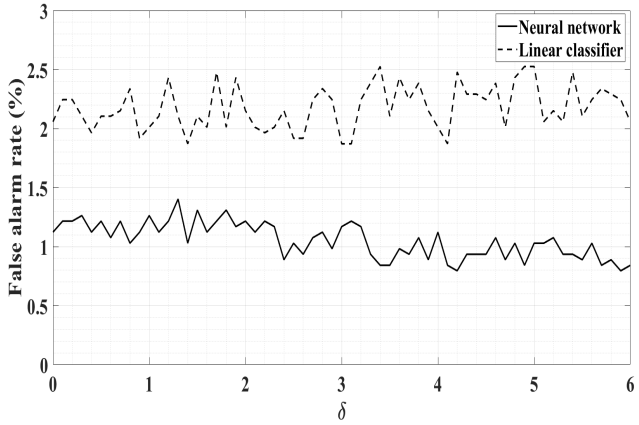


Figure 8. FAR with the proposed algorithm as Eutelsat tries to spoof Nilesat using experimental data.

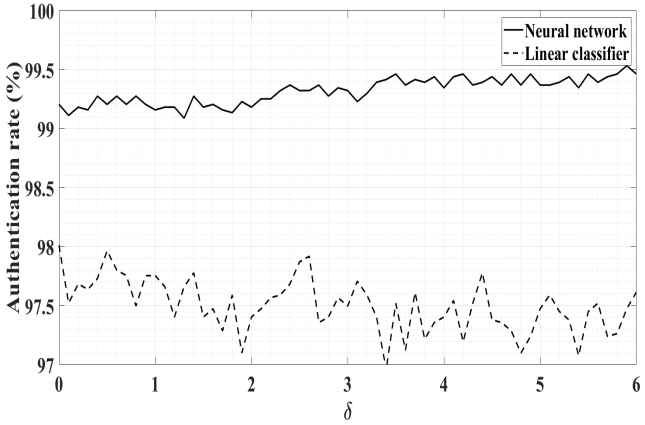


Figure 9. AR with the proposed algorithm as Eutelsat tries to spoof Nilesat using experimental data.

4.2. Simulation Results

This section details the link design parameters employed for simulation purposes. Table 2 summarizes these parameters for the satellite, drone, and ground station (GS)

antenna receivers. The atmospheric profile of the communication channel is established following the recommendations outlined by the ITU [40]. To achieve this, we first discretize the total atmosphere into 922 homogeneous layers, each exhibiting an exponential variation in thickness. Subsequently, each layer is assigned specific atmospheric parameters, including pressure, temperature, and water vapor density.

The proposed PLS is based on the atmospheric conditions along the channel. The atmospheric parameters such as pressure, temperature and water vapor density have been taken as stochastic such that the SNR shows dynamic variations. By varying the atmospheric parameters, we generate the SINR time-series signal. The scintillation signal from the SINR, which is rapidly varying, is extracted using the MODWT. The mean annual global reference atmosphere given in [53] serves as the basis for computing these atmospheric parameters within each layer of the atmosphere.

The attack model is defined as follows: the drone tunes its power and tries to spoof the ground station while being in the direction of line-of-sight between the ground station and LEO satellite. The attack model has been simulated at a frequency of 70 GHz to check the robustness of the proposed method. At each frequency, we consider elevation angles of 10°, 50°, and 90°, at which the drone varies its power level from 1 to 5 W while the satellite keeps the power level fixed at 5 W. At each elevation angle and given power level, we generate 1000 different SINR datasets. Each SINR dataset consists of 100 time samples. The drone height has been taken at 500 m above the earth's surface. These extensive datasets will allow us to study the effects of the drone's power tuning and its attempted spoofing on the communication link between the satellite and the ground station in the considered scenario. The ML model used to authenticate the source of the signals is an NN with the same specifications as provided in the last subsection.

The dataset contains a total of 2000 samples, with 1000 samples corresponding to satellite signals and 1000 samples corresponding to drone signals. Each sample is represented as a time series consisting of 100 time-domain values. For model development, the dataset is divided into training and testing subsets, where 1500 samples are used for training the network and the remaining 500 samples are reserved for evaluating its performance on unseen data or test data.

We analyze the performance results obtained at the operating frequency of 70 GHz, as illustrated in Figures 10 and 11, for a drone flying at an altitude of 500 m using the LC- and NN-based approaches, respectively. The figures present the authentication rate and missed detection rate for both methods. Since the false alarm rate (FAR) was found to be zero across all evaluated scenarios, the corresponding plots are omitted.

From the results, it is evident that the neural network achieves excellent performance, with an authentication rate consistently reaching 100% for the drone at 500 m altitude. Furthermore, the missed detection rate remains exceptionally low—below 0.5% in all scenarios—and in several cases approaches zero, indicating highly reliable classification. In contrast, the linear classifier (LC) exhibits significantly inferior performance. The authentication rate for LC remains below 70%, while the missed detection rate exceeds 60%, highlighting its limited capability in distinguishing between the two classes under the given conditions. These findings clearly demonstrate the superiority of the proposed NN-based method compared to the LC approach at 70 GHz.

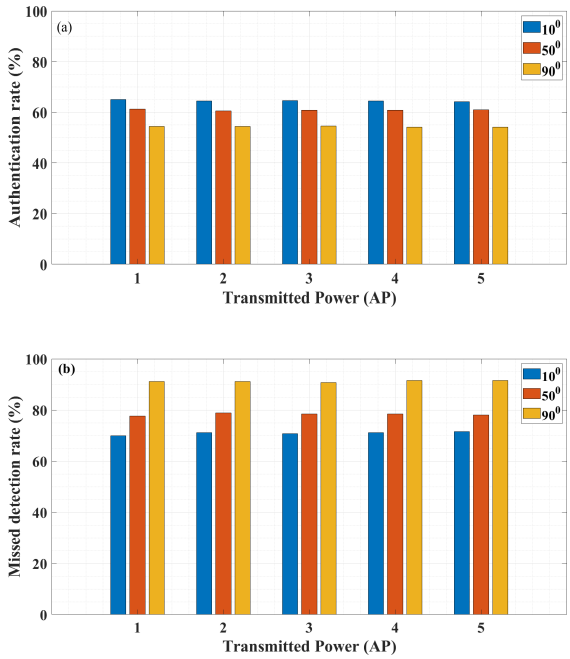


Figure 10. Performance metrics using the proposed method for the altitude of AP at 500 m at a frequency of 70 GHz: (**a**) authentication rate and (**b**) missed detection rate with LC.

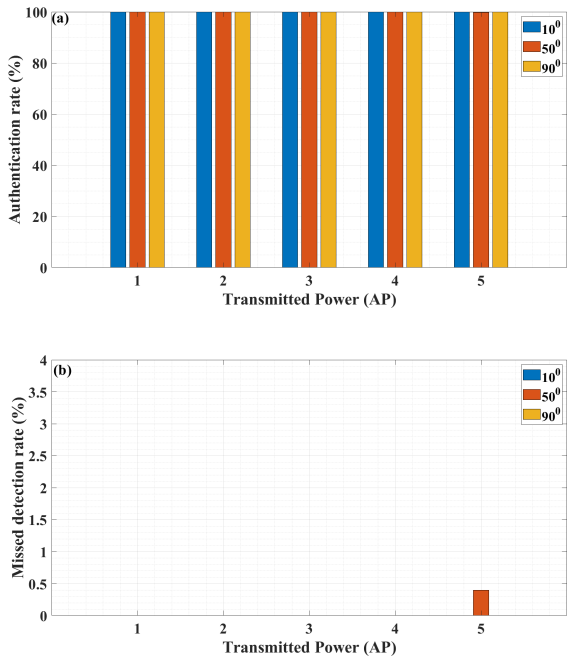


Figure 11. Performance metrics using the proposed method for the altitude of AP at 500 m at a frequency of 70 GHz: (**a**) authentication rate and (**b**) missed detection rate with NN.

To generate realistic time-series data for the SINR, we incorporated models for the variations in atmospheric parameters: pressure, temperature, and water vapor density. These variations are modeled as Gaussian random processes with the following characteristics:

- Mean Values: The average values for each parameter are adopted from the mean annual global reference atmosphere [53].
- Standard Deviations: The standard deviations for the pressure, temperature, and water vapor density variations are set to 10 hPa, 5 K, and 0.5 g/m^3, respectively. The parameters have been taken from [4].

- Furthermore, the tropospheric scintillation fading is modeled as a zero-mean Gaussian random process. The structure constant C_n^2, which characterizes the intensity of turbulence within the atmospheric channel, is set to 10^{-12}, as suggested in [54].

Table 2. Design parameters.

Definition	Symbol	Value
Antenna diameter (GS)		1 m
Antenna efficiency	$\eta_T^s, \eta_T^d, \eta_T^s$	0.8
Antenna temperature	T_p	290 K
Receiver temperature	T_{rx}	400 K
System bandwidth (GS)	B	1 GHz
Antenna diameter (Drone)		0.2 m
LEO transmitted power	P_T^s	5 W
Satellite altitude	h_s	1000 km
Antenna diameter (LEO)		3 m
Earth radius	R_e	6371 km
Earth's temperature	T_g	290 K
Emissivity	ϵ	0.95
Reflection coefficient	ρ_g	0.05

Figure 12 illustrates the receiver operating characteristics (ROC) curve at 70 GHz for the scenario in which the drone operates at an altitude of 500 m above ground level. As shown in the plot, the neural network achieves an almost perfect discrimination capability, yielding an area under the curve (AUC) of 0.9999. In contrast, the linear classifier performs only marginally better than random guessing, with an AUC of 0.5375. This substantial difference highlights the superior ability of the neural network to distinguish between classes under the given propagation conditions.

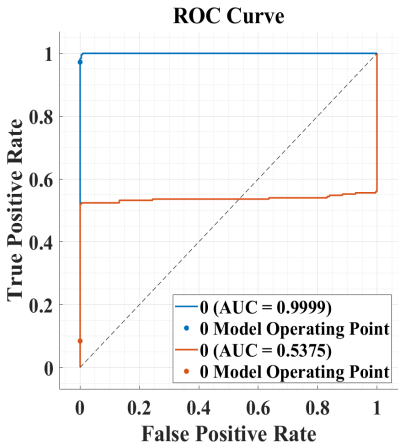


Figure 12. The ROC curve at 70 GHz for a drone at the height of 500 m.

Figures 13 and 14 present the authentication performance of the LC- and NN-based schemes for a drone operating at an altitude of 1000 m at the 70 GHz frequency band. The results are shown across a range of elevation angles to capture the impact of geometric variations on classification accuracy. As depicted, the authentication rate for the LC remains below 75%, indicating limited reliability under these conditions. In contrast, the neural

network consistently achieves an authentication rate of 100%, demonstrating its robustness and effectiveness even at higher altitudes.

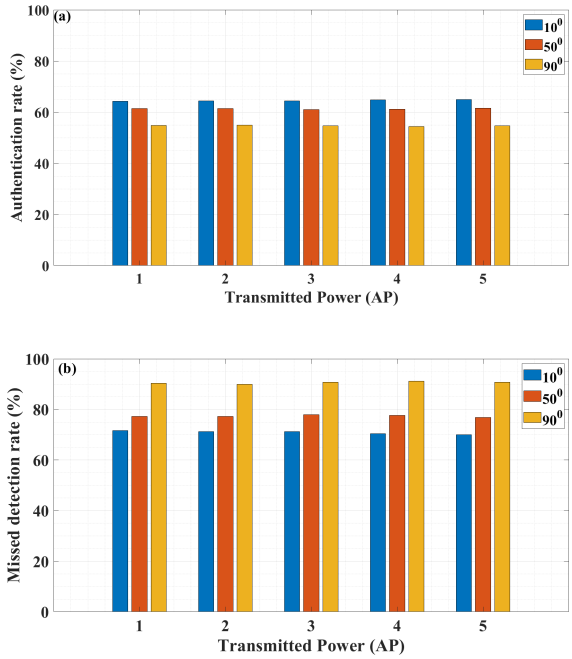


Figure 13. Performance metrics using the proposed method for the altitude of AP at 1000 m at a frequency of 70 GHz: (**a**) authentication rate and (**b**) missed detection rate with LC.

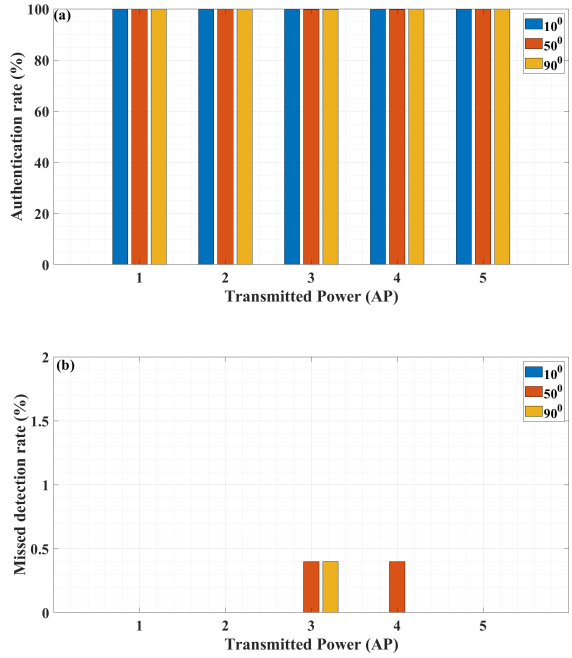


Figure 14. Performance metrics using the proposed method for the altitude of AP at 1000 m at a frequency of 70 GHz: (**a**) authentication rate and (**b**) missed detection rate with NN.

The notable performance gap highlights the advantage of the NN in exploiting rapid SINR variations, which serve as discriminative features for distinguishing between satellite and drone signals. This reinforces the superiority of the NN-based method as a more stable and accurate classification approach.

A similar trend is observed in the missed detection rate (MDR). For the LC, the MDR is approximately 90%, further emphasizing its poor detection capability. Meanwhile, the NN maintains an MDR below 0.5%, indicating highly reliable performance. These observations

collectively confirm the robustness of the proposed NN-based framework across different altitude scenarios.

Figure 15 shows the ROC curve at a height of 1000 m above the ground at a frequency of 70 GHz. The AUC is found to be 1 with neural network and 0.5245 with linear classifier. It again shows the superiority of a neural network with the proposed technique.

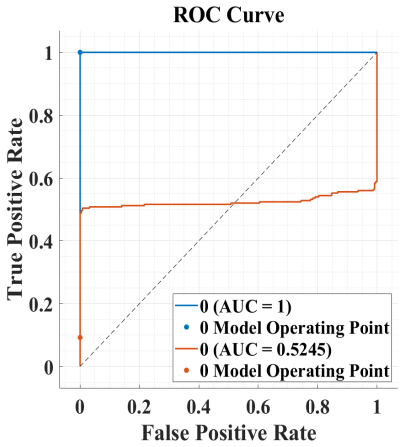


Figure 15. The ROC curve at 70 GHz for a drone at the height of 1000 m.

5. Conclusions

In this work, we presented a novel method that utilizes atmospheric effects to prevent MITM attacks on ground stations from an AP. These effects primarily arise from scintillation fading experienced within the satellite communication channel. We demonstrate that the spatial signatures of rapid SINR variations, extracted using wavelet transforms from the received signal, can be used to identify the source of the signal at the ground station antenna (satellite or AP). The proposed architecture feeds an NN with the extracted rapid fluctuations in the SINR samples, which have traversed distinct spatial paths through the atmospheric channel. In the considered scenario, our network achieves an accuracy exceeding 98%. Furthermore, experimental results obtained from a ground station in Israel validate the concept of utilizing the channel's spatiotemporal imprint (primarily scintillation) for authentication, demonstrating an authentication rate exceeding 98%. As a result, this architecture offers a robust and efficient method to safeguard the PLS of ground station receivers against MITM attacks launched by drones, operating in the line-of-sight direction.

Fundamentally, GEO Ku-band channels differ significantly from LEO/mmWave channels in key aspects such as Doppler dynamics, link intermittency, rain attenuation severity, scintillation statistics, and time-frequency coherence. These differences can materially alter the performance of anomaly detection, channel estimation, and physical-layer security methods. Consequently, extrapolating GEO-based results to LEO/mmWave networks may overstate the generalizability of the findings. However, the LEO channel would still show the scintillation effects as the signal traverses the atmosphere. Such scintillation effects would be missing in the drone's channel as it flies at a much lower height. Therefore, while the simulations presented here focus on Low Earth Orbit (LEO) satellite links, the proposed technique can be readily applied to enhance the security of communication with Medium Earth Orbit (MEO) and Geosynchronous Earth Orbit (GEO) satellites.

It should additionally be noted that packet-level statistics and higher-layer network behaviors are beyond the physical-layer scope of the present study. These characteristics depend on protocol-level interactions, buffering dynamics, and link-level scheduling mechanisms that are not directly addressed by the GEO–GEO physical-layer configuration. A comprehensive analysis of packet statistics and their relationship to spoofing-induced

signal perturbations will be developed in future work, where higher-layer modeling and cross-layer interactions will be incorporated.

Author Contributions: Conceptualization, R.K. and S.A.; Methodology, R.K. and S.A.; Software, R.K. and S.A.; Validation, R.K. and S.A.; Formal analysis, R.K. and S.A.; Investigation, R.K. and S.A.; Resources, S.A.; Writing—original draft, R.K.; Writing—review and editing, R.K. and S.A.; Visualization, R.K.; Supervision, S.A.; Project administration, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zhu, X.; Jiang, C. Integrated Satellite-Terrestrial Networks Toward 6G: Architectures, Applications, and Challenges. *IEEE Internet Things J.* **2022**, *9*, 437–461. [CrossRef]
2. Lin, X.; Cioni, S.; Charbit, G.; Chuberre, N.; Hellsten, S.; Boutillon, J.F. On the Path to 6G: Embracing the Next Wave of Low Earth Orbit Satellite Access. *IEEE Commun. Mag.* **2021**, *59*, 36–42. [CrossRef]
3. Kumar, R.; Arnon, S. Enhancing Cybersecurity of Satellites at Sub-THz Bands. In *Cyber Security, Cryptology, and Machine Learning*; Dolev, S., Katz, J., Meisels, A., Eds.; Springer International Publishing: Cham, Switzerland, 2022; pp. 356–365.
4. Kumar, R.; Arnon, S. Improving Physical Layer Security of Ground Stations Against GEO Satellite Spoofing Attacks. In *International Symposium on Cyber Security, Cryptology, and Machine Learning*; Springer: Cham, Switzerland, 2023; pp. 458–470.
5. Niu, H.; Xiao, Y.; Lei, X.; Chen, J.; Xiao, Z.; Li, M.; Yuen, C. A survey on artificial noise for physical layer security: Opportunities, technologies, guidelines, advances, and trends. *IEEE Commun. Surv. Tutor.* **2025**, 28, 341–381. [CrossRef]
6. Duan, Z.; Chang, Z.; Xie, N.; Sun, W.; Niyato, D. Adaptive Strategies in Enhancing Physical Layer Security: A Comprehensive Survey. *ACM Comput. Surv.* **2025**, *57*, 1–36. [CrossRef]
7. Manulis, M.; Bridges, C.P.; Harrison, R.; Sekar, V.; Davis, A. Cyber security in New Space. *Int. J. Inf. Secur.* **2020**, 20, 287–311. [CrossRef]
8. Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. Satellite-based communications security: A survey of threats, solutions, and research challenges. *Comput. Netw.* **2022**, *216*, 109246. [CrossRef]
9. Venkatesh, S.; Lu, X.; Tang, B.; Sengupta, K. Secure space time-modulated millimetre-wave wireless links that are resilient to distributed eavesdropper attacks. *Nat. Electron.* **2021**, *4*, 827–836. [CrossRef]
10. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.A.; Abreu, G.; Haas, H. Physical-Layer Security in 6G Networks. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1901–1914. [CrossRef]
11. Li, B.; Fei, Z.; Zhou, C.; Zhang, Y. Physical-Layer Security in Space Information Networks: A Survey. *IEEE Internet Things J.* **2020**, *7*, 33–52. [CrossRef]
12. Siles, G.A.; Riera, J.M.; Garcia-del Pino, P. Atmospheric Attenuation in Wireless Communication Systems at Millimeter and THz Frequencies [Wireless Corner]. *IEEE Antennas Propag. Mag.* **2015**, *57*, 48–61. [CrossRef]
13. Rappaport, T.S.; Xing, Y.; Kanhere, O.; Ju, S.; Madanayake, A.; Mandal, S.; Alkhateeb, A.; Trichopoulos, G.C. Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond. *IEEE Access* **2019**, *7*, 78729–78757. [CrossRef]
14. Curiac, D.I. Wireless Sensor Network Security Enhancement Using Directional Antennas: State of the Art and Research Challenges. *Sensors* **2016**, *16*, 488. [CrossRef]
15. Chen, X.; An, J.; Xiong, Z.; Xing, C.; Zhao, N.; Yu, F.R.; Nallanathan, A. Covert communications: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1173–1198. [CrossRef]
16. Lee, S.H.; Wang, L.; Khisti, A.; Wornell, G.W. Covert communication with channel-state information at the transmitter. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2310–2319. [CrossRef]
17. Fontanesi, G.; Ortíz, F.; Lagunas, E.; Garcés-Socarrás, L.M.; Baeza, V.M.; Vázquez, M.Á.; Vásquez-Peralvo, J.A.; Minardi, M.; Vu, H.N.; Honnaiah, P.J.; et al. Artificial intelligence for satellite communication: A survey. *IEEE Commun. Surv. Tutor.* **2025**, 28, 1381–1435. [CrossRef]
18. Kang, B.; Ye, N.; An, J. Achieving Positive Rate of Covert Communications Covered by Randomly Activated Overt Users. *IEEE Trans. Inf. Forensics Secur.* **2025**, *20*, 2480–2495. [CrossRef]

19. Zheng, T.X.; Wang, H.M.; Ng, D.W.K.; Yuan, J. Multi-antenna covert communications in random wireless networks. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 1974–1987. [CrossRef]
20. Gohari, A.; Ahmad, A.B.; Rahim, R.B.A.; Supa, A.S.M.S.; Abd Razak, S.; Gismalla, M.S.M. Involvement of Surveillance Drones in Smart Cities: A Systematic Review. *IEEE Access* **2022**, *10*, 56611–56628. [CrossRef]
21. Derhab, A.; Cheikhrouhou, O.; Allouch, A.; Koubaa, A.; Qureshi, B.; Ferrag, M.A.; Maglaras, L.; Khan, F.A. Internet of drones security: Taxonomies, open issues, and future directions. *Veh. Commun.* **2022**, *39*, 100552. [CrossRef]
22. JOUAV. How High Can A Drone Fly | Highest Altitude Drones 2025. Available online: https://www.jouav.com/blog/how-high-can-a-drone-fly.html (accessed on 2 March 2026).
23. Wu, Z.; Zhang, Y.; Yang, Y.; Liang, C.; Liu, R. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access* **2020**, *8*, 165444–165496. [CrossRef]
24. Yin, Z.; Jia, M.; Cheng, N.; Wang, W.; Lyu, F.; Guo, Q.; Shen, X. UAV-Assisted Physical Layer Security in Multi-Beam Satellite-Enabled Vehicle Communications. *IEEE Trans. Intell. Transp. Syst.* **2022**, *23*, 2739–2751. [CrossRef]
25. Schraml, M.G.; Schwarz, R.T.; Knopp, A. Multiuser MIMO Concept for Physical Layer Security in Multibeam Satellite Systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 1670–1680. [CrossRef]
26. Guo, K.; An, K.; Huang, Y.; Zhang, B. Physical Layer Security of Multiuser Satellite Communication Systems With Channel Estimation Error and Multiple Eavesdroppers. *IEEE Access* **2019**, *7*, 96253–96262. [CrossRef]
27. Li, J.; Han, S.; Tai, X.; Gao, C.; Zhang, Q. Physical Layer Security Enhancement for Satellite Communication Among Similar Channels: Relay Selection and Power Allocation. *IEEE Syst. J.* **2020**, *14*, 433–444. [CrossRef]
28. Geng, R.; Ye, N.; Liu, J.; Zhu, D. Towards channel state information based coding to enhance security in satellite communication. *J. Syst. Archit.* **2021**, *112*, 101843. [CrossRef]
29. Abdrabou, M.; Gulliver, T.A. Physical Layer Authentication for Satellite Communication Systems Using Machine Learning. *IEEE Open J. Commun. Soc.* **2022**, *3*, 2380–2389. [CrossRef]
30. Oligeri, G.; Sciancalepore, S.; Raponi, S.; Pietro, R.D. PAST-AI: Physical-Layer Authentication of Satellite Transmitters via Deep Learning. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 274–289. [CrossRef]
31. Jung, S.; Im, G.; Jung, D.H.; Kim, P.; Ryu, J.G.; Kang, J. Performance analysis of DSSS- and CSS-based physical layer for IoT transmission over LEO satellites. *ETRI J.* **2022**, *44*, 543–559. [CrossRef]
32. Abdrabou, M.; Gulliver, T.A. Threshold-Based Physical Layer Authentication for Space Information Networks. In Proceedings of the 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Solo, Indonesia, 3–5 November 2022; pp. 289–293. [CrossRef]
33. Kumar, R.; Arnon, S. Authentication Method for Spoofing Protection in Communication and Navigation Satellites: Utilizing Atmospheric Signature. *IEEE Commun. Lett.* **2024**, *28*, 128–132. [CrossRef]
34. Jiang, C.; Zhang, C.; Mu, L.; Zhang, Z.; Ge, J. Aerial RIS-aided physical layer security design for satellite communication among similar channels. *J. Inf. Intell.* **2023**, *1*, 54–67. [CrossRef]
35. Li, J.; Han, C.; Ye, N.; Pan, J.; Yang, K.; An, J. Instant Positioning by Single Satellite: Delay-Doppler Analysis Method Enhanced by Beam-Hopping. *IEEE Trans. Veh. Technol.* **2025**, *74*, 14418–14431. [CrossRef]
36. Ibwe, K.S. Sparse hybrid-field channel estimation in massive MIMO systems. *J. Electr. Syst. Inf. Technol.* **2025**, *12*, 86. [CrossRef]
37. Wang, H.; Zhang, K.; Fu, Q.; Wen, F.; Li, X. Enhanced channel estimation for hybrid-field XL-MIMO systems using joint sparse Bayesian learning. *IEEE Wirel. Commun. Lett.* **2025**, *14*, 3099–3103. [CrossRef]
38. Chen, L.; Ouyang, X.; Zeng, F.; Rui, Z.; Ming, Y. GNSS spoofing detection based on lightweight features and CGAN-ANN in unknown scenarios. *GPS Solut.* **2025**, *29*, 175. [CrossRef]
39. Sun, Z.; Wu, J.; Yang, J.; Huang, Y.; Li, C.; Li, D. Path planning for GEO-UAV bistatic SAR using constrained adaptive multiobjective differential evolution. *IEEE Trans. Geosci. Remote Sens.* **2016**, *54*, 6444–6457. [CrossRef]
40. ITU. *Recommendation: Attenuation by Atmospheric Gases and Related Effects*; ITU: Geneva, Switzerland, 2019; pp. 676–712.
41. Kumar, R.; Arnon, S. SNR Optimization for LEO Satellite at Sub-THz Frequencies. *IEEE Trans. Antennas Propag.* **2022**, *70*, 4449–4458. [CrossRef]
42. Marzano, F. Modeling antenna noise temperature due to rain clouds at microwave and Millimeter-wave frequencies. *IEEE Trans. Antennas Propag.* **2006**, *54*, 1305–1317. [CrossRef]
43. Bousquet, M.; Bousquet, G.; Sun, Z. *Satellite Communications Systems: Systems, Techniques and Technology*, 5th ed.; John Wiley & Sons: Hoboken, NJ, USA, 2009.
44. Series, P. Propagation data and prediction methods required for the design of Earth-space telecommunication systems. In *Recommendation ITU-R*; ITU: Geneva, Switzerland, 2015; pp. 618–712.
45. Liu, W.; Michelson, D.G. Effect of Turbulence Layer Height and Satellite Altitude on Tropospheric Scintillation on Ka-Band Earth–LEO Satellite Links. *IEEE Trans. Veh. Technol.* **2010**, *59*, 3181–3192. [CrossRef]

46. Kumar, R.; Arnon, S. Deep Learning based Scintillation Prediction for Satellite Link using Measured Data. In Proceedings of the 2022 45th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic, 13–15 July 2022; pp. 246–249. [CrossRef]
47. Ayecka. Ayecka Communications: TC1 Pro 2023. Available online: https://www.ayecka.com/tc-1 (accessed on 2 March 2026).
48. Yan, C.; Fu, L.; Zhang, J.; Wang, J. A Comprehensive Survey on UAV Communication Channel Modeling. *IEEE Access* **2019**, *7*, 107769–107792. [CrossRef]
49. Khuwaja, A.A.; Chen, Y.; Zhao, N.; Alouini, M.S.; Dobbins, P. A Survey of Channel Modeling for UAV Communications. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2804–2821. [CrossRef]
50. Zarrinnegar, K.; Sormayli, J.; Mosavi, M. Robust GNSS spoofing detector using optimized machine learning model on embedded platforms. *GPS Solut.* **2025**, *30*, 24. [CrossRef]
51. Mohanty, A.; Gao, G. A Survey of Machine Learning Techniques for Improving Global Navigation Satellite Systems. *arXiv* **2024**. [CrossRef]
52. Abdrabou, M.; Gulliver, T.A. Authentication for Satellite Communication Systems Using Physical Characteristics. *IEEE Open J. Veh. Technol.* **2023**, *4*, 48–60. [CrossRef]
53. ITU. *Recommendation P.618-14: Propagation Data and Prediction Methods Required for the Design of Earth-Space Telecommunication Systems*; ITU: Geneva, Switzerland, 2023.
54. Pereira, C.; Vanhoenacker-Janvier, D.; Jeannin, N.; Castanet, L.; Martellucci, A. Simulation of tropospheric scintillation on LEO satellite link based on space-time channel modeling. In Proceedings of the 8th European Conference on Antennas and Propagation (EuCAP 2014), Hague, The Netherlands, 6–11 April 2014; pp. 3516–3519. [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.