Eavesdropping of Terahertz RIS-enabled HAPS-integrated satellite communication

Security for Space Systems (3S) 2025

November 4-6, 2025 – ESTEC in Noordwijk, The Netherlands

D. van der Eijk*, S. Soderi*†, M. Conti*‡

* University of Padova, Italy

† IMT School for Advanced Studies, Italy

‡ Örebro University, Sweden

SPRITZ
Security & Privacy
Research Group

esa

Università
degli Studi
di Padova

Outline

SPRITZ Security & Privacy Research Group

esa

Università degli Studi di Padova

Outline

Satellite Communication (SatCom)

Background

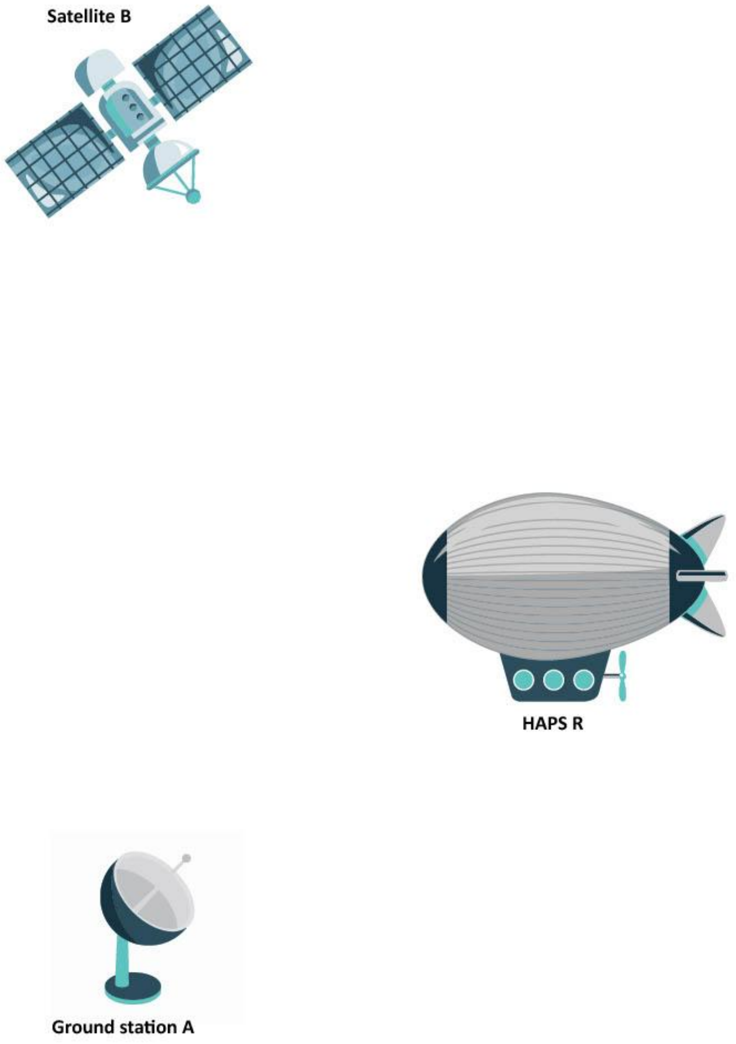
Non-Terrestrial Networks (NTNs) have become essential components of key critical infrastructures. This leads to an **expanding threat surface**.

Strategic attention:

- European Union 2023 Space Strategy for Security and Defense
- Increased NATO investments

High Altitude Platform Station (HAPS)

Background

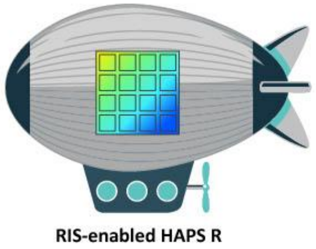


Solar-powered aircraft or balloon located in the **stratosphere** (~20 km altitude). **Long-endurance, quasi-stationary** platforms that have been theorized to manage aerial networks of UAVs, **act as interface with LEO satellites** or act as aerial data centers. Their unique position in the sky gives them **line-of-sight connections** to both satellites and users.

Reconfigurable Intelligent Surface (RIS)

Background

Set of elements capable of adjusting the amplitude and phase shift of an incident signal. **Passive RIS** adjust only the phase shift, whilst **active RIS** can adjust both.



Example integration scenarios:

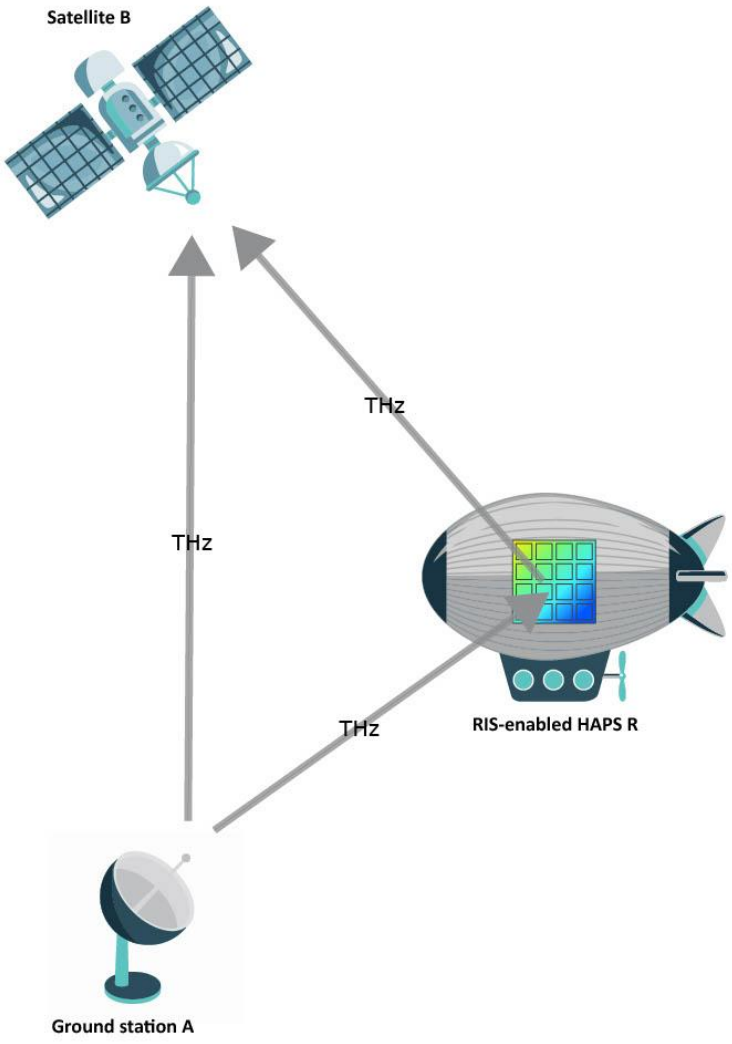
- Billboards or building facades
- Vehicle-to-vehicle (V2V) communication
- Mounted on a HAPS

Terahertz (THz) Frequency Band

Background

The relatively unexplored THz frequency band offers possibilities for **ultra-high capacity networking**. It is currently only partially regulated (<0.3 THz), of which the higher frequencies are generally allocated only for **experimental communication**.

However, THz band RF communication suffers from high propagation losses due to **absorption** and **rain attenuation**.



SPRITZ Security & Privacy Research Group · esa · Università degli Studi di Padova

Outline

Adversary Model

Threat Model

Threat objective:

The adversary aims for passive compromise of confidentiality by obtaining a higher SNR than the legitimate receiver.

Threat capabilities:

- Knowledge of key positions
- Adversary mobility
- Link tracking strategy
- Stealth assumptions

Eavesdropper Locations

Threat Model

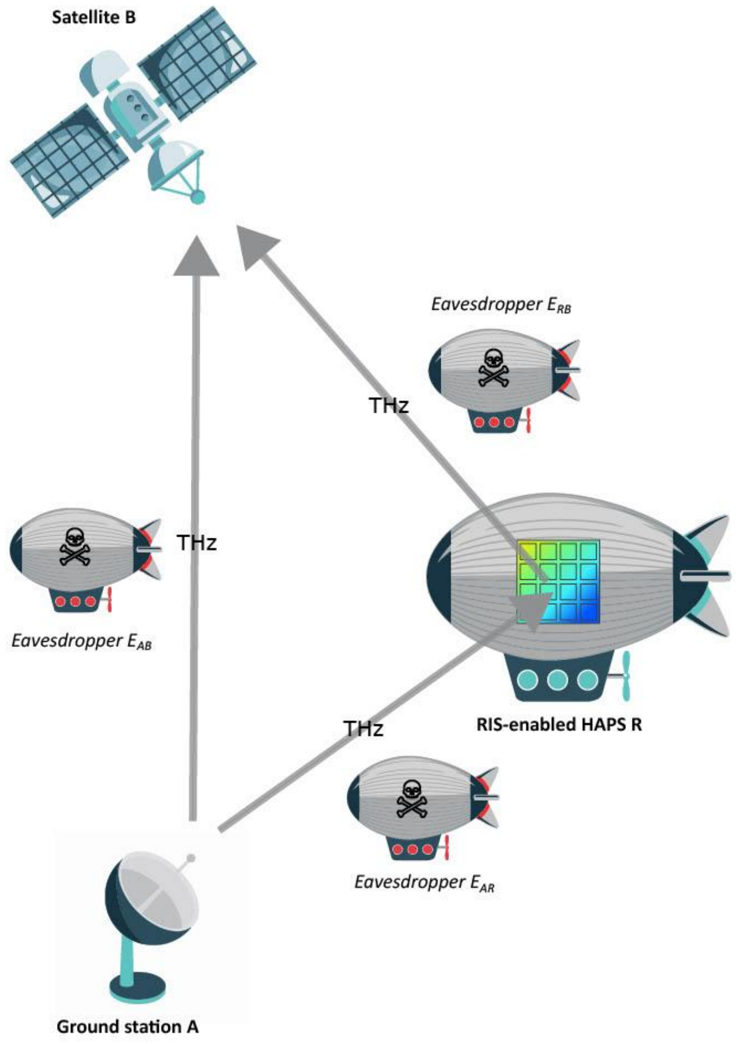
Direct scenario:

- E_{AB} located between ground station and satellite

RIS-enabled scenario:

- E_{AR} between ground station and RIS-enabled HAPS
- E_{RB} between RIS-enabled HAPS and satellite

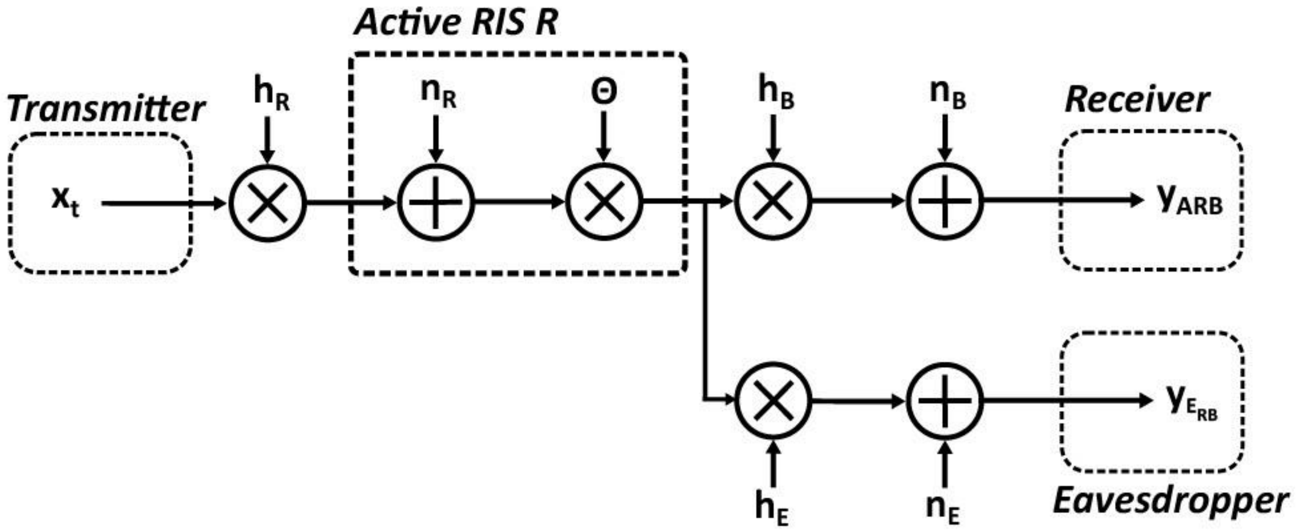
The **RIS alters the signal**, so E_{AR} and E_{RB} observe different signal characteristics.



Physical Layer Security (PLS)

Threat model

PLS uses the **wiretap model** to model the legitimate and eavesdropper channel. **Unique characteristics of the channels** can then be used to enhance secure communication where traditional upper-layer cryptographic methods (e.g. link layer encryption) are **too computationally intensive** and inflexible.



Outline

SPRITZ Security & Privacy Research Group

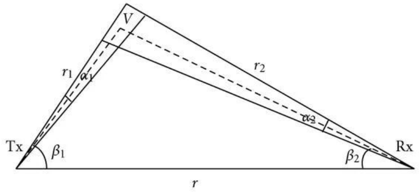
esa

Università degli Studi di Padova

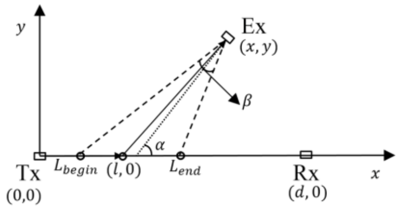
Related Works

Atmospheric scattering

Research into the effect of atmospheric scattering highlights how **physical phenomena** can lead to **redirection of signals**, which can result in possible **eavesdropping** of legitimate connections.



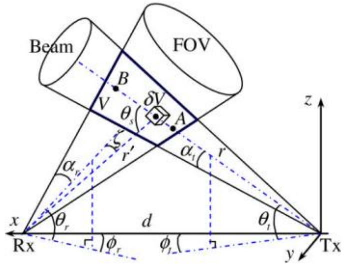
(Ding et al., 2010)



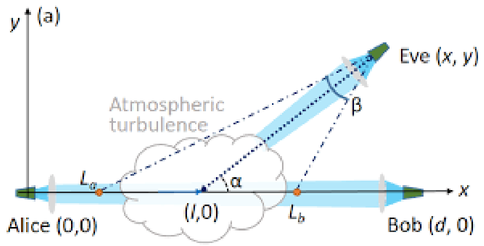
(Zou and Xu, 2016)

This work

(Zuo et al., 2013)



(Mei et al., 2024)



Contributions

Atmospheric scattering

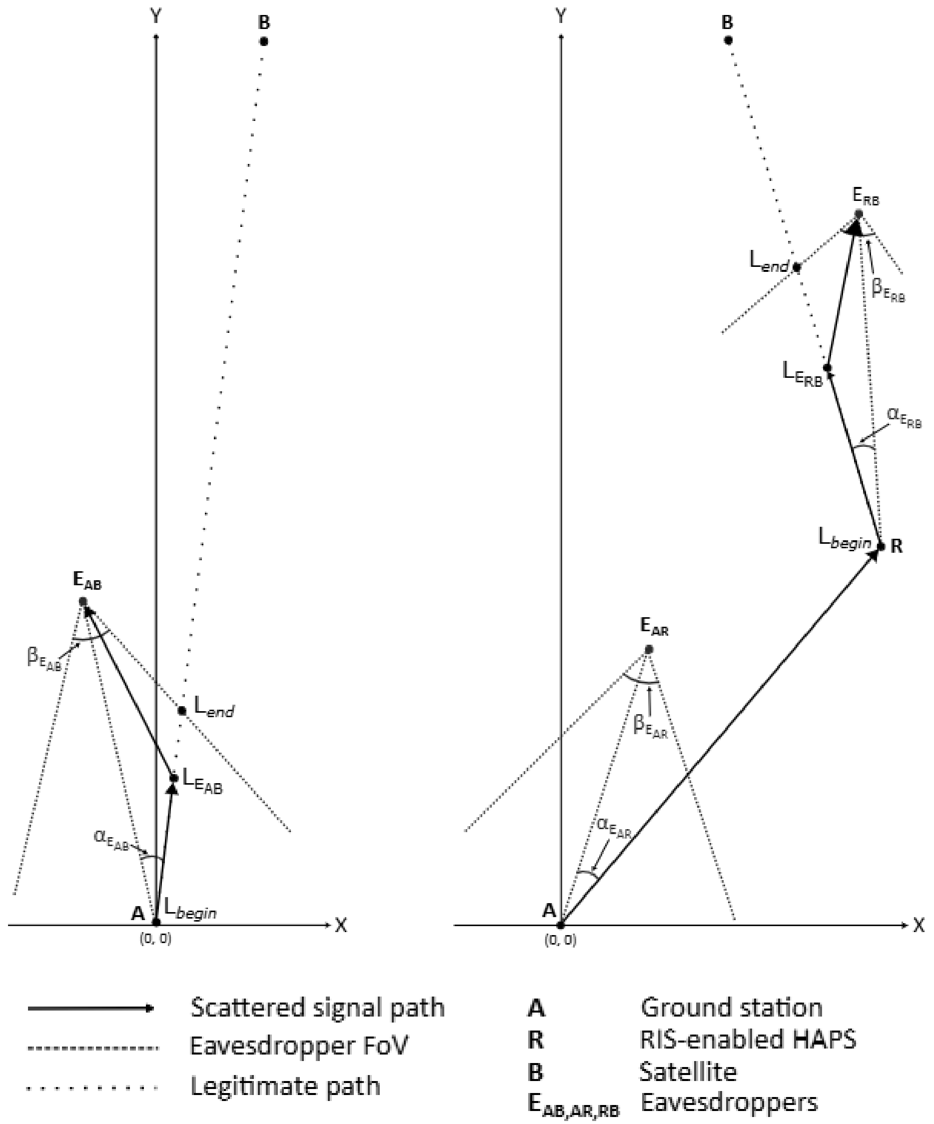
- We propose calculations for the secrecy capacity of **Terahertz direct and RIS-enabled HAPS-integrated uplink** communication.
- We introduce a **deterministic 2D single-scattering model** for NTN THz communication that captures the received signal at an eavesdropper.
- We quantify the **security benefits of employing a RIS-enabled HAPS** in uplink communication in **different weather conditions** through multiple security metrics.

Geometric Representation

Atmospheric scattering

Scattering phenomenon variables:

- **L_{Ex}**, which represents the location at which the signal scatters off the legitimate path
- **α, β**, which represent the scattering angles
- **L_{begin}, L_{end}**, which represent the edges of the eavesdroppers' FoV on the legitimate channel



SPRITZ Security & Privacy Research Group · esa · Università degli Studi di Padova

Non-Line-Of-Sight Channel Coefficient

Atmospheric scattering

The NLOS channel coefficient captures the **cumulative scattered signal** along the propagation path **towards the eavesdropper**.

$$h_{\mathrm{NLOS}} = \sqrt{G_t G_r} \int_{L_{\mathrm{begin}}}^{L_{\mathrm{end}}} \Omega(x_l)\, p(\mu)\, \alpha_{\mathrm{sca}}\, e^{-\alpha_{\mathrm{atm}} d}\, dx_l ,$$

where

- G_t, G_r: transmitter and receiver antenna gains,
- $\Omega(xl)$: solid angle,
- $p(\mu)$: scattering phase,
- α_{sca}: total scattering attenuation,
- α_{atm}: total atmospheric attenuation,
- d: total propagation distance.

SPRITZ Security & Privacy Research Group

esa

Università degli Studi di Padova

Outline

SPRITZ Security & Privacy Research Group · esa · Università degli Studi di Padova

Received signal

Security analysis

The received signal captures the impact of **transmission**, **propagation**, and **reception** of a signal through the atmosphere in the **presence of noise**. For the direct AB channel, the received signal is given as

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

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

$$h_{AB} = h_{FSPL} \cdot h_{atm},$$

where h_{FSPL} and h_{atm} represent free space path loss and atmospheric attenuation respectively.

SPRITZ Security & Privacy Research Group · esa · Università degli Studi di Padova

Received signal

Security analysis

For the active RIS-enabled ARB channel, the received signal is given as

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

with the pilot signal transmitted $x_t \in C$, $|x_t| = 1$, transmit power P, AWGN $n_{t,RB} \sim CN(0, \sigma^2_{RB} I_{NB})$ for NB antennas, RIS-amplified noise $n_{t,AR} \sim CN(0, \sigma^2_{AR} I_M)$ for M RIS-elements, AR channel $h_{AR} \in C^{M \cdot 1}$, and RB channel $h_{RB} \in C^{N_B \cdot M}$. We have reflection coefficient matrix $\Theta_t = \mathrm{diag}(\theta_t)$, with corresponding reflection coefficients $\theta_t = [\theta_{t,1}, \ldots, \theta_{t,M}]^T$ with

$$\theta_{t,m} = \alpha_m e^{j\phi_{t,m}},$$

where α_m represent the amplitude gain and $e^{j\phi_{t,m}}$ the phase shift induced by the RIS.

Signal-to-Noise Ratio

Security analysis

The SNR can be interpreted as a measure of how much stronger the desired signal is compared to the background noise. For the direct AB channel, the SNR is given as

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

For the RIS-enabled channel ARB the SNR is given as

$$\gamma_{ARB} = \frac{P\left|\sum_{m=1}^{M} h_{RB,m}\alpha_m e^{j\phi_{t,m}} h_{AR,m}\right|^2}{\sigma_{AR}^2 \sum_{m=1}^{M} |h_{RB,m}\alpha_m e^{j\phi_{t,m}}|^2 + \sigma_B^2}.$$

Secrecy Capacity

Security analysis

The SC represents the maximum **secure communication rate** (in bits/s/hz) over the legitimate channel.

$$C_s^{EX} = \max\left\{\log_2(1+\gamma_{\mathrm{m}}) - \log_2(1+\gamma_{E_X,\mathrm{max}}),\ 0\right\},$$

where γ_{m} is the legitimate main channel SNR and $\gamma_{EX,\,\mathrm{max}}$ is the maximum SNR of the corresponding eavesdropper.

Outline

Simulation Parameters

Results

TABLE II: Simulation overview

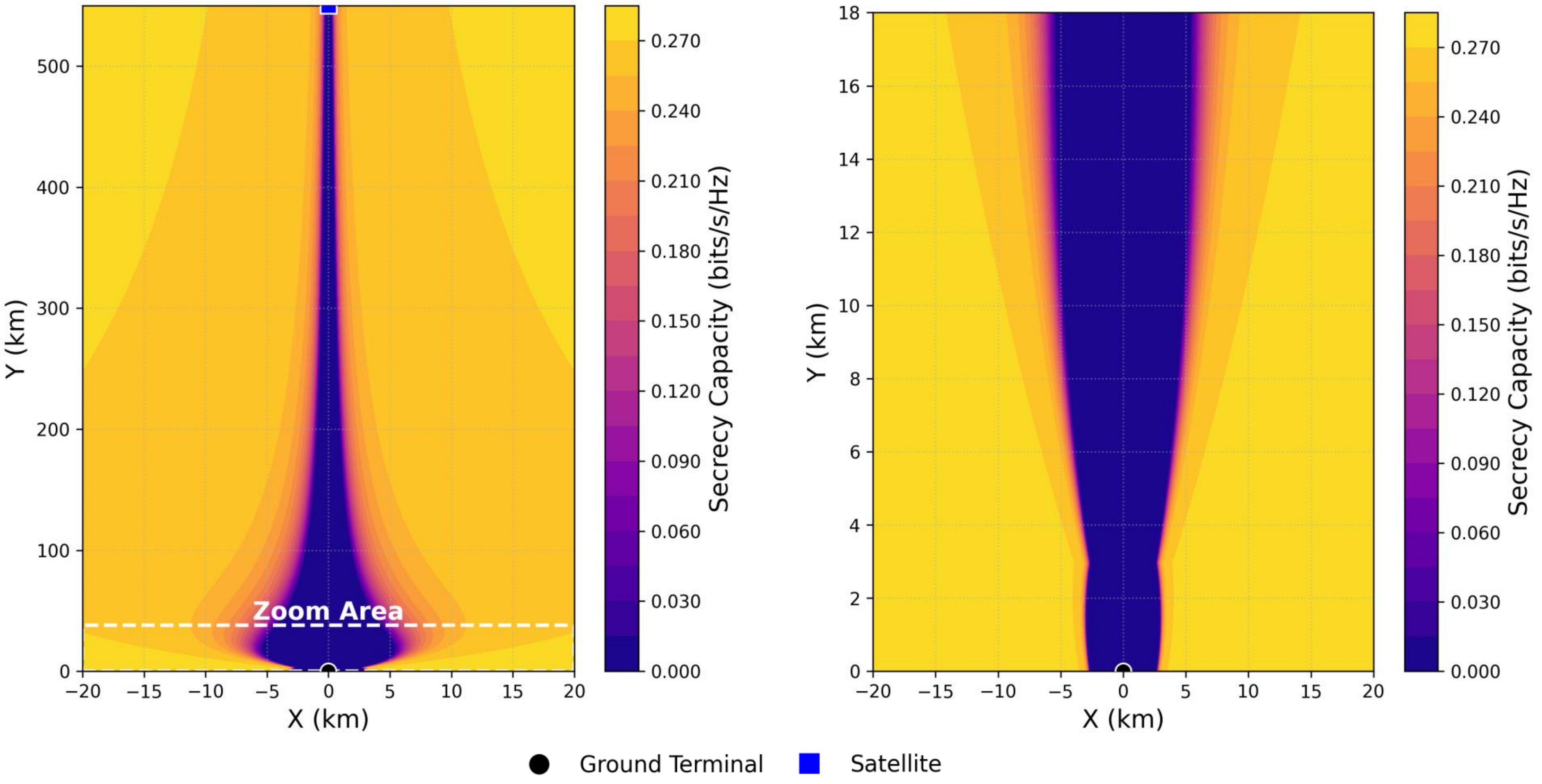
Component	Details
Ground Station	Altitude: 0 km Antenna: 2 m diameter Location: Noordwijk, Netherlands Season: Summer
RIS-HAPS	Altitude: 18 km RIS surface: 1.5 × 1.5 m
Satellite	Altitude: 550 km Antenna: 1 m diameter
Eavesdroppers	Antenna: 0.5 m diameter
Weather condition	Strong rain (ITU-R 1817-1)

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

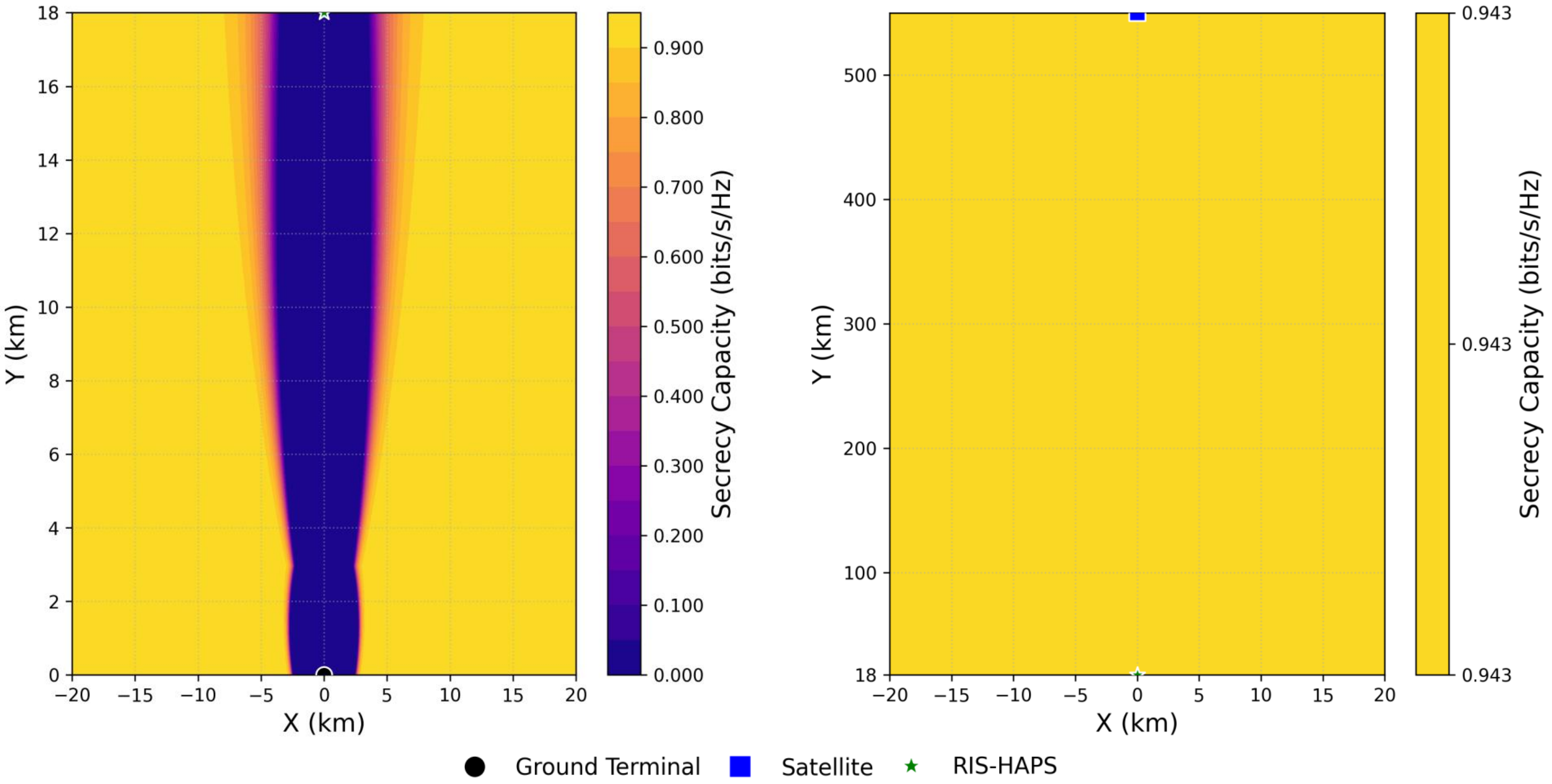
Secrecy Capacity Heatmaps

Results



Secrecy Capacity Heatmaps

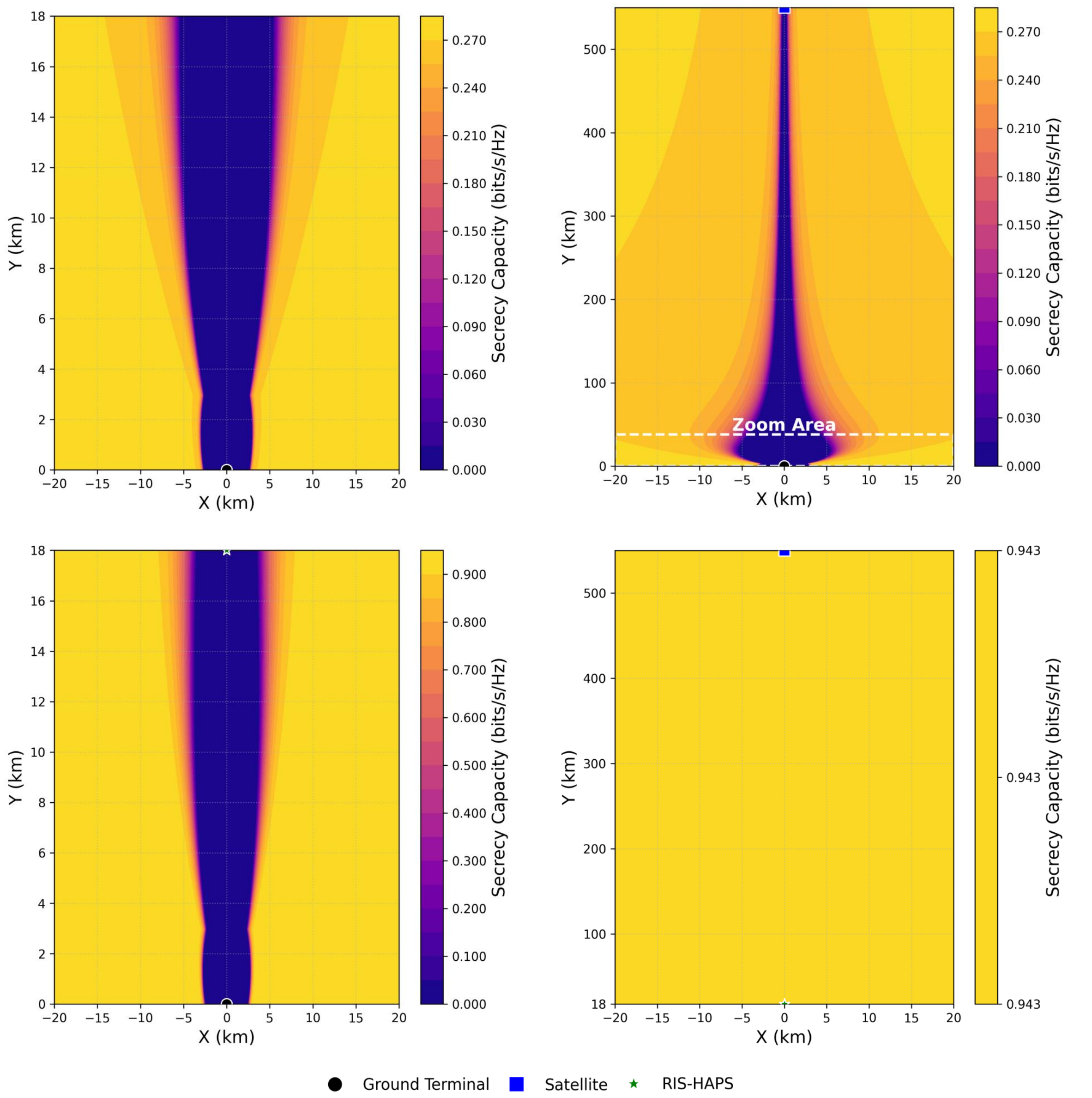
Results



Secrecy Capacity Heatmaps

Results

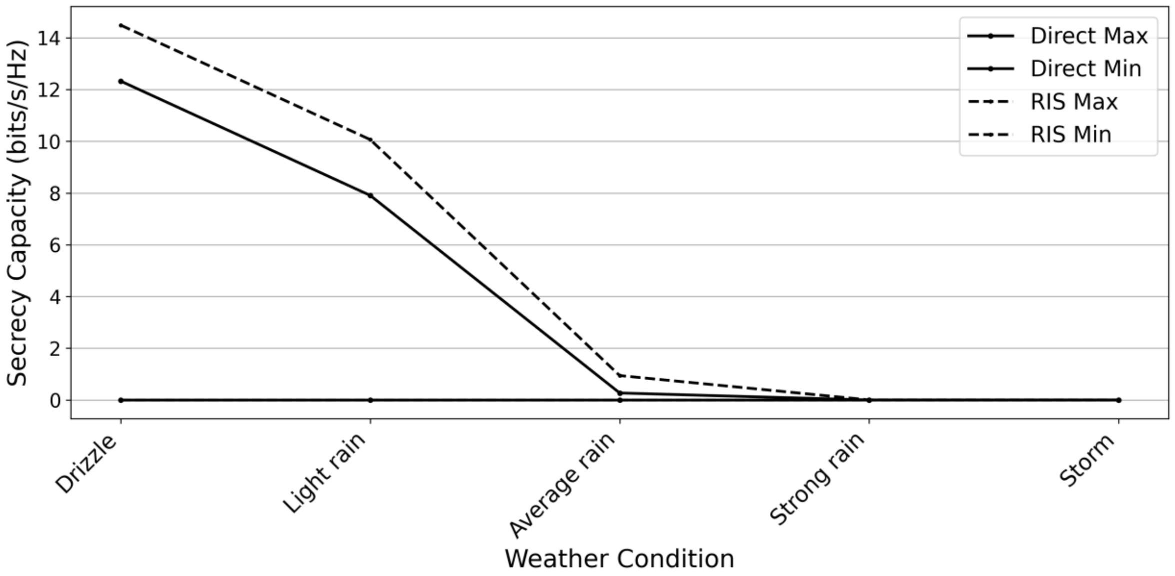
Integrating a RIS-enabled HAPS **reduces the area vulnerable to eavesdropping attacks** below the HAPS. It eliminates physical-layer eavesdropping above the RIS-enabled HAPS since the **physical phenomenon** that cause **scattering are not present at higher altitudes.** Additionally, it increases the **maximum secrecy capacity.**



Spatial Metrics in Weather Conditions

Results

In all weather conditions, the **maximum SC is higher for the RIS-enabled HAPS** scenario. However, the minimum SC is always zero, indicating a weakness to eavesdropping.

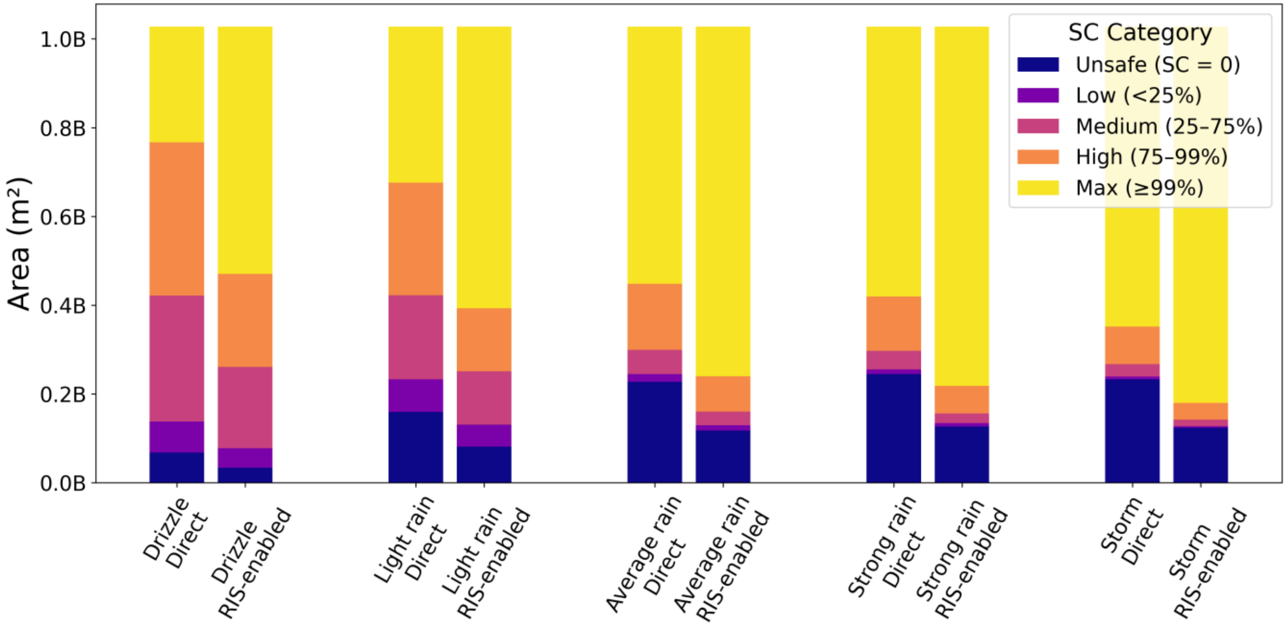


Label	Rain Rate [mm/h]	Visibility [m]
Drizzle	0.25	18100
Light rain	2.5	5900
Average rain	12.5	2800
Strong rain	25	1900
Storm	100	770

Spatial Metrics in Weather Conditions

Results

In lighter weather conditions, the **insecure area is larger** for both scenarios. The RIS-enabled HAPS scenario has a **smaller insecure area** compared to the direct scenario.



SPRITZ Security & Privacy Research Group

esa

Università degli Studi di Padova

Outline

1. Background
2. Threat model
3. Atmospheric scattering
4. Security analysis
5. Results
6. **Conclusions**

Conclusions

- Terahertz satellite uplinks are **vulnerable to eavesdropping attacks** within a non-negligible area around the communication signal,
- Integrating an active RIS-enabled HAPS **reduces the insecure area by 48%** compared to direct transmission,
- There exists a strategic **trade-off between spatial secrecy and data rates**: lighter weather conditions have larger insecure regions but allow higher secrecy rates.

Eavesdropping of Terahertz RIS-enabled HAPS-integrated satellite communication

Security for Space Systems (3S) 2025

November 4-6, 2025 – ESTEC in Noordwijk, The Netherlands

D. van der Eijk*, S. Soderi*†, M. Conti*‡

daanjannes.vandereijk@studenti.unipd.it

SPRITZ
Security & Privacy
Research Group

esa

Università
degli Studi
di Padova