Eavesdropping of Terahertz RIS-enabled HAPS-integrated satellite communication

1st Daan van der Eijk
Department of Mathematics
University of Padua
Padua, Italy
daanjannes.vandereijk@studenti.unipd.it

2nd Simone Soderi
Department of Mathematics
University of Padua
Padua, Italy
simone.soderi@unipd.it

3rd Mauro Conti
Department of Mathematics
University of Padua, Italy
and
AI, Robotics and Cybersecurity Center (ARC)
Örebro University, Sweden
mauro.conti@unipd.it

***Abstract*—Satellite Communication (SatCom) systems are evolving rapidly to meet increasing demands for high-speed data transmission. In this context, the Terahertz (THz) frequency band has gained attention due to its untapped high bandwidth, but introduces new Physical-Layer Security (PLS) challenges, especially in uplinks to Low-Earth Orbit (LEO) satellites, where scattering due to atmospheric influence may enable interception outside the main beam. Integrating a Reconfigurable Intelligent Surface (RIS)-enabled High Altitude Platform Station (HAPS) as a relay node offers a promising approach to mitigating these security risks.**

In this work, we propose, to the best of our knowledge, the first deterministic 2D single-scattering model specifically tailored to evaluate Non-Line-Of-Sight (NLOS) eavesdropping risks in THz-band satellite uplinks. The model includes atmospheric attenuation, Free Space Path Loss (FSPL), and single-scattering effects to analytically compute the Signal-to-Noise Ratio (SNR) and Secrecy Capacity (SC) for both legitimate and eavesdropping links under varying weather conditions. Simulations reveal non-negligible insecure spatial areas around the communication beam where the SC drops to zero. However, using a RIS-enabled HAPS reduces this area by 48%. These findings reveal key physical-layer risks in THz communication while simultaneously showing the potential of RIS-assisted HAPS in securing THz-frequency Non-Terrestrial Network (NTN) uplinks against these risks.

***Index Terms*—Low Earth orbit satellites, Satellite communications, Attenuation, Scattering, Atmospheric modelling**

I. Introduction

Nielsen's law states that the Internet connection speed of high-end users grows by approximately 50% per year [1]. To meet the growing demand for low-latency Internet, Non-Terrestrial Networks (NTNs) are being explored [2]. These networks integrate satellites and Inter-Satellite Links (ISLs) to achieve high data rates [3]. The significant reduction in space launch costs over the last decade has enabled the deployment of Low-Earth Orbit (LEO) satellite networks for global Internet access, including SpaceX's Starlink [4] and the European Union (EU)'s IRIS^2 [5], which is expected to be operational by 2030.

Satellite Communication (SatCom), which considers a user, ground, and space segment [6], has simultaneously emerged as a prominent target for cyber threats [7]. The growing importance of satellite security is reflected in the EU's 2023 Space Strategy for Security and Defence, which highlights the urgency of addressing increasing cyber risks [8]. Real-world incidents, such as satellites manoeuvring suspiciously close to other communication satellites [9], and systematic jamming of navigation systems [10], emphasize the relevance and existence of real-time cyber risks. Therefore, as new SatCom technologies push the boundaries of speed and capacity, it is essential that research efforts equally prioritize ensuring the security of these communications.

In addition to SatCom, the Third Generation Partnership Program (3GPP) is exploring the use of High Altitude Platform Station (HAPS) in NTNs, which also consider an air segment, for Sixth Generation (6G) Internet [11]. HAPS, which are unmanned vehicles in the stratosphere, can maintain quasi-stationary positions, enabling high-speed and ubiquitous internet access [12]. Recent advancements in solar panel efficiency, lightweight composite materials, and autonomous avionics have significantly enhanced their performance and viability [13]. Additionally, HAPS mega-constellations are theorized to enable low-latency, secure, and efficient long-distance communication with satellites [11].

An additional promising technology to address the growing demand for high-speed Internet is Reconfigurable Intelligent Surface (RIS) [14]. A RIS consists of a large array of passive reflecting elements on a flat surface, which can individually control the phase shifts and reflection angles of incident electromagnetic waves [15]. This enables dynamic beam forming, mitigation of multipath fading, and support for full-duplex communication without the constraints of conventional relays, and with minimal power consumption [16]–[19]. This is a particularly significant advantage over traditional relay technology for HAPS platforms, where limited energy-storage capacity remains a key barrier to large-scale deployment [20]. However, RIS-assisted communication suffers from multiplicative fading, where the end-to-end path loss is the product of the losses over each individual segment, resulting in significantly degraded signal strength compared to direct communication. To address this limitation, active RIS elements capable of signal amplification have been proposed, at the cost of introducing additional noise [21].

Moreover, research and standards organizations for telecommunications are exploring the use of the 0.1-1 Terahertz (THz) frequency bands for satellite communication, also in combination with active or passive RIS [22]. Due to its untapped wide bandwidth, the THz spectrum is attractive for high-data-rate communication [23]. RIS-assisted systems operating in this band have already been demonstrated to enhance achievable ISL capacity [24]. Despite these benefits, THz signals suffer from severe path loss due to atmospheric effects over long distances [25].

Combining HAPS, RIS technology, and use of the THz frequency band offers a promising approach to sustaining the exponential network capacity growth predicted by Nielsen's law [26], [27]. Despite promising advancements, comparatively little research has focused on the security aspect of these state-of-the-art systems. An effective approach to securing high-speed RIS-enabled links lies in the application of Physical-Layer Security (PLS) techniques [15]. PLS exploits the inherent properties of the communication channel to provide information-theoretic confidentiality [28]. It complements upper-layer cryptographic methods, which may be impractical in NTN scenarios where strict trade-offs in payload design in terms of energy use and computational power make traditional encryption less effective [29].

The following subsection reviews existing literature on the application of PLS to systems involving HAPS, RIS technology, and communication over the THz band.

A. Related works

The PLS of a THz point-to-point channel was considered in [30], building on earlier work by [31]. Their study evaluates the Secrecy Capacity (SC) and Secrecy Outage Probability (SOP) of the channel by considering both the legitimate Line-Of-Sight (LOS) and the Non-Line-Of-Sight (NLOS) channel caused by scattering of the signal. They identified a non-trivial insecure region where an eavesdropper could receive a stronger signal than the legitimate receiver, resulting in an SC of zero.

Furthermore, the PLS of a legitimate optical satellite-to-HAPS communications with a malicious satellite eavesdropping was investigated in [32]. The Average Secrecy Capacity (ASC), SOP, and Secrecy Throughput (ST) were calculated for both the uplink, which refers to communication towards the satellite, and the downlink, which refers to communication returning from the satellite [6]. Monte Carlo simulations demonstrated that downlink communication was more secure. Additionally, turbulence-induced fading was found to significantly degrade secrecy performance.

THz uplink communication from ground stations to HAPS in the presence of multiple eavesdropping HAPS was analysed in [33]. The authors developed a comprehensive statistical model for the THz feeder link that incorporated key impairments, including molecular absorption, path loss, and atmospheric turbulence. They derived closed-form expressions for SOP and SC under realistic THz channel conditions, accounting for beam misalignment and multipath fading effects. Their analysis revealed that accurate THz channel modelling was crucial for evaluating and enhancing physical layer security in integrated ground-aerial networks, especially when facing multiple aerial eavesdroppers.

Finally, the security of THz RIS-HAPS-enabled satellite-to-ground downlink communication in the presence of terrestrial eavesdroppers was investigated in [34]. The authors derived expressions for the Ergodic Secrecy Rate (ESR) and proposed algorithms leveraging the Channel State Information (CSI) of the receivers to enhance system security. Simulation results demonstrated that the use of the RIS and the proposed algorithms significantly improved the overall security of the system. This is the only previous work that has considered the PLS of RIS-HAPS-enabled satellite communication in the THz frequency band.

B. Contributions

This work makes the following key contributions:

1) We propose calculations for the SC of active RIS-enabled HAPS THz ground-to-satellite uplink communication. While the downlink scenario has been studied previously [34], to the best of our knowledge, this is the first work addressing the uplink.
2) We introduce a deterministic 2D single-scattering model for NTN THz communication that accurately captures the received signal at an eavesdropper, accounting for atmospheric effects.
3) We quantify the security benefits of employing a RIS-enabled HAPS in ground-to-satellite communication in different weather conditions through multiple security metrics.

C. Organization

The remainder of this paper is organized as follows. Section II presents the model used to calculate attenuation caused by atmospheric effects, as well as the model for computing the NLOS channel coefficient. In Section III, we introduce the calculations for determining the secrecy capacity of the system. Section IV explores the model through simulations. Finally, Section V concludes the paper with remarks on the implications of this research.

II. System Model

This section formalizes the mathematical framework underlying the communication model. It outlines how the distances between system entities are computed in Subsection A and presents the attenuation calculations that characterize signal degradation along the transmission path in Subsections B, C, and D.

A. Distance Calculations

For simplicity, we consider all entities located on a two-dimensional plane, where the horizontal axis x represents distance along the ground and the vertical axis y corresponds to altitude. The ground station is set as the reference point in this coordinate system. We consider a transmitting ground station A, a RIS-integrated HAPS R, and a receiving satellite B. A is located in the graph at (x_A, y_A), the HAPS R at (x_R, y_R)

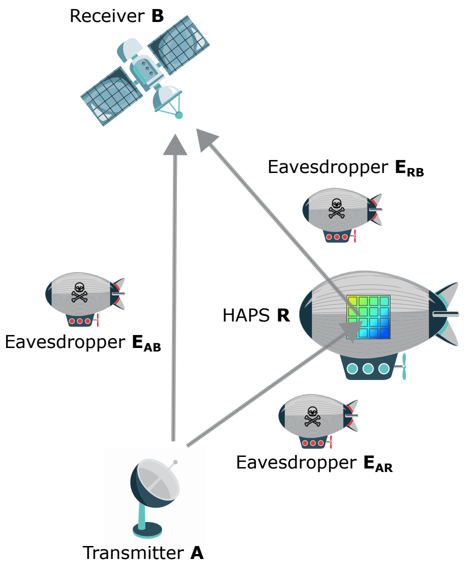


Fig. 1: Representation of the direct scenario and the RIS-enabled HAPS scenario with eavesdroppers.

and B at (x_B, y_B). The direct scenario has one eavesdropper E_{AB}, whose location is denoted as $(x_{E_{AB}}, y_{E_{AB}})$. The RIS-enabled HAPS scenario has two eavesdroppers: one positioned between the ground station and the HAPS and one between the HAPS and the satellite. These eavesdroppers are denoted as E_{AR} and E_{RB} respectively, and their location is given as $(x_{E_{AR}}, y_{E_{AR}})$ and $(x_{E_{RB}}, y_{E_{RB}})$.

1) Cartesian Distances: The distance between the legitimate transmitter and the eavesdropper depends on the point on the legitimate link where the signal scatters towards the eavesdropper, which will be explained in more detail in Section II-D. This scattering point L_X, with $X \in \{AR, RB, AB\}$, since we model scattering on all three links, is located at coordinates (x_{L_X}, y_{L_X}). Relevant for the distance calculations is that the scattering points lie along the legitimate links, which in the direct scenario is defined as

$$y_{L_{AB}} = \frac{y_B - y_A}{x_B - x_A} \cdot x_{L_{AB}}, \tag{1}$$

with similar expressions for $y_{L_{AR}}$ and $y_{L_{RB}}$ in the RIS-enabled HAPS scenario. Figure 2 illustrates a signal propagating along the legitimate channel and subsequently scattering toward the eavesdropper within its Field of View (FoV).

Given the scattering point, we calculate the distances between ground station A and the eavesdroppers as

$$\begin{aligned} d_{AE_X} \quad = \quad & I_{|X=RB}\, d_{AR} + \\ & \sqrt{(x_{L_X} - x_{P_X})^2 + (y_{L_X} - y_{P_X})^2} + \\ & \sqrt{(x_{E_X} - x_{L_X})^2 + (y_{E_X} - y_{L_X})^2}, \end{aligned} \tag{2}$$

where the point P_X is the location of the legitimate transmitter

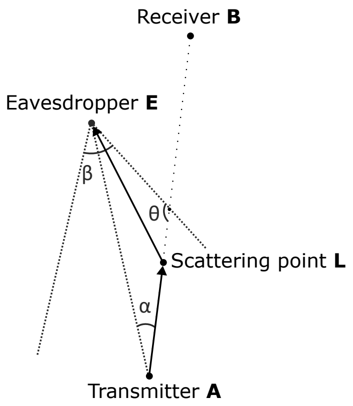


Fig. 2: Geometric representation of a scattered signal in the direct scenario.

and

$$I_{|X=RB} = \begin{cases} 1, & X = RB \\ 0, & \text{otherwise} \end{cases}, \tag{3}$$

which takes into account that a signal scattering from the RB link has also already travelled across the AB link.

2) Sliced Atmosphere Distances: The effects of some types of signal attenuation vary as a function of altitude as the signal travels through the atmosphere. To simplify the analysis, the atmosphere is subdivided into N horizontal layers of thickness $\hat{\delta}_m$ [35]. The thickness of layer m in km is given as

$$(\hat{\delta}_m) = 0.0001 \exp\left(\frac{m-1}{100}\right). \tag{4}$$

The distance that the signal travels through each layer of the atmosphere is given as

$$d_m = \frac{\hat{\delta}_m}{\sin \omega}, \tag{5}$$

$$\omega = \begin{cases} \zeta, & \text{if } m \leq z \\ \psi, & \text{if } m > z \end{cases}, \tag{6}$$

where z denotes the index of the layer containing the RIS, ζ is the elevation angle of the signal path from the ground station to the RIS, and ψ is the elevation angle from the RIS to the satellite.

B. Atmospheric Attenuation

Attenuation represents a decrease in signal power in transmission from one point to another. The overall attenuation h_{atm} the signal experiences due to atmospheric influence over path length d is given following Beer-Lambert law as [30], [36], [37]

$$h_{atm} = e^{-\alpha_{atm} d} = e^{-(\alpha_T + \alpha_A + \alpha_S + \alpha_R)d}, \tag{7}$$

with α_T the attenuation due to atmospheric turbulence, α_A the attenuation due to absorption by gases like water vapour, α_S the attenuation due to scattering, and α_R the attenuation due to rain. The following subsections will give insight into the calculation of these attenuation factors.

1) Atmospheric Turbulence Attenuation: We use the layered atmosphere model to model the different levels of atmospheric turbulence at different altitudes. We have [30], [38]

$$\alpha_T = \frac{|10 \log (1 - \sqrt{\sigma_I^2})|}{\sum_{m=1}^{N} d_m}, \tag{8}$$

with slice distance d_m, where the total scintillation index σ_I^2 is equal to the sum of all scintillation indices of the slices that the signal traversed [39]

$$\sigma_I^2 = \sum_{m=1}^{N} \sigma_I^2(d_m). \tag{9}$$

2) Absorption Attenuation: The absorption attenuation is given as in ITU-R P.676 [35], which defines absorption loss up to 1 THz for a slant path through the atmosphere. The values for dry air pressure p, temperature T, and water-vapour density ρ as functions of altitude up to 100 km are calculated according to the standard atmosphere model in [40]. At altitudes above 100 km, the level of absorption attenuation becomes negligible and is therefore not considered in this analysis.

As before, the layered atmosphere model is employed to account for the variation in absorption attenuation as the signal propagates through the atmosphere. Accordingly, the total absorption attenuation due to atmospheric gases is given by

$$\alpha_A = \sum_{m=1}^{N} \gamma_m, \tag{10}$$

where γ_m denotes the specific attenuation in the m-th atmospheric layer.

3) Scattering Attenuation: Scattering attenuation, which primarily occurs within the troposphere, is modelled using Mie scattering [41]. Since this type of attenuation is assumed to remain relatively constant throughout the troposphere, the layered atmosphere model is not applied to this attenuation factor. Its contribution over the total propagation distance is approximated using the Kruse relation [31], [42]

$$\alpha_S = \frac{d_t}{d} \cdot \frac{3.912}{V} \left(\frac{\lambda_{nm}}{550_{nm}} \right)^{-q}, \tag{11}$$

with visibility V in kilometres, wavelength λ in nanometres, distance travelled through the troposphere d_t, total distance travelled d, and piecewise function q.

4) Rain Attenuation: The attenuation due to rain over a total distance d can be calculated for frequencies up to 1 THz using ITU-R P.838 [43]

$$\alpha_R = \frac{d_{h_R}}{d} \cdot k R^{\alpha}, \tag{12}$$

where d_{h_R} is the distance travelled below the mean annual rain height, which can be calculated from the freezing level altitude [44], R is the rain rate in mm/h, and coefficients k and α are frequency-dependent coefficients obtained from curve-fitting power-law expressions as given in [43].

C. Free Space Path Loss (FSPL)

Under FSPL the received signal is given as [37]

$$y(t) = \text{Re} \left\{ \left[\frac{\lambda \sqrt{G_t G_r} u(t - \tau_l) e^{-j \frac{2\pi d}{\lambda}}}{4\pi d} \right] e^{j 2\pi f_c t} \right\}, \tag{13}$$

with transmitter and receiver gain G_t, G_r, distance travelled d and wavelength λ, time delay $\tau_l = d/c$, carrier frequency f_c, and baseband signal $u(t)$.

Time delay τ_l affects timing but not the amplitude or phase shift relevant for physical layer security, and can therefore be neglected [37]. The term $e^{j2\pi f_c t}$ represents the carrier oscillation, but since we focus on the complex envelope of the received signal, the free-space path loss effect can be captured by the channel coefficient

$$h_{FSPL} = \frac{\sqrt{G_t G_r} \lambda}{4\pi d} \cdot e^{-j \frac{2\pi d}{\lambda}}, \tag{14}$$

and it represents the amplitude and phase shift of the received signal as a function of the distance it travels.

D. NLOS Attenuation

The NLOS attenuation for a THz system with an eavesdropper E_X, with $X \in \{AR, RB, AB\}$, is given as [30], [37]

$$\begin{aligned} h_{\text{NLOS},E_{AR}} = \; & \sqrt{G_T G_{E_X}} \cdot \\ & \int_{L_a}^{L_b} \Omega(x_l)\, p(\mu_{E_X})\, \alpha_{\text{sca},E_X} \cdot \\ & e^{-\alpha_{\text{atm},X} d_X}\, dx_l, \end{aligned} \tag{15}$$

with legitimate transmitter antenna gain G_T and eavesdropper antenna gain G_X. The term α_{sca} incorporates only the scattering attenuation α_S and the rain attenuation α_R. The integral captures the scattered energy along the legitimate link towards the respective eavesdropper. The integration is limited to the section of the legitimate link that the eavesdropper can observe. This is then multiplied by the square root of the product of the antenna gains at the legitimate transmitter and the eavesdropper, representing the directional gain effects on both ends of the link. The details for the integration bounds and the calculation of factors $\Omega(x_l), p(\mu_{E_X})$, can be found in Appendix A.

III. Problem formulation

In this section, we discuss how the received signal can be calculated from the attenuation factors in Subsections A and B. We then calculate the Signal-to-Noise Ratio (SNR) from these received signals in Subsections C, D, and E, and finally compute the SC of the legitimate channels based on their performance against their respective eavesdropper in Subsection F.

TABLE I: Relevant channel attenuation factors (weak: $C_n^2 < 10^{-17}$, strong: $C_n^2 > 10^{-13}$)

Channel	FSPL	NLOS	Atmospheric influence
AR	✓	✗	✓ (strong)
RB	✓	✗	✓ (weak)
AB	✓	✗	✓ (weak)
$\mathrm{AE_{AR}}$	✗	✓	✓ (strong)
$\mathrm{RE_{RB}}$	✗	✓	✓ (weak)
$\mathrm{AE_{AB}}$	✗	✓	✓ (strong)

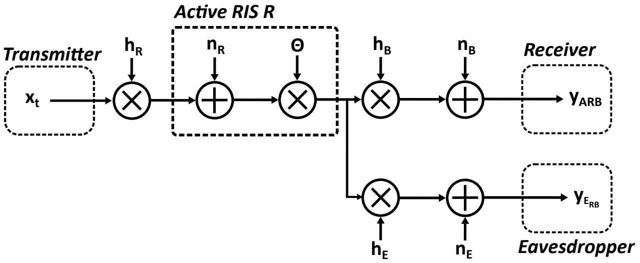


Fig. 3: Wiretap model for signal via active RIS-enabled HAPS.

A. Received signal of legitimate link

The received signal captures the impact of transmission, propagation, and reception of a signal through the atmosphere in the presence of noise. This subsection explains how the received signal is calculated for each legitimate link. We use the classic wiretap model to represent links without RIS influence [28]. For links affected by RIS, the model depicted in Fig. 3 is applied. Table I summarizes the attenuation factors relevant to each channel.

1) Direct model: For the direct AB channel, the signal received by satellite B from ground station A at time slot t is given by

$$y_{t,AB} = \sqrt{P} h_{AB} x_t + n_{AB}, \tag{16}$$

with the pilot signal transmitted $x_t \in \mathbb{C}, |x_t| = 1$, transmit power P, AWGN $n_{t,AB} \sim \mathcal{CN}(0, \sigma_{AB}^2)$ and channel coefficient

$$h_{AB} \quad = h_{FSPL} \cdot h_{atm} \tag{17}$$

2) RIS-enabled model: THz communication relies on highly directional beams that are narrowly focused on the intended receiver [24]. Due to this, and the high relative velocity of the satellite, a signal aimed at the HAPS is extremely unlikely to instead reach the satellite. We therefore consider only the RIS-enabled signal path via the HAPS. The signal received by satellite B from the ground station A via the active RIS-integrated HAPS R at time slot t is expressed as [45]

$$y_{t,ARB} = \sqrt{P}(\mathbf{h}_{RB} \mathbf{\Theta}_t \mathbf{h}_{AR}) x_t + \mathbf{h}_{RB} \mathbf{\Theta}_t \mathbf{n}_{t,AR} + \mathbf{n}_{t,RB}, \tag{18}$$

with the pilot signal transmitted $x_t \in \mathbb{C}, |x_t| = 1$, transmit power P, AWGN $\mathbf{n}_{t,RB} \sim \mathcal{CN}(0, \sigma_{RB}^2 \mathbf{I}_{N_B})$ for N_B antennas, RIS-amplified noise $\mathbf{n}_{t,AR} \sim \mathcal{CN}(0, \sigma_{AR}^2 \mathbf{I}_M)$ for M RIS-elements, AR channel $\mathbf{h}_{AR} \in \mathbb{C}^{M \cdot 1}$, and RB channel $\mathbf{h}_{RB} \in \mathbb{C}^{N_B \cdot M}$. For the reflection coefficient matrix we have $\mathbf{\Theta}_t = \mathrm{diag}(\boldsymbol{\theta}_t)$, with corresponding reflection coefficients $\boldsymbol{\theta}_t = [\theta_{t,1}, ..., \theta_{t,M}]^T$, where $\theta_{t,m} = \alpha_m e^{j\phi_{t,m}}$. Here, α_m represents the amplitude gain factor introduced by the active RIS elements. We define the AR channel as $\mathbf{h}_{AR} = [h_{AR,1}, ..., h_{AR,M}]$ where the channel coefficient is defined using the same physical model as h_{AB}, and the RB channel is defined in the same manner as $\mathbf{h}_{RB} = [h_{RB,1}, ..., h_{RB,M}]$.

B. Received signal of wiretap links

This subsection explains how the received signal is calculated for the links towards the eavesdropper.

1) Direct model: We can express the received signal at the eavesdropper HAPS positioned between the ground station and the legitimate satellite in time frame t as

$$y_{t,E_{AB}} = \sqrt{P} h_{E_{AB}} x_t + n_{E_{AB}}, \tag{19}$$

with AWGN $n_{t,E_{AB}} \sim \mathcal{CN}(0, \sigma_{E_{AB}}^2)$ and

$$h_{E_{AB}} \quad = h_{NLOS,E_{AB}}. \tag{20}$$

2) RIS-enabled model: The received signal at the eavesdropper E_{AR} is calculated similar to the received signal of the eavesdropper E_{AB} in the direct model.

Since the eavesdropper HAPS between the legitimate RIS-integrated HAPS receives a signal influenced by the RIS, the received signal is calculated similar to Equation (18), with $\mathbf{h}_{E_{RB}} = [h_{E_{RB},1}, ..., h_{E_{RB},M}]$ where $h_{E_{RB},m}$ is similar to $h_{E_{AB}}$.

C. SNR of legitimate links

The SNR can be interpreted as a measure of how much stronger the desired signal is compared to the background noise. This subsection explains how to calculate the SNR from the received signal for the legitimate links.

1) Direct model: The SNR of the legitimate direct link is given as

$$\gamma_{AB} = \frac{P|h_{AB}|^2}{\sigma_{AB}^2}. \tag{21}$$

2) RIS-enabled model: The SNR of the legitimate link is given as

$$\gamma_{ARB} = \frac{P\left|\mathbf{h}_{RB} \mathbf{\Theta}_t \mathbf{h}_{AR}\right|^2}{\sigma_{AR}^2 |\mathbf{h}_{RB} \mathbf{\Theta}_t|^2 + \sigma_{RB}^2}, \tag{22}$$

where we note that the gain of the RIS G_R will be applied twice because it is both a receiver and a transmitter [46]. This formula can be extended to

$$\begin{aligned} \gamma_{ARB} \quad &= \frac{P\left|\sum_{m=1}^{M} h_{RB,m} \alpha_m e^{j\phi_{t,m}} h_{AR,m}\right|^2}{\sigma_{AR}^2 \sum_{m=1}^{M} |h_{RB,m} \alpha_m e^{j\phi_{t,m}}|^2 + \sigma_B^2} \\ &= \frac{PM^2\left|h_{RB} \alpha_m e^{j\phi_t} h_{AR}\right|^2}{\sigma_{AR}^2 M |h_{RB} \alpha_m e^{j\phi_t}|^2 + \sigma_{RB}^2}, \end{aligned} \tag{23}$$

where m represents the RIS-elements. Because they are assumed to be identical, they introduce a combined factor M [47].

D. SNR of wiretap links

The SNR for the eavesdropper in the direct scenario $\gamma_{E_{AB}}$ and eavesdropper $\gamma_{E_{AR}}$ in the RIS-enabled HAPS scenario are calculated similar to Equation (21). Because eavesdropper $\gamma_{E_{RB}}$ receives the RIS-influenced signal, we calculate the SNR similar to Equation (22).

E. Maximum SNR for RIS-enabled model

Similar to [48]–[51], we assume the worst-case scenario for the instantaneous SNR of the eavesdropper E_{RB}. Therefore, we pick

$$\phi_{t,m} = \vartheta_{R,m} + \vartheta_{E_{RB},m}, \tag{24}$$

where $\vartheta_{R,m}$ and $\vartheta_{E_{RB},m}$ represent the phase shift for the channel coefficients. Picking $\phi_{t,m}$ like this cancels out the channel phases, allowing the eavesdropper E_{RB} to achieve achieve the maximum SNR. Since γ_{AB}, $\gamma_{E_{AB}}$, and $\gamma_{E_{AR}}$ do not have any RIS influence, their maximum SNR values remain the same as those previously calculated.

F. Secrecy Capacity (SC)

The SC can be calculated using the SNRs as [52]

$$C_s^{Ex} = \max\left\{\log_2(1+\gamma_{\mathrm{m}}) - \log_2(1+\gamma_{\mathrm{e}}),\, 0\right\}, \tag{25}$$

where γ_{m} and γ_{e} represents the SNR of the legitimate main link and their respective eavesdropper.

IV. Numerical results

This section discusses how the security of the system model was analyzed through the use of Python simulations. It first outlines the setup of the simulations in Subsections A and B, and then analyzes the simulation results in Subsections C and D.

A. Simulation Setup

The simulation setup and parameter values used in the experiments are summarized in Tables II and III. The weather condition should corresponds to a 99.99% percentage uptime scenario for the considered location, as specified in ITU-R Recommendation P.837-7 [53]. For Noordwijk, the Netherlands, this is the Strong Rain weather condition.

TABLE II: Simulation overview

Component	Details
Ground Station	Altitude: 0 km Antenna: 2 m diameter Location: Noordwijk, Netherlands Season: Summer
RIS-HAPS	Altitude: 18 km RIS surface: 1.5 × 1.5 m
Satellite	Altitude: 550 km Antenna: 1 m diameter
Eavesdroppers	Antenna: 0.5 m diameter
Weather condition	Strong rain (ITU-R 1817-1)

TABLE III: Parameter overview

Name	Sign	Value
Frequency	f	240 GHz
Noise temperature	T	303.15 K
Bandwidth	B	10 GHz
Transmit Power	P	10 W
RIS/antenna efficiency	η	0.65
Troposphere altitude	h_t	9 km
Ground wind speed	ω_g	21 m/s
Beam slew rate	ω_s	0.02 rad/s
Ground level C_n^2	A_{ground}	1.7×10^{-14} m$^{2/3}$
Polarization tilt	τ	45°
Freezing level altitude	h_0	2.6 km
Eavesdropper FoV	β	40°
HG asymmetry factor	g	0.2
HG anisotropy weight	f	0.5

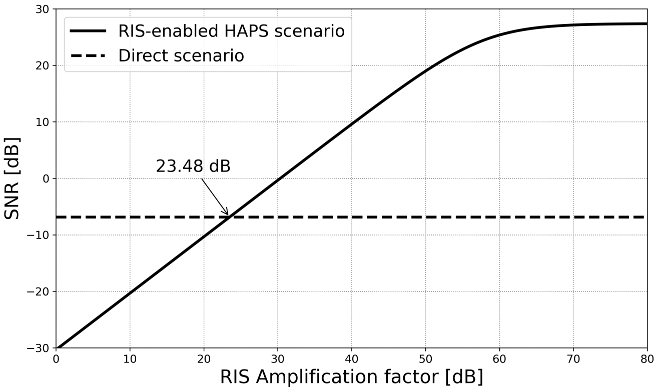


Fig. 4: Legitimate SNR for amplification factor α_m.

B. Multiplicative Fading

Since the total path loss in a ground station–RIS–satellite link is the product of the path losses of its two segments, the overall loss is typically several tens of dB higher than that of the direct ground station–satellite link [21], [54]. Figure 4 shows the SNR of the legitimate ground station–satellite link versus amplification factor. Diminishing returns appear beyond 60 dB due to noise from active RIS amplification. The active RIS outperforms the direct link only above 23.48 dB amplification.

To overcome the multiplicative fading while preserving margin for hardware impairments, noise-figure degradation, and limited power, we set the per-element amplification to 30 dB. State-of-the-art Complementary Metal-Oxide-Semiconductor (CMOS) reflection amplifiers at F-band deliver 28 dBi of gain with practical power consumption and noise figures [55], and experimental active RIS elements have demonstrated up to 40 dB per-element gain [56]. Hence, 30 dB is both feasible and sufficiently conservative.

C. Effect of Weather Conditions

To explore the effect of different weather conditions, given in Table IV, Fig. 5 shows the atmospheric attenuation coefficient α_{atm} for a range of frequencies for a moderate C_n^2. At lower frequencies, more severe weather conditions result in increased attenuation. However, at higher frequencies, the

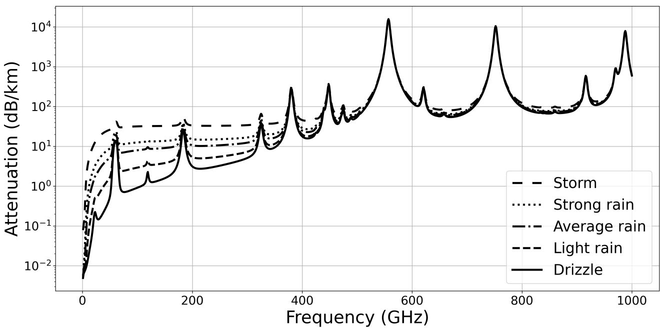


Fig. 5: Atmospheric attenuation vs frequency under different deather conditions ($C_n^2 = 10^{-15}$).

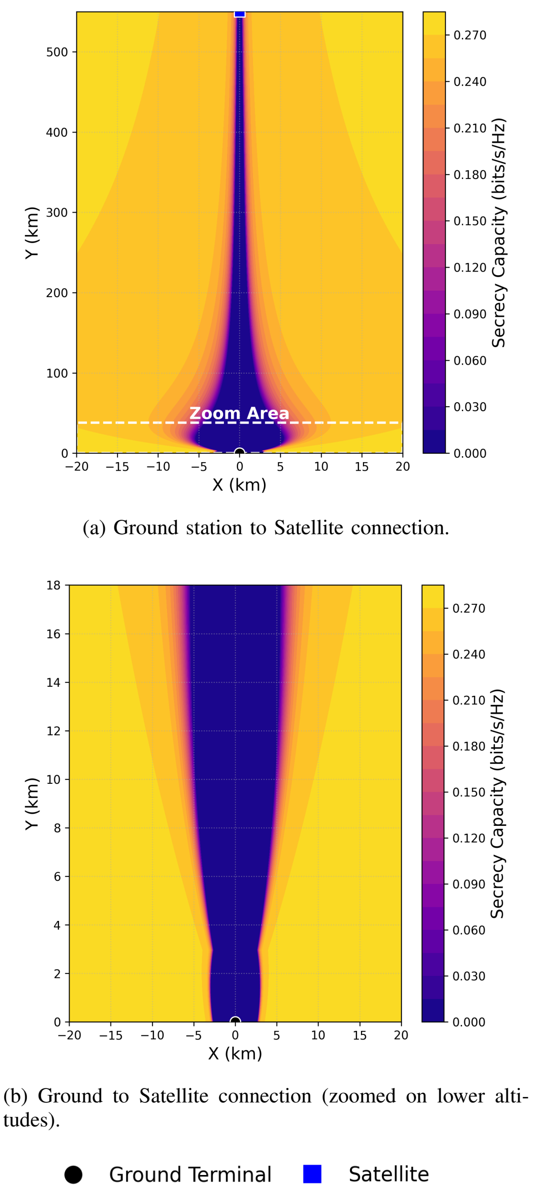
influence of weather becomes less significant, as attenuation due to atmospheric absorption is already dominant.

TABLE IV: Weather conditions and corresponding parameters (based on ITU-R P.1817-1)

Label	Rain Rate [mm/h]	Visibility [m]
Drizzle	0.25	18100
Light rain	2.5	5900
Average rain	12.5	2800
Strong rain	25.0	1900
Storm	100.0	770

D. Secrecy Capacity (SC) Evaluation

To analyse the model, we consider different eavesdropper locations. The results are presented in Fig. 6 for the direct scenario and in Fig. 7 for the RIS-enabled HAPS scenario. Most notably, for both the RIS-enabled HAPS and the direct scenario, there is an insecure area where $C_s = 0$, indicating that the eavesdropper experiences a higher SNR than the legitimate receiver. This shows that THz SatCom uplink is vulnerable to eavesdropping attacks. Importantly, this insecure region is centred along the channel between the legitimate transmitter and receiver. However, the RIS-enabled HAPS scenario results in a smaller insecure area compared to the direct transmission scenario for similar SNR. Additionally, only the first link between the ground station and the RIS is vulnerable, as we observe that from the RIS to the satellite there is no insecure area. This is because scattering and rain attenuation are negligible at these altitudes, making eavesdropping due to scattering effectively impossible.



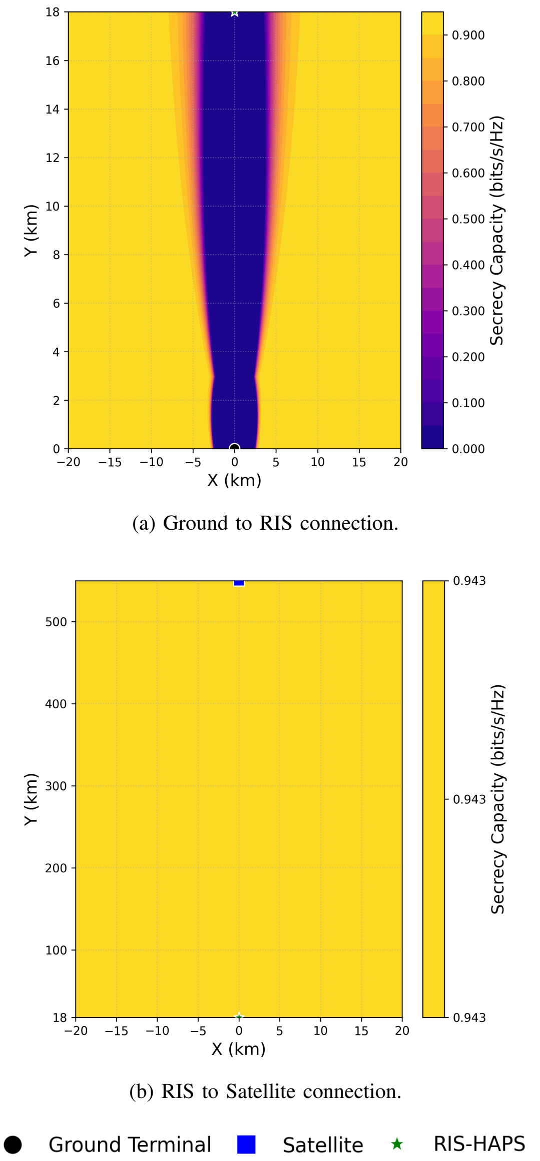
(a) Ground station to Satellite connection.

(b) Ground to Satellite connection (zoomed on lower altitudes).

Fig. 6: Secrecy Capacity in Gbps distribution for 2D positions of the eavesdropper for the direct scenario.

Fig. 8 presents the minimum and maximum secrecy capacities observed across all eavesdropper locations within the X-range $[-20, 20]$ km and Y-range $[0, 25]$ km, for the direct and RIS-enabled scenario. The upper bound of the Y-range corresponds to the maximum operational altitude of a HAPS [11]. Figure 8 supports the insights drawn from Figs. 6 and 7: under all weather conditions, both scenarios exhibit insecure regions where secrecy capacity is zero. However, these insecure areas are consistently larger in the direct transmission scenario. This observation is further supported by Fig. 9, which categorizes the spatial distribution of secrecy capacity into discrete performance ranges. In the RIS-integrated HAPS scenario, all insecure regions are smaller and the direct transmission scenario consistently exhibits larger insecure areas across all weather conditions. In the strong rain scenario specifically, the unsafe area of the RIS-enabled model is 48% smaller, showing the clear advantage of the inclusion of a RIS-enabled HAPS.

Figures 8 and 9 illustrate a clear trade-off between secrecy capacity and spatial security under varying weather conditions. In lighter weather conditions (e.g., drizzle), higher maximum secrecy capacity values are attainable. However, this comes at the cost of a larger insecure area. Thus, uplink communication must be planned strategically: one must either ensure a wider eavesdropper-free area to transmit at higher rates during light



(a) Ground to RIS connection.

(b) RIS to Satellite connection.

Fig. 7: Secrecy Capacity in Gbps distribution for 2D positions of the eavesdropper for the RIS-enabled scenario.

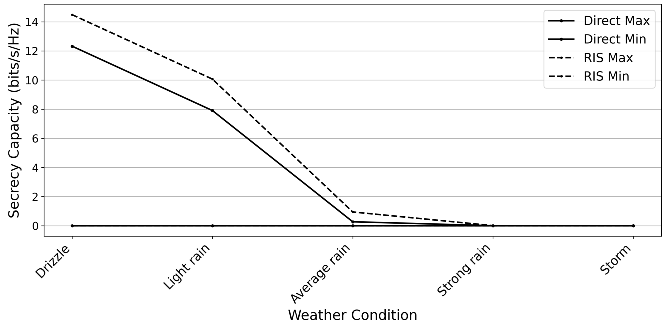


Fig. 8: Minimum and maximum secrecy capacity per weather condition.

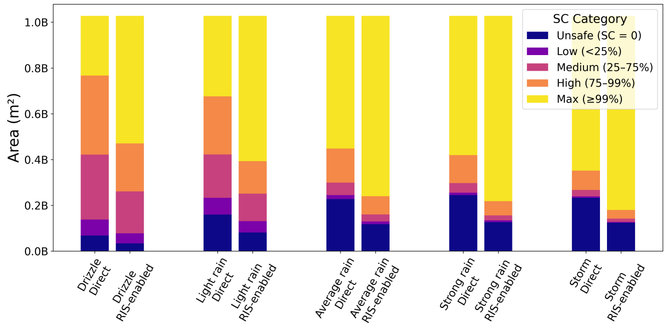


Fig. 9: Secrecy capacity area distribution per weather condition.

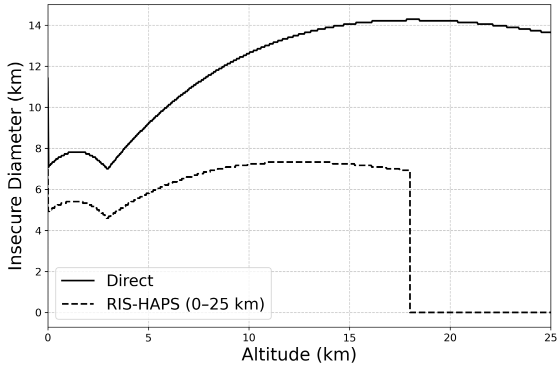


Fig. 10: Diameter of unsafe area around link.

weather, or accept lower transmission rates in exchange for reduced security risk.

The extent of the insecure region surrounding the link is further analysed in Fig. 10. As shown, the diameter of the insecure area in the direct transmission scenario increases over the first 14 km of altitude and then stabilizes at approximately 16 km throughout the remainder of the HAPS operational range. The RIS-enabled HAPS exhibits an insecure region that is approximately 33% narrower wide up until the RIS, beyond which the channel becomes effectively secure. Consequently, the adversary's ability to eavesdrop is confined to the region below the HAPS.

V. Conclusions

This work has evaluated the security benefits of employing an active RIS-enabled HAPS in a ground-to-satellite uplink scenario operating in the 0.1-1 THz frequency band. A comprehensive theoretical framework was developed to calculate the channel coefficients for both legitimate and eavesdropping links, incorporating key attenuation factors, a NLOS scattering model, and free-space path loss. Eavesdropping attacks were simulated across various legitimate communication paths, enabling a comparative assessment of the security performance between direct transmission and RIS-enabled HAPS scenarios.

The results show that THz SatCom uplink communication is vulnerable to eavesdropping attacks within a non-negligible area around the communication signal. Additionally, the results indicate that integrating an active RIS-enabled HAPS reduces the insecure area by 48%, defined as the spatial region where the secrecy capacity is zero, provided the RIS amplification factor is sufficiently high. The analysis also reveals a strategic trade-off: lighter weather conditions have larger insecure regions but allow for higher data rates. Therefore, operators are faced with a choice between spatial secrecy and data rates.

These findings reveal the vulnerability of direct THz satellite uplinks to eavesdropping and highlight active RIS-enabled HAPS as a promising countermeasure, emphasizing the need for further advancements to enhance physical-layer security.

Appendix A
NLOS factors

A. Integration Bounds

To establish the integration bounds, we examine the intersection point between the legitimate links, as described in Equation (1), and the edges of the eavesdropper observation field, which is defined by the eavesdropper's observation angle, given as

$$y_{L_X} - y_{E_X} = \tan(\theta_X) \cdot (x_{L_X} - x_{E_X}), \tag{26}$$

with $X \in \{AR, RB, AB\}$ and where θ_X is the angle at which the edges of the observation field intersect with the link. It is defined by the scattering angle α_X and the angle of observation β_X

$$\theta_X = \begin{cases} \alpha_X - \beta_X/2 \text{ for } L_a, L_c, L_e \\ \alpha_X + \beta_X/2 \text{ for } L_b, L_d, L_f \end{cases} . \tag{27}$$

$$L_{a,b} = \min\left[\max\left[\frac{y_{E_1} - \tan(\theta_1) x_{E_1}}{\frac{y_R - y_A}{x_R - x_A} - \tan(\theta_1)}, 0\right], x_R\right], \tag{28}$$

$$L_{c,d} = \min\left[\max\left[\frac{y_{E_2} - \tan(\theta_2) x_{E_2}}{\frac{y_B - y_R}{x_B - x_R} - \tan(\theta_2)}, x_R\right], x_B\right], \tag{29}$$

$$L_{e,f} = \min\left[\max\left[\frac{y_{E_D} - \tan(\theta_D) x_{E_D}}{\frac{y_B - y_A}{x_B - x_A} - \tan(\theta_D)}, 0\right], x_B\right]. \tag{30}$$

We can use Equation (1) and similar to find y_{L_X} for a given x_{L_X}. The distance of the legitimate transmitter to the eavesdroppers is then calculated as in Equation (2).

B. Solid Angle

The solid angle $\Omega(x_{L_X})$ is the angle formed at the scattering point L_X that defines the spread of the scattered signal reaching the eavesdropper's antenna. It quantifies how much scattered signal from the communication path is captured by the eavesdropper, and is given as

$$\Omega(x_{L_X}) = \frac{A_{\text{eff}}}{\left[(x_{E_X} - x_{L_X})^2 + (y_{E_X} - y_{L_X})^2\right]^{3/2}} \cdot \frac{(x_{E_X} - x_{L_X}) + (y_{E_X} - y_{L_X}) \tan\alpha}{\sqrt{1 + \tan^2\alpha}}, \tag{31}$$

with receiving effective antenna aperture A_{eff} and scattering angle towards the eavesdropper α.

C. Scattering phase function

The scattering phase function, which represents the Probability Density Function (PDF) of the scattering angle, is modelled using a generalized Henyey-Greenstein function as

$$P(\mu_X) = \frac{1 - g^2}{4\pi} \cdot \left[\frac{1}{(1 + g^2 - 2g\mu_X)^{3/2}} + f\,\frac{3\mu_X^2 - 1}{2(1 + g^2)^{3/2}}\right], \tag{32}$$

with model parameters g, f, and μ_X being the cosine of the scattering angle at the scattering point (x_{L_X}, y_{L_X}).

The cosine values μ_X for each eavesdropper E_X, with $X \in \{AR, RB, AB\}$, are computed as

$$\mu_{AR} = \frac{A_1 C_1 + B_1 D_1}{\sqrt{A_1^2 + B_1^2} \cdot \sqrt{C_1^2 + D_1^2}} \tag{33}$$

$$\mu_{RB} = \frac{C_2 E_2 + D_2 F_2}{\sqrt{C_2^2 + D_2^2} \cdot \sqrt{E_2^2 + F_2^2}} \tag{34}$$

$$\mu_{AB} = \frac{A_D C_D + B_D D_D}{\sqrt{A_D^2 + B_D^2} \cdot \sqrt{C_D^2 + D_D^2}} \tag{35}$$

with the components defined as

$$\begin{aligned} A_X &= x_{L_X} - x_{P_X}, \quad B_X = y_{L_X} - y_{P_X}, \\ C_X &= x_{E_X} - x_{L_X}, \quad D_X = y_{E_X} - y_{L_X}, \\ E_X &= x_{L_X} - x_R, \quad F_X = y_{L_X} - y_R, \end{aligned}$$

where the point P_X is the location of the legitimate transmitter.

References

[1] J. Nielsen, "Nielsen's law of internet bandwidth," *Nielsen Norman Group*, 01 2023, accessed: 2025-05-27. [Online]. Available: https://www.nngroup.com/articles/law-of-bandwidth/

[2] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, p. 109246, 2022.

[3] K. Woellert, P. Ehrenfreund, A. J. Ricco, and H. Hertzfeld, "Cubesats: Cost-effective science and technology platforms for emerging and developing nations," *Advances in Space Research*, vol. 47, no. 4, pp. 663–684, 2011.

[4] N. Saeed, A. Elzanaty, H. Almorad, H. Dahrouj, T. Y. Al-Naffouri, and M.-S. Alouini, "Cubesat communications: Recent advances and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1839–1862, 2020.

[5] European Commission, "Iris²: Secure connectivity," https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity, 2023, accessed: 2025-06-17.

[6] Z. S. Gérard Maral, Michel Bousquet, *Introduction*. John Wiley & Sons, Ltd, 2020, ch. 1, pp. 1–27.

[7] I. Transmitter. (2023, 04) Cybersecurity in orbit: The growing vulnerability of space-based systems. Accessed: 2025-05-27. [Online]. Available: https://transmitter.ieee.org/cybersecurity-in-orbit-the-growing-vulnerability-of-space-based-systems/

[8] European External Action Service, "Eu space strategy for security and defence," https://www.eeas.europa.eu/eeas/eu-space-strategy-security-and-defence-0, 2023, accessed: 2025-06-17.

[9] J. Mooney, "Russian proton-m launches olymp-k-2 military satellite," https://www.nasaspaceflight.com/2023/03/proton-olymp-k-2/, 2023, accessed: 2025-06-17.

[10] The Defense Post, "Eu warns russia of sanctions over any attack in space," https://thedefensepost.com/2025/01/30/eu-russia-space-sanctions, 2025, accessed: 2025-06-17.

[11] G. Karabulut Kurt, M. G. Khoshkholgh, S. Alfattani, A. Ibrahim, T. S. J. Darwish, M. S. Alam, H. Yanikomeroglu, and A. Yongacoglu, "A vision and framework for the high altitude platform station (haps) networks of the future," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, pp. 729–779, 2021.

[12] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6g era: Challenges and opportunities," *IEEE Network*, vol. 35, no. 2, pp. 244–251, 2021.

[13] J. Qiu, D. Grace, G. Ding, M. Zakaria, and Q. Wu, "Air-ground heterogeneous networks for 5g and beyond via integrating high and low altitude platforms," *IEEE Wireless Communications*, vol. 26, pp. 140–148, 12 2019.

[14] "Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence — 6gflagship.com," https://www.6gflagship.com/key-drivers-and-research-challenges-for-6g-ubiquitous-wireless-intelligence/, accessed: 17-06-2025.

[15] M. H. Khoshafa, O. Maraqa, J. M. Moualeu, S. Aboagye, T. M. N. Ngatched, M. H. Ahmed, Y. Gadallah, and M. D. Renzo, "Ris-assisted physical layer security in emerging rf and optical wireless communication systems: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2024.

[16] Y. Han, S. Jin, C.-K. Wen, and T. Q. S. Quek, "Localization and channel reconstruction for extra large ris-assisted massive mimo systems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 5, pp. 1011–1025, 2022.

[17] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *CoRR*, vol. abs/1810.03961, 2018. [Online]. Available: http://arxiv.org/abs/1810.03961

[18] M. Di Renzo, K. Ntontin, J. Song, F. H. Danufane, X. Qian, F. Lazarakis, J. De Rosny, D.-T. Phan-Huy, O. Simeone, R. Zhang, M. Debbah, G. Lerosey, M. Fink, S. Tretyakov, and S. Shamai, "Reconfigurable intelligent surfaces vs. relaying: Differences, similarities, and performance comparison," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 798–807, 2020.

[19] C. Huang, G. C. Alexandropoulos, A. Zappone, M. Debbah, and C. Yuen, "Energy efficient multi-user miso communication using low resolution large intelligent surfaces," in *2018 IEEE Globecom Workshops (GC Wkshps)*, 2018, pp. 1–6.

[20] HAPS Alliance Aviation Working Group, "Haps certification pathways," White paper, HAPS Alliance, 2024, available at https://hapsalliance.org/wp-content/uploads/formidable/12/HAPS_Certification_Pathways_2024-3.pdf, accessed June 2025.

[21] Z. Zhang, L. Dai, X. Chen, C. Liu, F. Yang, R. Schober, and H. V. Poor, "Active ris vs. passive ris: Which will prevail in 6g?" *IEEE Transactions on Communications*, vol. 71, no. 3, pp. 1707–1725, 2023.

[22] ETSI Industry Specification Group (ISG) TeraHertz (THz), "Terahertz modeling (thz); identification of use cases for thz communication systems," European Telecommunications Standards Institute (ETSI), Group Report GR THz 001 V1.1.1, 01 2024.

[23] C. Chaccour, M. N. Soorki, W. Saad, M. Bennis, P. Popovski, and M. Debbah, "Seven defining features of terahertz (thz) wireless systems: A fellowship of communication and sensing," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 967–993, 2022.

[24] K. Tekbiyik, G. K. Kurt, A. R. Ektı, and H. Yanikomeroglu, "Reconfigurable intelligent surfaces empowered thz communication in leo satellite networks," *IEEE Access*, vol. 10, pp. 121 957–121 969, 2022.

[25] T. Schneider, A. Wiatrek, S. Preussler, M. Grigat, and R.-P. Braun, "Link budget analysis for terahertz fixed wireless links," *IEEE Transactions on Terahertz Science and Technology*, vol. 2, no. 2, pp. 250–256, 2012.

[26] A. S. Abdalla, T. F. Rahman, and V. Marojevic, "Uavs with reconfigurable intelligent surfaces: Applications, challenges, and opportunities," 2020.

[27] C. E. Worka, F. A. Khan, Q. Z. Ahmed, P. Sureephong, and T. Alade, "Reconfigurable intelligent surface (ris)-assisted non-terrestrial network (ntn)-based 6g communications: A contemporary survey," *Sensors*, vol. 24, no. 21, 2024.

[28] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[29] S. Shahzad, K. Joiner, L. Qiao, F. Deane, and J. Plested, "Cyber resilience limitations in space systems design process: Insights from space designers," *Systems*, vol. 12, no. 10, 2024. [Online]. Available: https://www.mdpi.com/2079-8954/12/10/434

[30] Y. Mei, Y. Ma, J. Ma, L. Moeller, and J. F. Federici, "Eavesdropping risk evaluation on terahertz wireless channels in atmospheric turbulence," *IEEE Access*, vol. 9, pp. 101 916–101 923, 2021.

[31] D. Zou and Z. Xu, "Information security risks outside the laser beam in terrestrial free-space optical communication," *IEEE Photonics Journal*, vol. 8, no. 5, pp. 1–9, 2016.

[32] O. B. Yahia, E. Erdogan, G. K. Kurt, I. Altunbas, and H. Yanikomeroglu, "Optical satellite eavesdropping," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 10 126–10 131, 2022.

[33] E. Illi and M. Qaraqe, "On the secrecy enhancement of an integrated ground-aerial network with a hybrid fso/thz feeder link," 2024. [Online]. Available: https://arxiv.org/abs/2403.16072

[34] J. Yuan, G. Chen, M. Wen, R. Tafatzolli, and E. Panayirci, "Secure transmission for thz-empowered ris-assisted non-terrestrial networks," 2022.

[35] International Telecommunication Union Radiocommunication Sector (ITU-R), "Attenuation by atmospheric gases," Recommendation ITU-R P.676-11, 2016.

[36] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Transactions on Wireless Communications*, vol. 10, no. 10, pp. 3211–3221, 2011.

[37] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[38] L. Dordova and O. Wilfert, "Calculation and comparison of turbulence attenuation by different methods," *Radioengineering*, vol. 19, 04 2010.

[39] L. Andrews, *Field Guide to Atmospheric Optics*, ser. Field Guides. SPIE Press, 2019. [Online]. Available: https://books.google.it/books?id=WnHwuQEACAAJ

[40] International Telecommunication Union Radiocommunication Sector (ITU-R), "Reference atmospheres," Recommendation ITU-R P.835-7, 2024.

[41] M. S. Awan, Marzuki, E. Leitgeb, B. Hillbrand, F. Nadeem, and M. S. Khan, "Cloud attenuations for free-space optical links," in *2009 International Workshop on Satellite and Space Communications*, 2009, pp. 274–278.

[42] A. Naboulsi, H. Sizun, and F. de Fornel, "Propagation of optical and infrared waves in the atmosphere," in *Proceedings of SPIE - The International Society for Optical Engineering*, vol. 5891, 2005, p. 58910E. [Online]. Available: https://api.semanticscholar.org/CorpusID:6277869

[43] International Telecommunication Union Radiocommunication Sector (ITU-R), "Specific attenuation model for rain for use in prediction methods," Recommendation ITU-R P.838-3, 2005.

[44] ——, "Rain height model for prediction methods," Recommendation ITU-R P.839-4, 2013.

[45] C. Pan, G. Zhou, K. Zhi, S. Hong, T. Wu, Y. Pan, H. Ren, M. D. Renzo, A. Lee Swindlehurst, R. Zhang, and A. Y. Zhang, "An overview of signal processing techniques for ris/irs-aided wireless systems," *IEEE Journal of Selected Topics in Signal Processing*, vol. 16, no. 5, pp. 883–917, 2022.

[46] I. Yildirim, A. Uyrus, and E. Basar, "Modeling and analysis of reconfigurable intelligent surfaces for indoor and outdoor applications in future wireless networks," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 1290–1301, 2021.

[47] E. Bjornson, H. Wymeersch, B. Matthiesen, P. Popovski, L. Sanguinetti, and E. de Carvalho, "Reconfigurable intelligent surfaces: A signal processing perspective with wireless applications," *IEEE Signal Processing Magazine*, vol. 39, no. 2, p. 135–158, 03 2022.

[48] T. Hossain, S. Shabab, A. S. M. Badrudduza, M. K. Kundu, and I. S. Ansari, "On the physical layer security performance over ris-aided dual-hop rf-uowc mixed network," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2246–2257, 2023.

[49] Q. Chen, M. Li, X. Yang, R. Alturki, M. D. Alshehri, and F. Khan, "Impact of residual hardware impairment on the iot secrecy performance of ris-assisted noma networks," *IEEE Access*, vol. 9, pp. 42 583–42 592, 2021.

[50] R. Deka, M. S. Alam, I. Ahmed, and S. Anees, "Performance analysis of a ris-haps assisted fso-uwoc system for ground-air-underwater connectivity," in *2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall)*, 2024, pp. 1–5.

[51] A. B. Sarawar, A. S. M. Badrudduza, M. Ibrahim, I. S. Ansari, and H. Yu, "Secrecy performance analysis of integrated rf-uwoc

iot networks enabled by uav and underwater-ris," 2024. [Online]. Available: https://arxiv.org/abs/2407.18766

[52] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[53] International Telecommunication Union Radiocommunication Sector (ITU-R), "Characteristics of precipitation for propagation modelling," Recommendation ITU-R P.837-7, 2017.

[54] M. Najafi, V. Jamali, R. Schober, and H. V. Poor, "Physics-based modeling and scalable optimization of large intelligent reflecting surfaces," *CoRR*, vol. abs/2004.12957, 2020.

[55] N. Landsberg and E. Socher, "A low-power 28-nm cmos fd-soi reflection amplifier for an active f-band reflectarray," *IEEE Transactions on Microwave Theory and Techniques*, vol. 65, no. 10, pp. 3910–3921, 2017.

[56] R. Long, Y. Liang, Y. Pei, and E. G. Larsson, "Active reconfigurable intelligent surface aided wireless communications," *IEEE Transactions on Wireless Communications*, vol. 20, no. 8, pp. 4962–4975, 2021. [Online]. Available: https://doi.org/10.1109/TWC.2021.3064024