SECURITY FOR SPACE SYSTEMS (3S)
ESA-ESTEC 4-6 NOVEMBER 2025, NOORDWIJK, NL

AN END-TO-END GEO SATELLITE LINKS SIMULATION FRAMEWORK FOR CYBER RANGE APPLICATIONS

ALESSANDRO SANTORSOLA, DANIELE MAMMONE, STEFANO LONGARI, FRANCESCO TOPPUTO, AND MATTEO MERGÈ

BV·TECH

OUTLINE

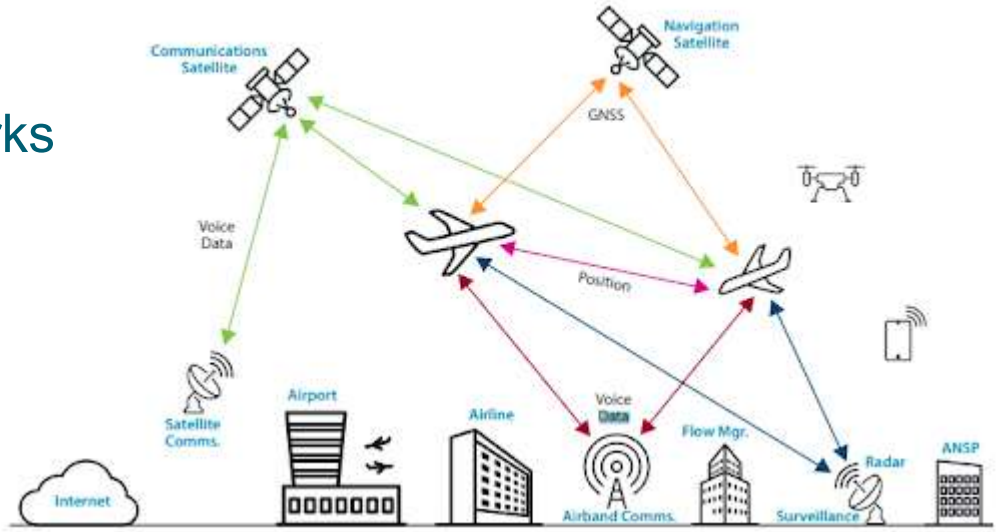
Agenzia Spaziale Italiana

- Introduction
- The SOCRATE Project
- Proposed Contribution
- Conclusions

BV TECH · POLITECNICO MILANO 1863 · DART Group · NECST laboratory

INTRODUCTION

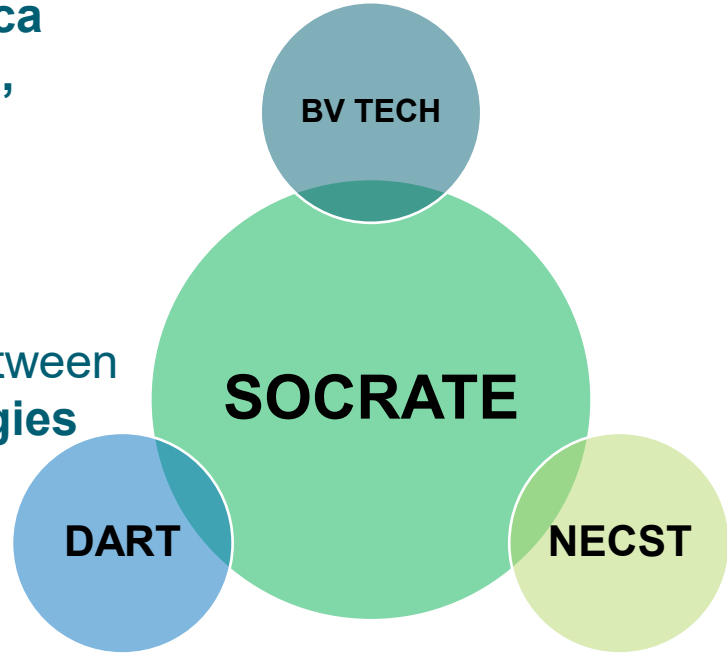
- **Satellite systems** are **critical infrastructures** increasingly exposed to **cyber-physical** threats.
- Integration of **terrestrial** and **non-terrestrial** networks expands the **attack surface**.
- **Cyber ranges** are essential tools to test and train operators under realistic adversarial conditions.
- Space-focused cyber ranges lack end-to-end link modeling and standard protocol integration.



THE SOCRATE PROJECT

Managed and co-funded by **Agenzia Spaziale Italiana (ASI)** through Mid-Term Research and Development projects **“Giornate della Ricerca Accademica Spaziale” (Research Day) ASI 2020,** topics **“Scientific Instrumentation, Cybersecurity and Advanced Materials”**

The **SOCRATE Project** proposal stems from a long-term collaboration between **BV TECH** and the **Departments of Aerospace Sciences and Technologies (DAER)** and **Electronics, Information and Bioengineering (DEIB)** of **Polytechnic University of Milan**

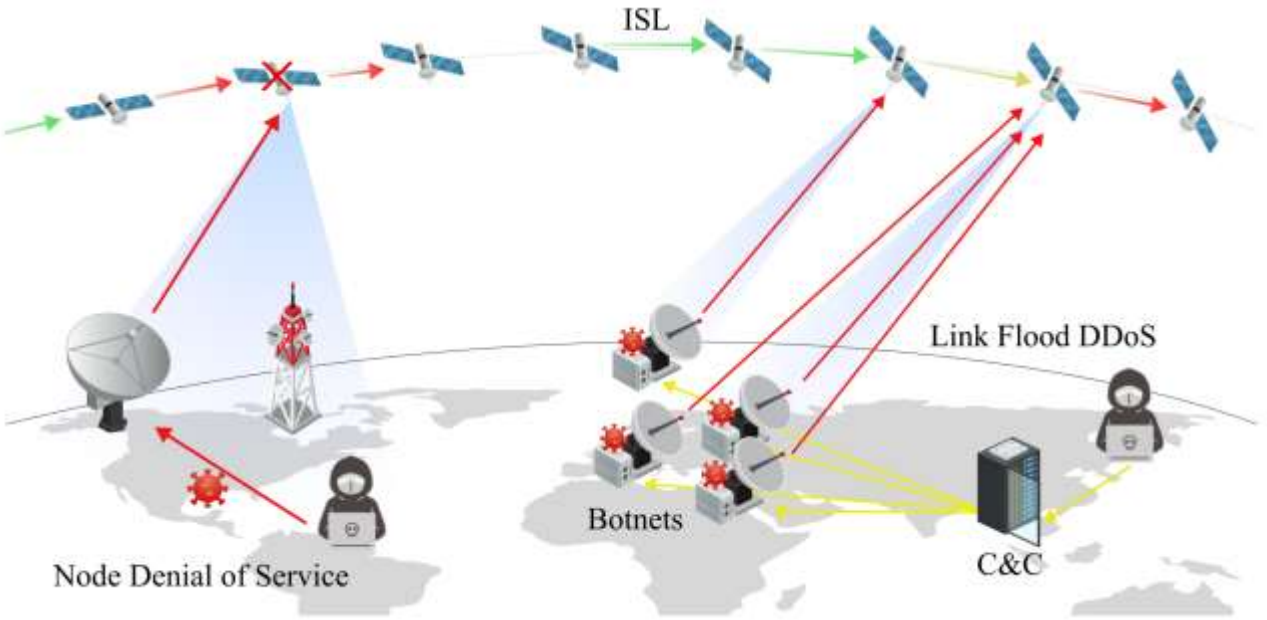


THE SOCRATE PROJECT

Satellite **O**perations **C**yber **RA**nge for **T**esting and **E**valuation

Goals:

- **Simulate** both **cyber and physical events** that may affect the system itself once the satellite is in orbit
- **Simulating the effect of external environmental parameters** (e.g. solar radiation, EM disturbances, Space Weather effects)
- **Simulate realistic satellite sub-system behaviour and interaction** (e.g. production and distribution of energy to various users)



Simulated Components:

- Terrestrial Segment
- Communication Channel
- Satellite

THE SOCRATE PROJECT

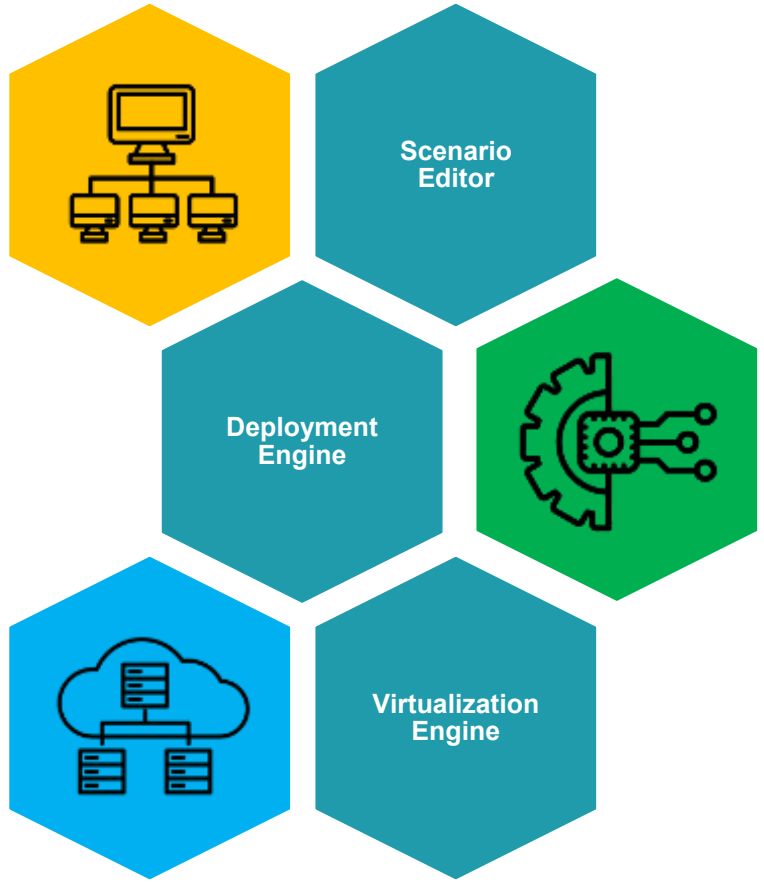
The **BV TECH Cyber Range** is a hybrid/virtual environment designed to simulate real-world cybersecurity scenarios

Features:

- **Full customization of Network topology,** Number of nodes, System typology (Unix, Windows), Attack and defense tools, both real and virtualized HW connections
- **Physical Models**, i.e., OT Models integration
- **Efficient** HW resources allocation

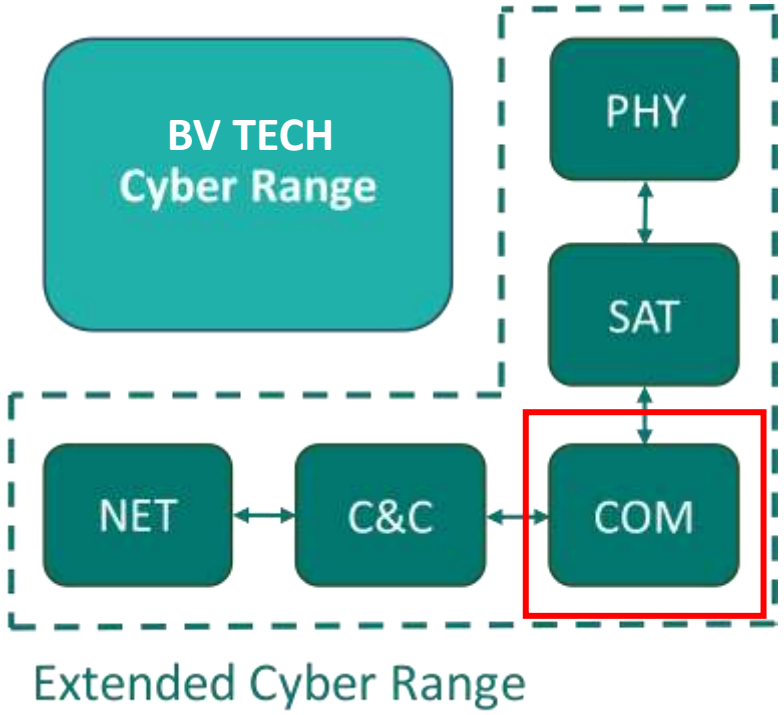
Scopes:

- **Replicate** the complexity of real-world systems in a controlled environment
- **Develop** security strategies
- **Individuals** or **Teams** can practice in attack & defense strategy



THE SOCRATE PROJECT

- **SOCRATE** models the different elements which are part or affect the satellite mission system through separate modules and the interaction and interfaces between them
- The **PHY** module defines the physical parameters that influence the behavior of the simulator
- The **SAT** module has various on-board subsystems, including (i) OBC, (ii) TT&C, (iii) PROP, (iv) POW (v) AOCS, and (vi) THERMAL
- The **COM** module defines the satellite-Earth bidirectional channel. The COM module defines the transmission mode and antenna system characteristics (frequencies, modulation, bandwidth, antenna gain, S/N ratio, BER, etc)
- The **C&C** Module is a simplified operator interface that allows satellite command transmissions and responses and/or signals to be received from the satellite
- The **NET** module allows the modeling of both legitimate and non-legitimate terrestrial transmission stations to simulate the possibility of unauthorized access to the ground-satellite communication channel



GOAL OF THIS WORK

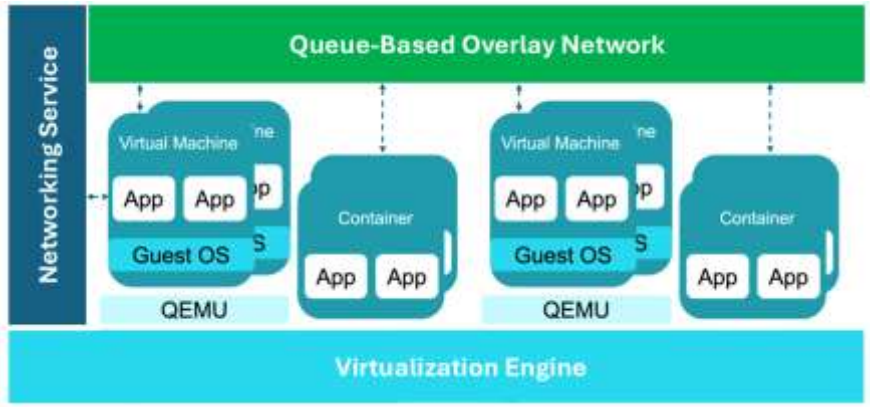
Develop a **modular system-level simulation** framework for GEO satellite links:

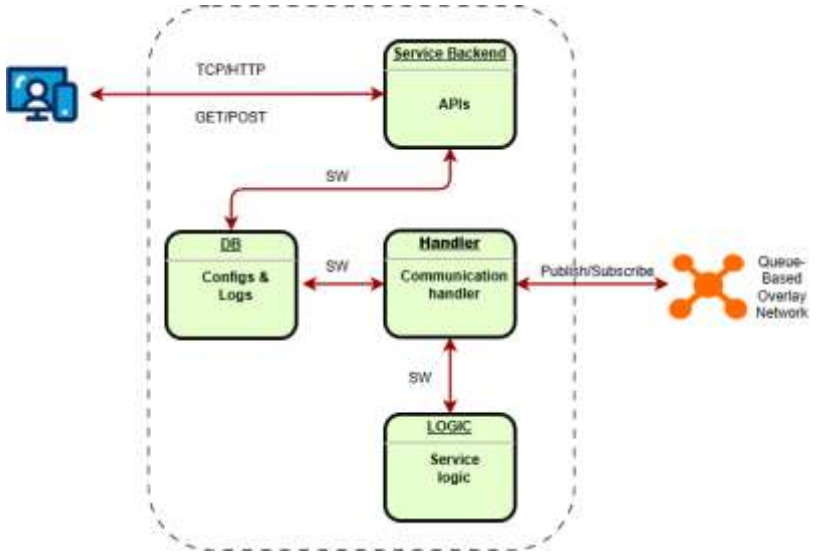
- Designed for cyber range environments.
- Provides **realistic** end-to-end modeling from ground to space.
- Integrates **CCSDS** and **SLE** protocol stacks.
- Enables **realistic emulation** of jamming, interference, and environmental effects.
- **Complete control over the information flow** — from data packets to individual bits and RF waveforms

The Proposed framework uniquely combines CCSDS/SLE protocol emulation with **ITU-compliant RF modeling**.

PROPOSED FRAMEWORK

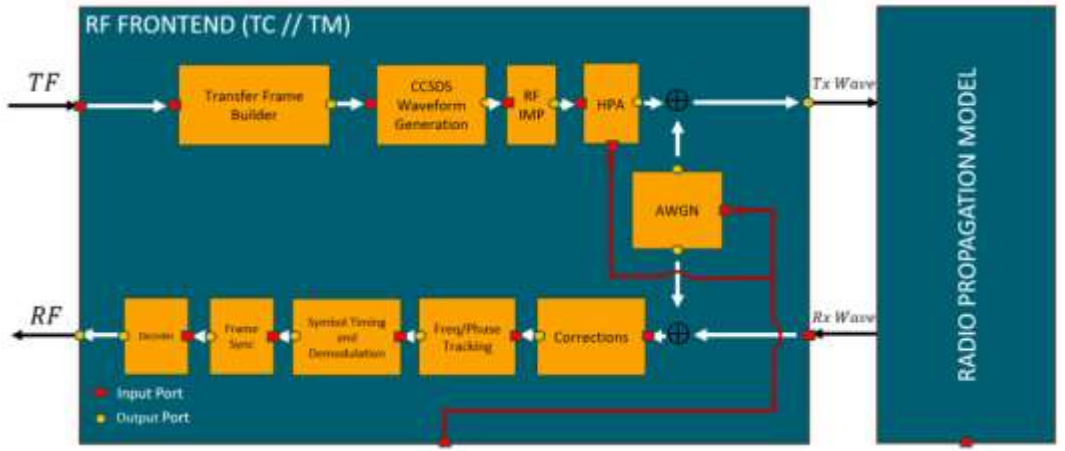
- **Virtualized design**: supports both Virtual Machines (VMs) and containers
- **Queue-based overlay network**: event-driven interactions with fine-grained control over packet flow, latency, and delay.
- **Modular block-based**: separates service logic, communication handling, data management, and API exposure.
- **Independent deployment**: components can be developed, tested, and deployed individually.
- **Message structure:**
  - Uplink/Downlink branch: raw bitstreams, SNR, BER, channel capacity, and transmission errors
  - Link Info: contextual metadata (timestamp, ground station parameters, satellite position).





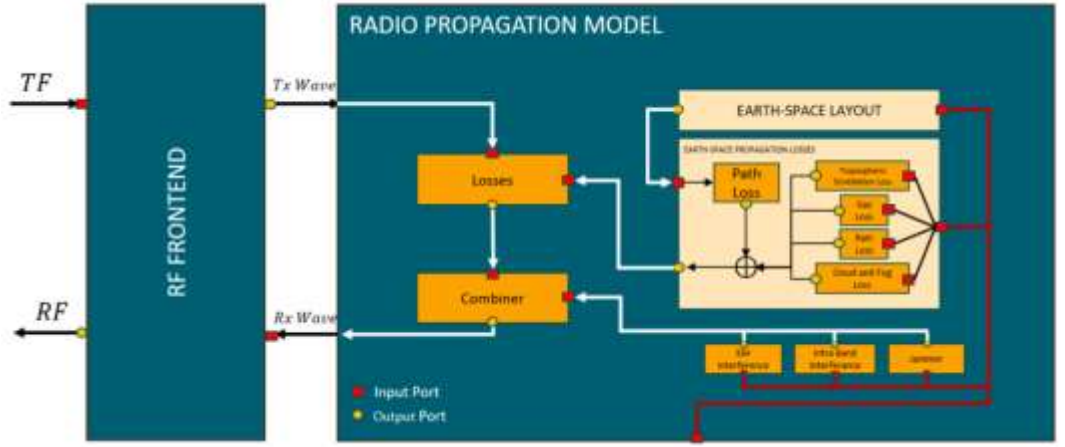
RF FRONTEND

1. **RF CCSDS Frontend**: handles modulation and waveform generation
2. **Radio Propagation Model**: simulates channel and environmental effects.



RF CCSDS Frontend generates complex baseband **CCSDS TC/TM waveforms** from input bitstreams.

- Frames data into CCSDS transfer frames (up to 800 octets).
- Amplifies the signal to transmission power.
- Adds Additive White Gaussian Noise (AWGN) based on earth–space link parameters.
- Receiver chain performs synchronization, demodulation, and decoding to obtain the output packet.



RADIO PROPAGATION MODEL

Radio Propagation module evaluates **satellite link budget** under realistic Earth–space conditions.

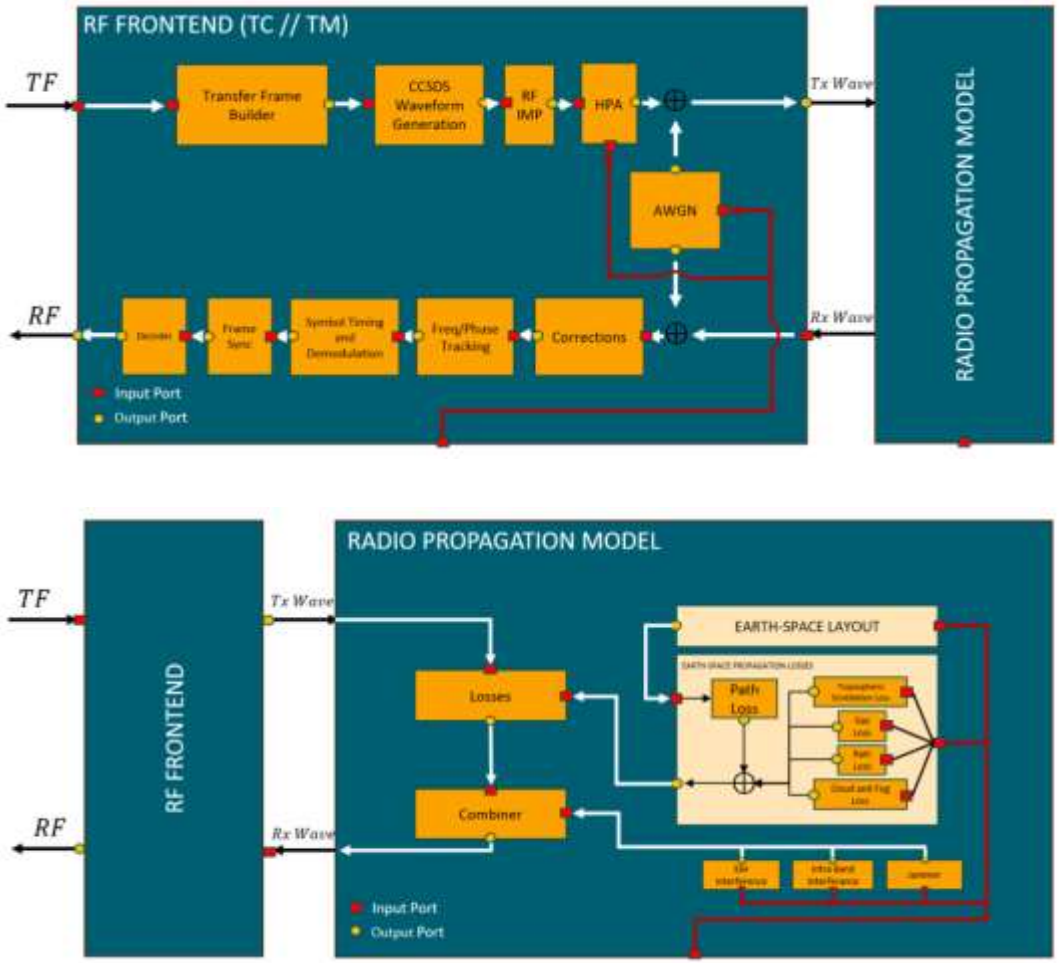
- Implements **ITU-R P.618** propagation model with real meteorological data (Meteostat).
- Free-space path loss, atmospheric attenuation, polarization, pointing, rain, and cloud attenuation

$$EIRP = P_{tx} - L_f - L_{tx} + G_{tx} \qquad L_{fs} = 20log_{10}\left(\frac{4\pi d}{\lambda}\right)$$

$$P_{rx} = EIRP - L_{fs} - L_{atm} - L_{pol} - L_{point}$$

$$\frac{C}{N_0} = P_{rx} + \frac{G}{T} - 10log_{10}(k_{Boltz}) - L_{rx}$$

$$\frac{E_b}{N_0} = \frac{C}{N_0} - 10log_{10}(rate)$$



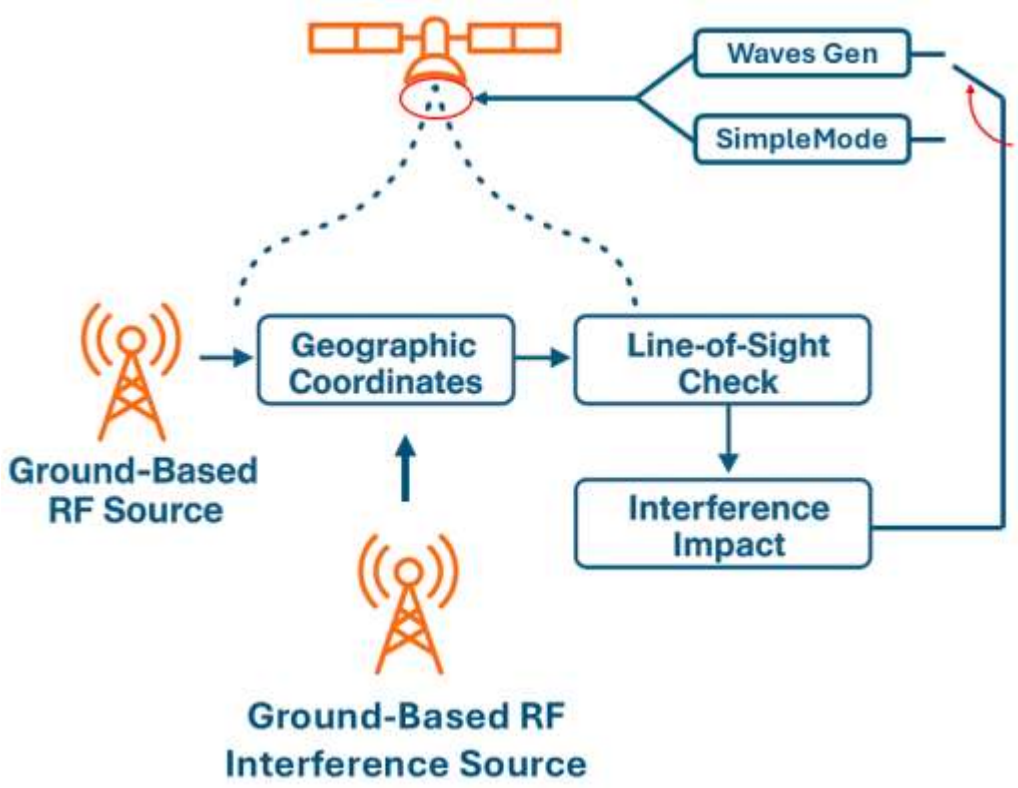
INTERFERENCE MODELING

Includes both **intentional** and **unintentional interference** modeling.

- **Intentional**: i.e., jamming
- **Unintentional**: spectral overlap, EM interference

Implemented through waveform-level signal superposition of distinct carriers, bandwidths, and power levels.

Each interfering source follows the same transmission and propagation model with line-of-sight verification.



SOLAR FLARES

Solar flare noise based on **ITU-R S.1525**.

The model considers the **Sun aligned behind the satellite from the Earth's perspective** (worst case).

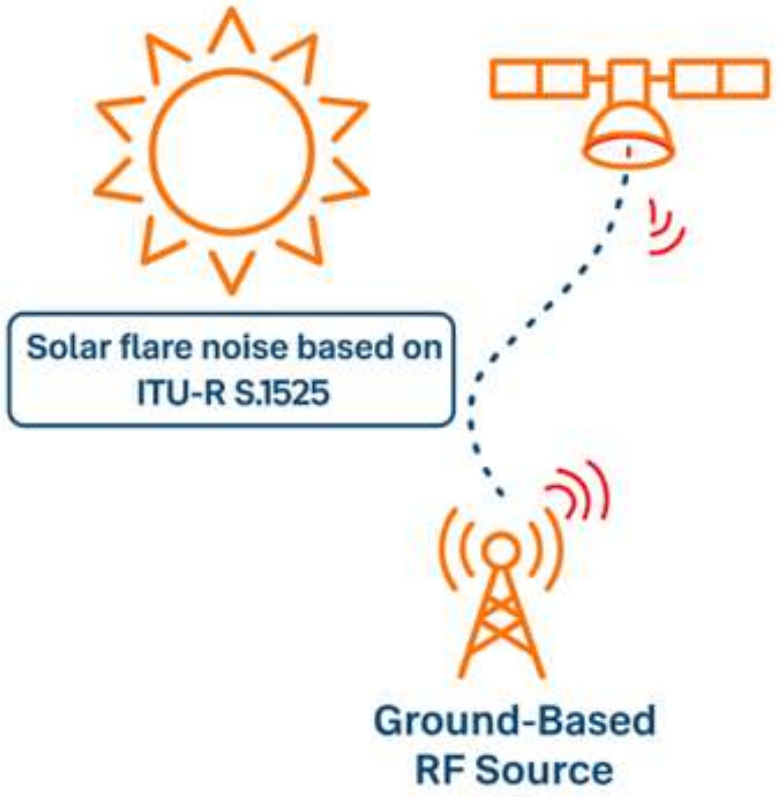
It contributes to high-intensity radio emissions that degrade the SNR.

The interference is based on solar radio flux density and antenna characteristics

$P_{sun} = S_{sun} A_{eff} B$

S_{sun} $solar\ spectral\ density\ W/m^2$/Hz

$A_{eff} = \eta\pi \left(\frac{D}{2}\right)^2$ $effective\ antenna\ area$



PROPAGATION DELAY

Channel modules introduce a baseline propagation delay representing the physical transmission time of a satellite link.

The propagation delay is given by:

$$T_p = \frac{d}{c}$$

where d is the line-of-sight distance and c is the speed of light (~3×10^8 m/s).

Distance (d) is computed by converting satellite and ground station coordinates into ECEF coordinates using the WGS-84 ellipsoid.

The relative vector is then projected into the local NED frame, and its Euclidean norm gives the line-of-sight distance.

MODELS INTEGRATION

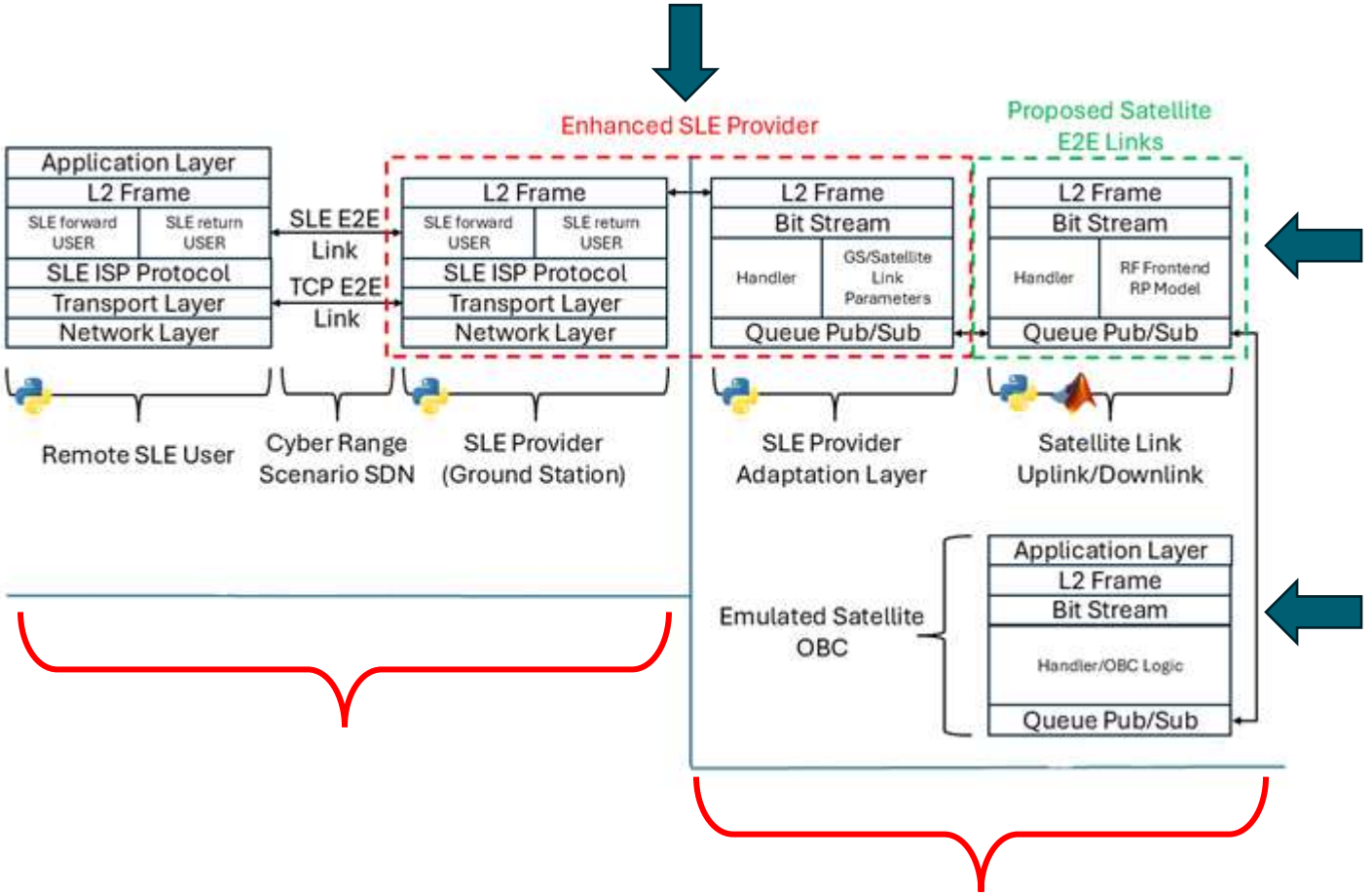
1. **Satellite Threat Scenario** – emulates SLE User(s) and Ground Station Provider(s) roles.

2. **Satellite Scenario Infrastructure** – simulates wireless links using the queue-based architecture.

SLE User and Provider communicate over a TCP/IP stack managed by the virtualization platform

SLE Provider based on open-source **visionspacetec/sle-provider**, extended for queue-based data exchange via publish/subscribe

Bitstreams generated from CCSDS Level-2 Frames and passed through queues between modules



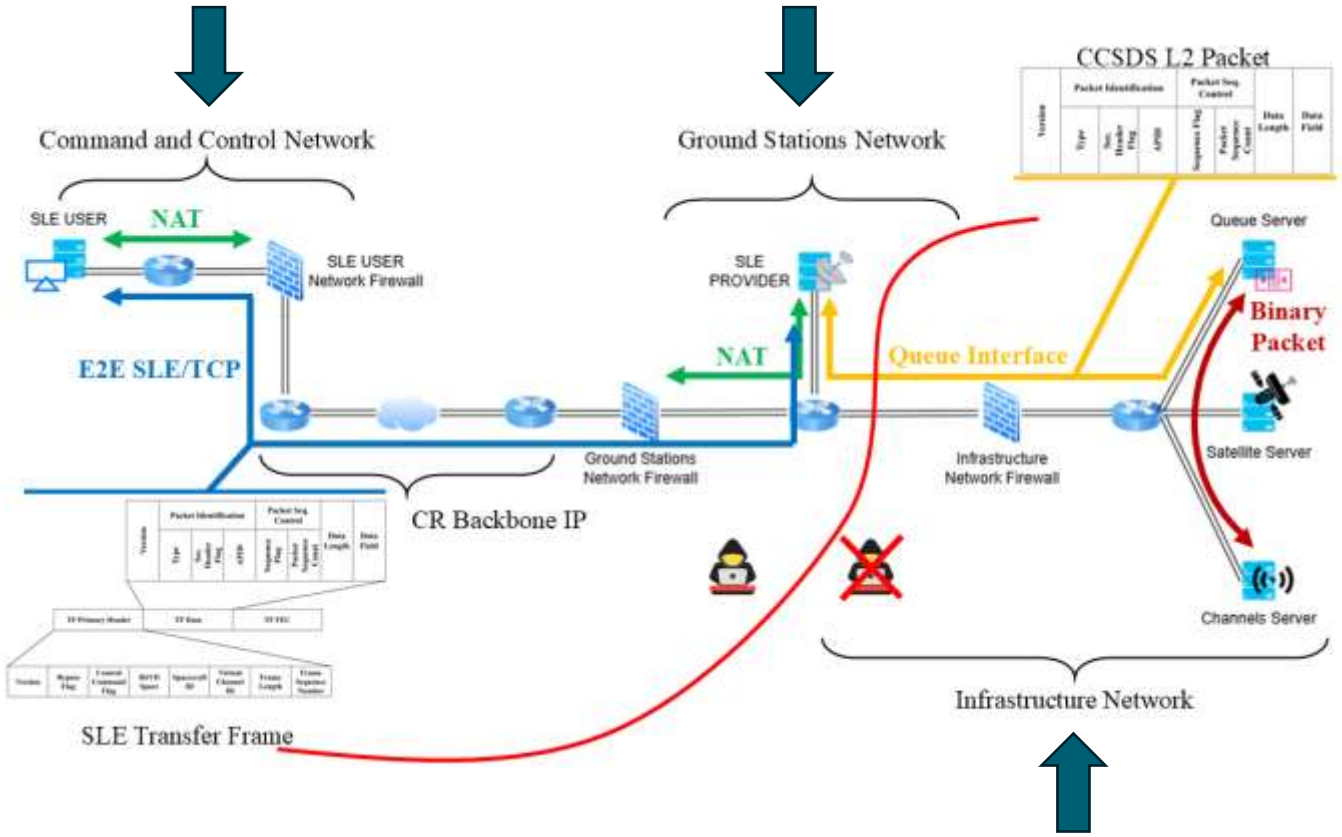
REFERENCE TOPOLOGY & VALIDATION

1. **Command & Control Network** – hosts the SLE User.
2. **Ground Stations Network** – hosts the SLE Provider.
3. **Infrastructure Network** – includes queue and channel servers.

Each zone is protected by firewalls to enforce network segmentation policies

NAT exposes only selected services (e.g., SLE Provider), keeping internal modules isolated

The red boundary defines a trust boundary protecting backend components from external access.



REFERENCE TOPOLOGY & VALIDATION

Agenzia Spaziale Italiana

Validation Scenario
Simplified but realistic single-link setup: one Ground Station (GS) and one GEO satellite.

Provides a controlled, traceable baseline for assessing system behavior under normal and stressed conditions.

Geographical Configuration
Ground Station: Latitude 40.53°, Longitude 17.43°
Satellite: Nominal GEO slot, Latitude 3.06°, Longitude 0.11°, altitude ≈ 38,224 km.

Physical Layer Parameters
Frequency band: Ka-band (≈30 GHz). Bandwidth: 36 MHz
Bitrate: 10 Mbps
Includes atmospheric attenuation

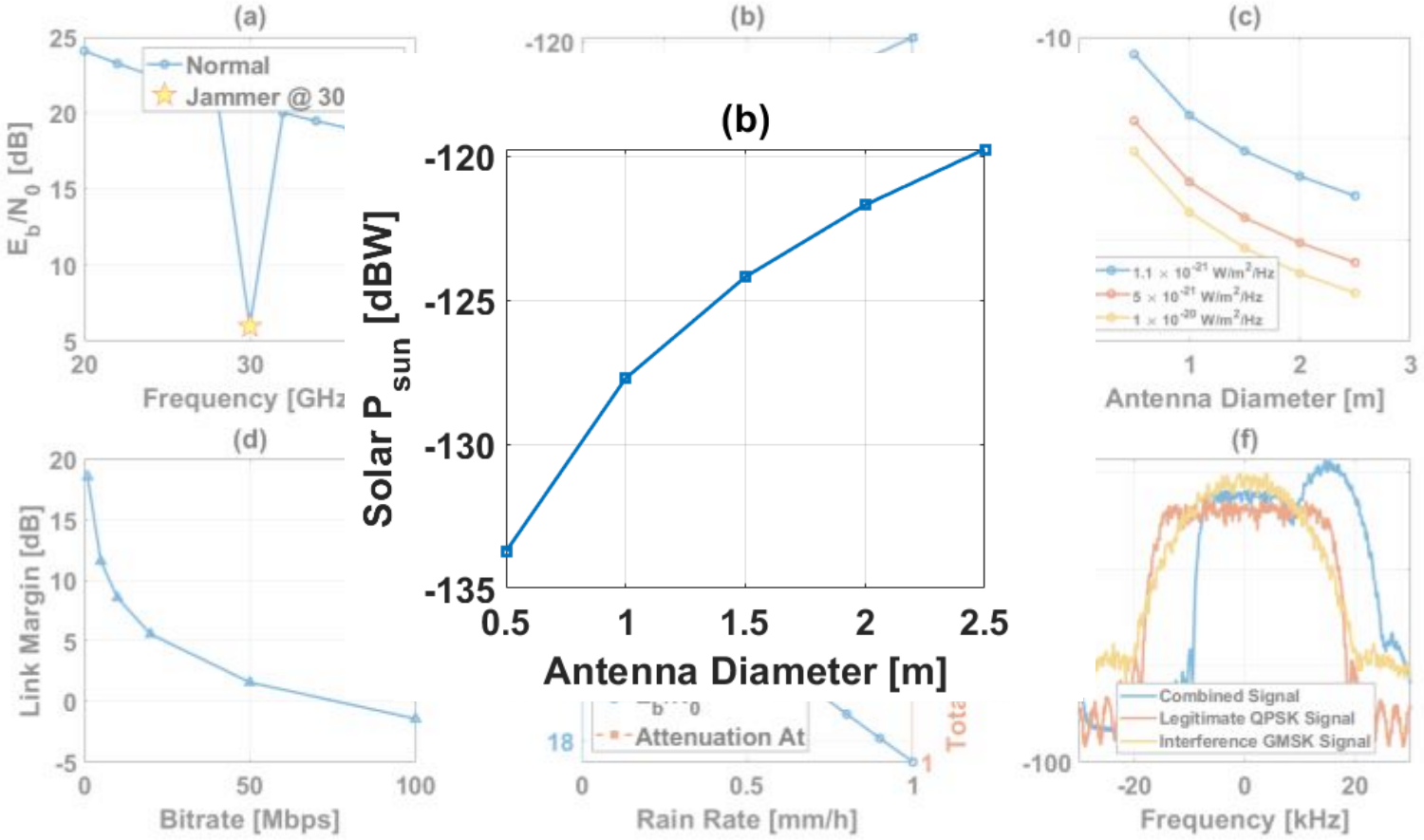
Parameter	Value	Unit / Note
Ground Station (GS) Configuration		
Latitude	40.53	degrees
Longitude	17.43	degrees
Altitude	120	meters
Parasite GS Configuration		
Latitude	40.63	degrees
Longitude	17.94	degrees
Altitude	120	meters
Satellite (SAT) Configuration		
Latitude	3.06	degrees
Longitude	0.11	degrees
Altitude	38224	km
Transmitter (GS)		
HPA Output Power	23	dBW
Output Back-Off (OBO)	6	dB
Feeder Loss	2	dB
Other Losses	3	dB
Antenna Gain	46.5	dBi
Receiver (SAT)		
Interference Loss	2	dB
G/T (Gain over Temp)	25	dB/K
Feeder Loss	1	dB
Other Losses	1	dB
Link Properties		
Carrier Frequency	30	GHz
Bandwidth	36	MHz
Bit Rate	10	Mbps
Required E_b/N_0	10	dB
Availability	99.9	%
Implementation Loss	2	dB
Polarization Mismatch	45	degrees
Antenna Mispointing Loss	1	dB
Radom Loss	1	dB
Solar Interference Power Estimation		
Antenna diameter	1.2	m
Antenna efficiency	60	%
Solar flux density	1.1×10^{-21}	$W/m^2/Hz$

BV TECH · POLITECNICO MILANO 1863 · DART Group · NECST laboratory

VALIDATION

The link quality (Eb/N_0) decreases from 20 GHz to 40 GHz due to higher free-space path loss and atmospheric attenuation; a sharp drop at 30 GHz confirms the correct modeling of jammer injection.

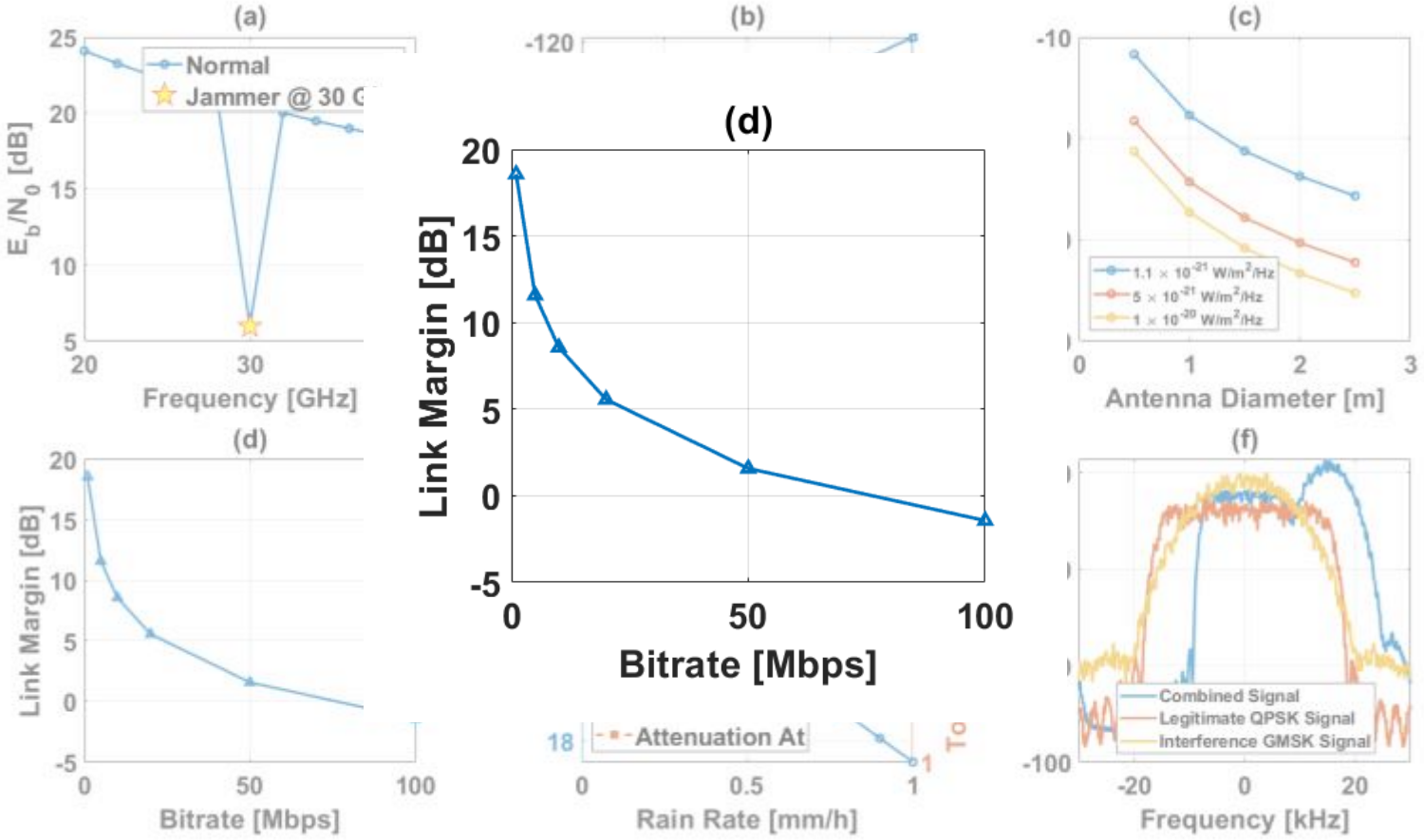
Received solar noise power increases with antenna aperture, showing that larger antennas collect more broadband interference despite higher gain.



VALIDATION

Under quiet, moderate, and higher solar interference, the framework reproduces progressive Eb/N degradation, validating its ability to emulate space-weather effects.

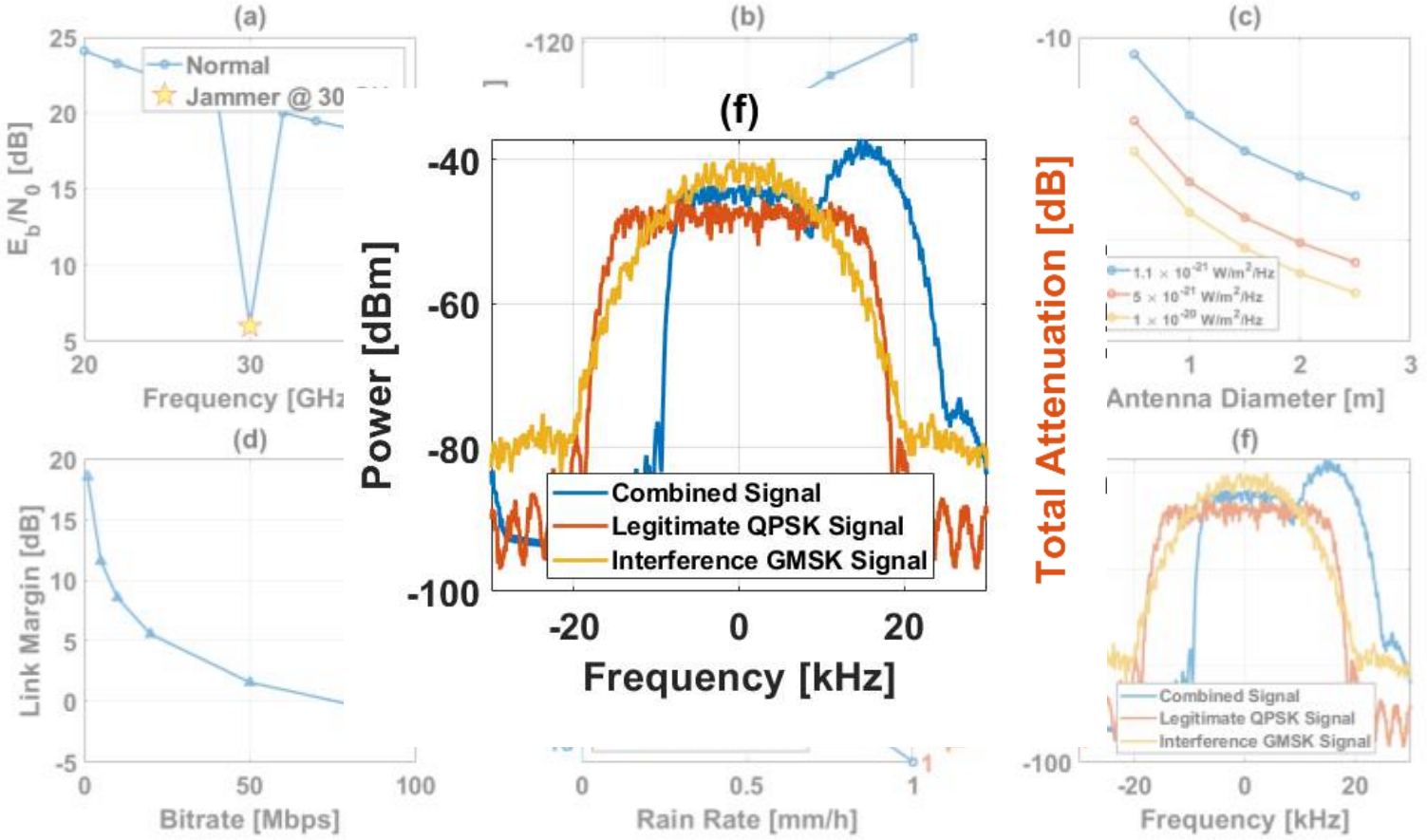
The link margin decreases as bitrate increases; the connection remains stable up to mid-range rates before approaching outage thresholds.



VALIDATION

Increasing rain rate produces higher attenuation and linear Eb/N_0 degradation, confirming realistic weather-aware behavior aligned with ITU-R P.618.

The combined QPSK + GMSK waveforms reveal evident in-band interference, demonstrating the framework's capability to model spectral coexistence and jamming.



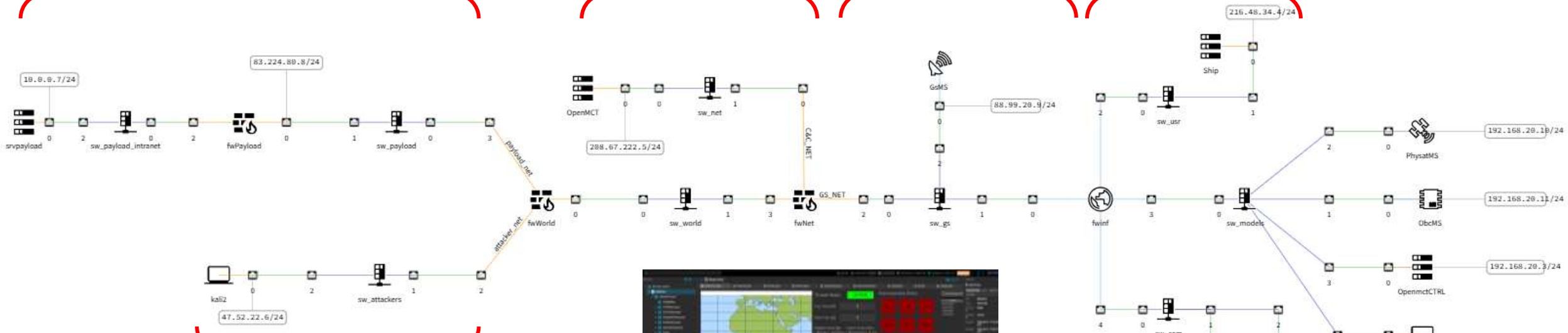
HOW IT WORKS?

Payload Net

C&C Net

GS Net

Payload Source (if needed)



Attackers Net

Infrastructure Net

CONCLUSIONS

- The **proposed work presents** a comprehensive **end-to-end framework for satellite link modeling**, integrating both space-specific communication protocols (CCSDS/SLE) and realistic physical-layer representations.

- The **framework covers the entire transmission chain**, from data encapsulation and waveform generation to RF propagation modeling, accurately reproducing environmental and channel impairments.

- **Interference scenarios**—including jamming, spectral overlap, and solar events—are explicitly modeled, enabling assessment of link robustness under different operational conditions.

- This **framework** provides a foundation for **secure**, **high-fidelity training and resilience evaluation**, bridging the gap between system-level cybersecurity and physical-layer dynamics in space communications.

- **Future work will focus** on extending the framework to **LEO and MEO constellations**, evaluating **multi-link scalability**, and incorporating **operator-in-the-loop** validation for hands-on cyber-range experimentation.

ACKNOWLEDGEMENT

The SOCRATE Project was managed and co-funded by **Agenzia Spaziale Italiana (ASI),** through Mid-Term Research and Development projects **“Giornate della Ricerca Accademica Spaziale” (Research Day) ASI 2020**, topics **“Scientific Instrumentation, Cybersecurity and Advanced Materials”**

THANK YOU FOR YOUR ATTENTION!

(QUESTIONS TIME)

Contacts:
Alessandro Santorsola: alessandro.santorsola@bvtech.com
BV TECH Cybersecurity Lab, Polytechnic University of Bari

Daniele Mammone: daniele.mammone@polimi.it
Polytechnic University of Milan

Stefano Longari: stefano.longari@polimi.it
Polytechnic University of Milan

Francesco Topputo: francesco.topputo@polimi.it
Polytechnic University of Milan

Matteo Mergè: matteo.merge@asi.it
Italian Space Agency