Securing Satellite Key Distribution via Covert Channels: A Cooperative Jamming and Watermarking Approach

SECURITY FOR SPACE SYSTEMS (3S) 2025
NOV 04-06, 2025 - ESTEC in Noordwijk, The Netherlands

S. Soderi[*†‡], E. Casini[§], M. Conti[†‡]

[*]*IMT School for Advanced Studies, Lucca, Italy*

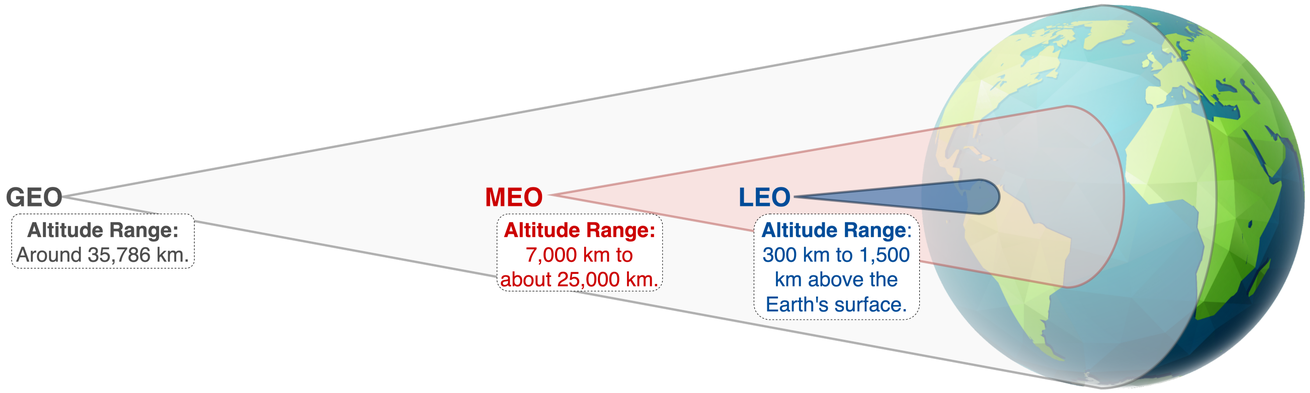
[†]*Cybersecurity National Laboratory, CINI - Roma, Italy*

[§]*ESA, European Space and Technology Center, ESTEC, Noordwjik, The Netherlands*

[‡]*University of Padova, Italy*

Outline

Satellite Industry



Mega-satellite projects with thousands of satellites in **Low Earth Orbit (LEO) clearly demonstrate the renewed interest in satellite communications and networks** by industrial ecosystems and standardisation organisations.

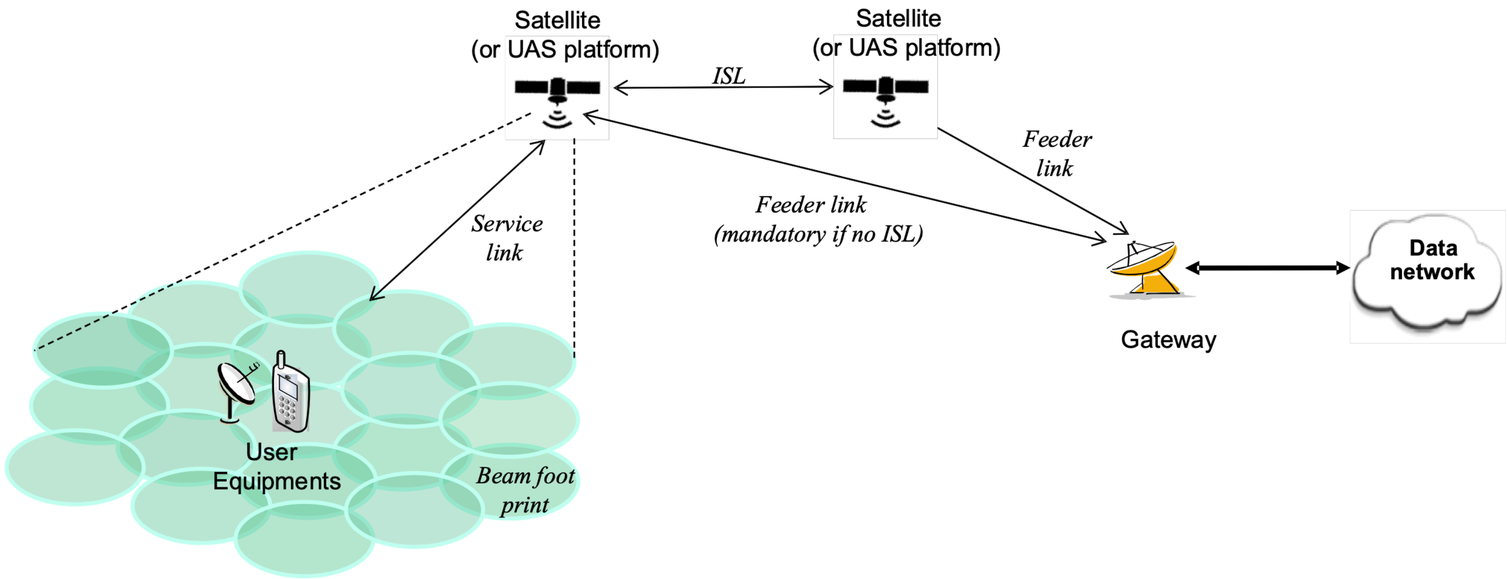
Types of NTN platforms , 3GPP TR 38.821 V16.2.0 (2023-03)

Platforms	Altitude range	Orbit	Typical beam footprint size
Low-Earth Orbit (LEO) satellite	300 – 1500 km	Circular around the earth	100 – 1000 km
Medium-Earth Orbit (MEO) satellite	7000 – 25000 km		100 – 1000 km
Geostationary Earth Orbit (GEO) satellite	35 786 km	National station keeping position fixed in terms of elevation/azimuth with respect to a given earth point	200 – 3500 km
UAS platform (including HAPS)	8 – 50 km (20 km for HAPS)		5 - 200 km
High Elliptical Orbit (HEO) satellite	400 – 50000 km	Elliptical around the earth	200 – 3500 km

European Union issued in 2023 **Space Strategy for Security and Defense.** A plan to protect EU space assets.
A key component is the IRIS²

Role of Satellites in Non-Terrestrial Networks and 6G

*A **non-terrestrial network (NTN)** refers to a network, or segment of networks using RF resources on board a satellite (or UAS platform).*



Field of view of the satellite (or UAS platform)

NTN network typical scenario - 3GPP TR 38.821 V16.2.0 (2023-03)

Advantages

- **Enabling**
  - massive machine-type communications (mMTC)
  - ultra-reliable low-latency communications (URLLC)
- **Global coverage**

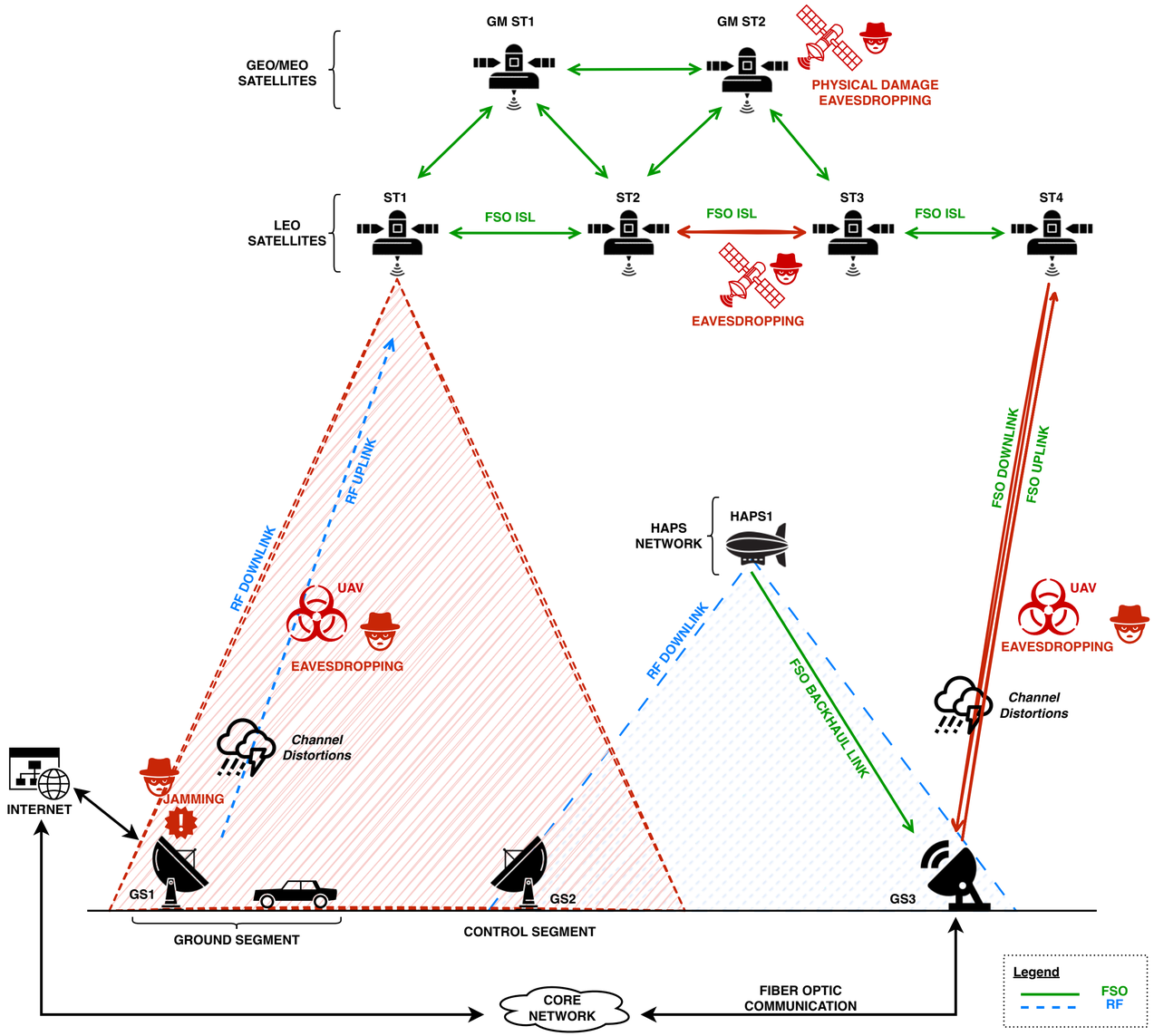
Disadvantages

- **High networking complexity**

Security Threats in RF FSO NTN

Physical Layer Security

Directivity of RF or FSO communications improves SATCOM security, **but we assume that this is not sufficient.**



Russian satellite Luch-5X approaches US and EU SATCOM

- Concerns about **Luch-5X** (military satellite) **moving near US-owned and EU satellites.**
  - Russian government has claimed they are not aggressive and are simply performing their designated role.
- **Data collection** and **signal analysis**
- Many reported incidents

SPACENEWS

Newslette

News | More Categories | Sponsored | Post a Press Release | Video | More | Media Kit

Kay Sears, Intelsat General

WASHINGTON — A mysterious Russian military satellite parked itself between two Intelsat satellites in geosynchronous orbit for five months this year, alarming company executives and leading to classified meetings among U.S. government officials.

[*] Proton rocket that launched the Luch-5X into space

A Proton-M rocket stands poised to launch the Luch/Olimp satellite from Baikonur in September 2014. (credit: Roscosmos)

The Guardian

Eur

'Act of espionage': France accuses Russia of trying to spy on satellite data

Defence minister says Russia's Luch-Olymp craft got 'so close' to French military satellite last year

Florence Parly, France's defence minister, said officials took the 'appropriate measures' and observed the Russian craft manoeuvring near other targets as well Photograph: Vesa Moilanen/Rex/Shutterstock

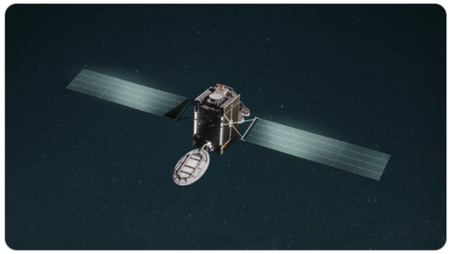
Olimp and Yenisei-2: Russia's secretive eavesdropping satellites (part 1)

by Bart Hendrickx
Monday, November 20, 2023

The Lost Comms
@thelostcomms

Russian spy satellite approaches Norwegian communication satellites

The infamous Russian Olymp K2 satellite is maneuvering towards three Norwegian communication satellites. The distance has shrunk from 80 to 20 kilometers during July.



6:29 PM · Jul 25, 2024 · **6,261** Views

Source [*]: Williaam Graham. "Russian Proton-M launches Olymp-K-2 military satellite." NASASpaceFlight (2023). https://www.nasaspaceflight.com/2023/03/proton-olymp-k-2/

Motivation

INTRODUCTION

What ...

- **Harden Digital Infrastructures:** NTN and LEO satellite constellations, are enabling high-speed Internet, navigation, and remote sensing. Unfortunately, **real incidents highlight the gravity of security threats.**

- **Computational Load Control:** Strong encryption protects data but requires frequent key exchanges due to fast-moving LEO satellites, **introducing computational overhead and key management complexity.**

- **Attacker's Location:** RF/FSO beams can offer narrower coverage than RF and enhance the security, but **without the knowledge of the attacker's position**, we cannot avoid the eavesdropping or jamming.

Contribution

INTRODUCTION

EXPLOITING HIDDEN TRANSMISSIONS AND COOPERATIVE FRAMES OBFUSCATION TO HARDEN THE SECURE KEY DISTRIBUTION

Main Contribution

Combining cooperative **frames obfuscation with physical layer watermarking** remaining compatible with CCSDS/USLP protocols.

Key Intuition

The legitimate **transmitter and receiver collaborate** to selectively mask parts of the bitstream. Only the receiver **knows** which bits are jammed and can easily rebuild the original data.

Minimizes Tx Changes

An attacker **examining the spectrum observes no noticeable change**, making it extremely difficult to identify which portions of the signal are obfuscated.

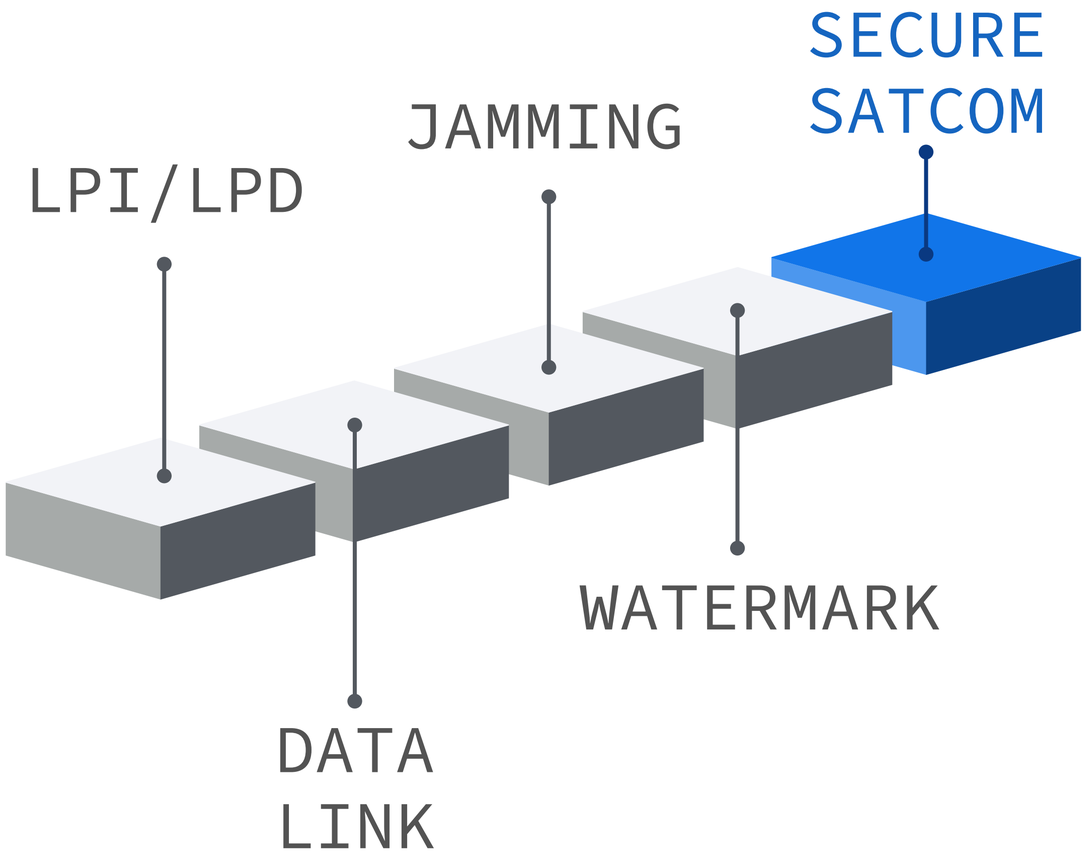
Additional Contributions

Avoids major hardware or protocol modifications by inserting watermark and jamming in CCSDS protocols.

Background

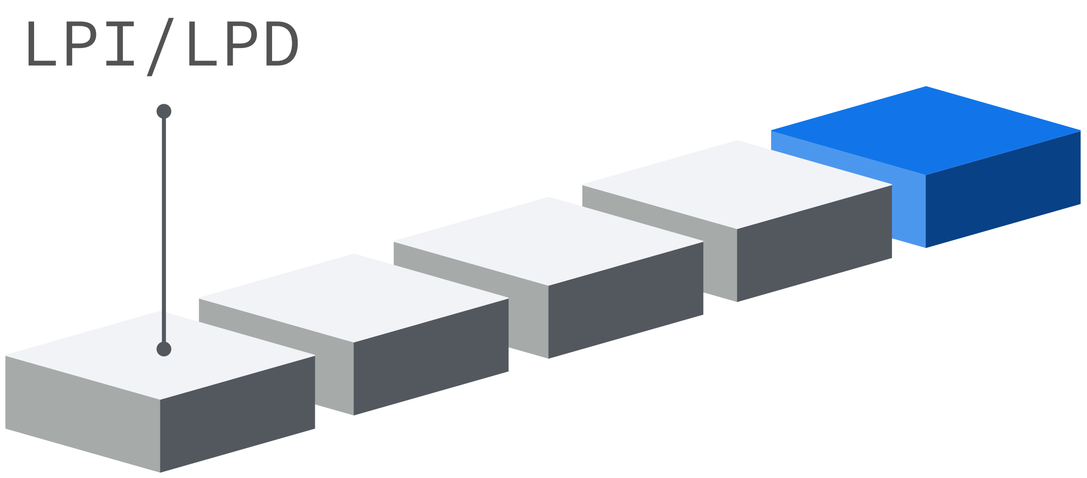
WHAT ARE THE KEY ELEMENTS OF THIS PROPOSAL?

Short Recalls useful for understating this proposal.



TRANSEC LPI/LPD Communications

BACKGROUND



TRANSEC

Transmission Security (TRANSEC) which is a component of Communications Security (COMSEC). **TRANSEC aims to protect transmissions from interception and exploitation by means other than cryptanalysis.**

LPI/LPD

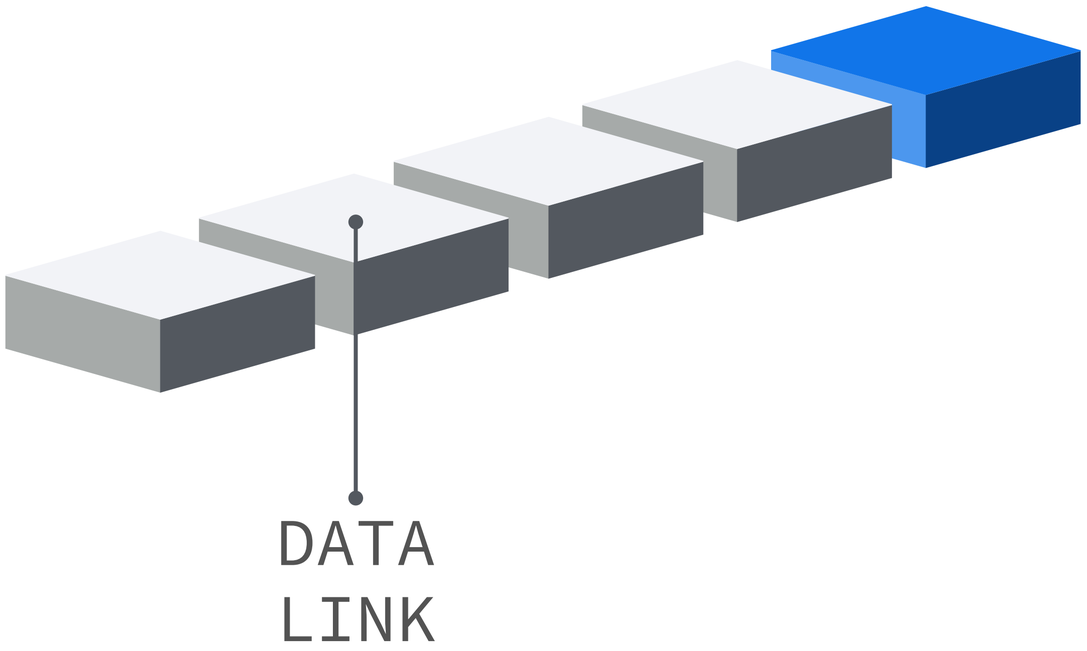
Low Probability of Intercept (LPI) uses frequency hopping and directional antennas to prevent signal capture. **Low Probability of Detection (LPD)** hides the signal's existence by spreading energy across wider bandwidths, reducing power spectral density below noise thresholds.

Example

Spread spectrum techniques like **DSSS** distribute signals using **pseudorandom codes**, making them difficult to detect and intercept while maintaining authorized receiver capability.

Space Data Link Protocol

BACKGROUND

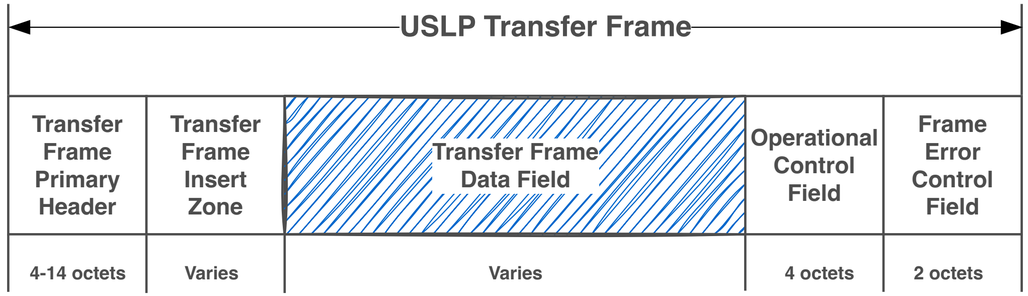


Space Data Link Protocol (CCSDS USLP)

The **Unified Space Link Protocol (USLP)** is the CCSDS standard for satellite data link communications. It provides a flexible transfer frame structure supporting multiple virtual channels, multiplexing, and service types (telemetry, telecommand, high-rate data) without separate hardware.

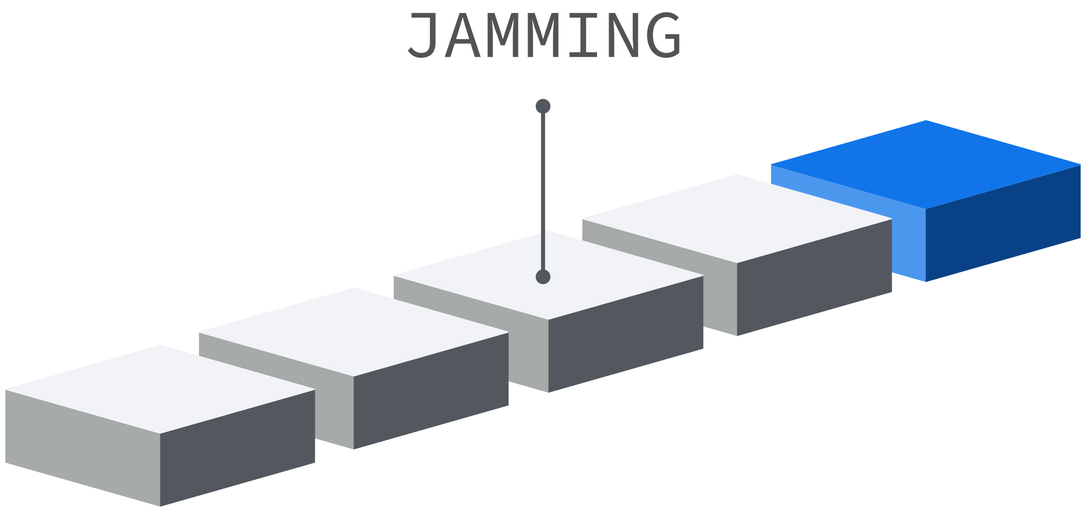
How do we use it?

The protocol includes optional security headers for cryptographic parameters and **can embed protection mechanisms directly within the payload Transfer Frame Data Field (TFDF)** — such as watermarked signal — while preserving standard USLP framing, enabling backward compatibility with existing systems.



Cooperative Jamming: Frame Obfuscation

BACKGROUND



Cooperative Jamming

Cooperative jamming (friendly jamming) is a physical layer security technique where legitimate **transmitter and receiver intentionally inject structured interference** that authorized receivers can remove, while eavesdroppers cannot.

Frame Obfuscation

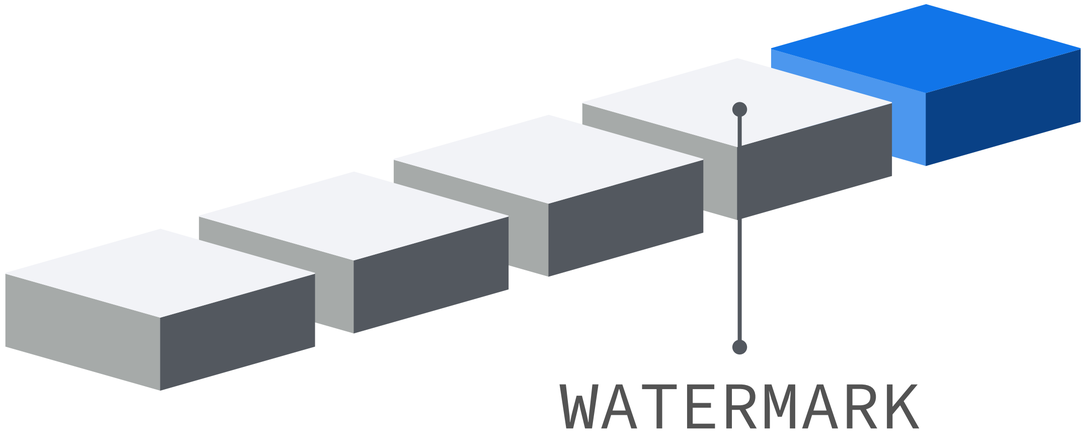
Frame obfuscation **deliberately corrupts specific USLP frames** based on **indexes** communicated via a covert LPI/LPD channel.

Eavesdropper's Channel gets worse

The authorized receiver uses a shared spreading code and watermark information to recover obfuscated data perfectly, while an **eavesdropper sees** effective erasures on obfuscated frames and watermark-induced interference on clean frames, **significantly degrading eavesdropper capacity without hardware modifications.**

Spread Spectrum Watermark

BACKGROUND



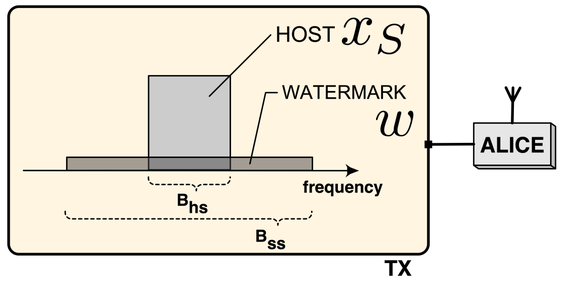
Watermarking

Watermarking is a method for **embedding** a signal that carries a message within another (host) signal .

Spread Spectrum (SS) Watermarking

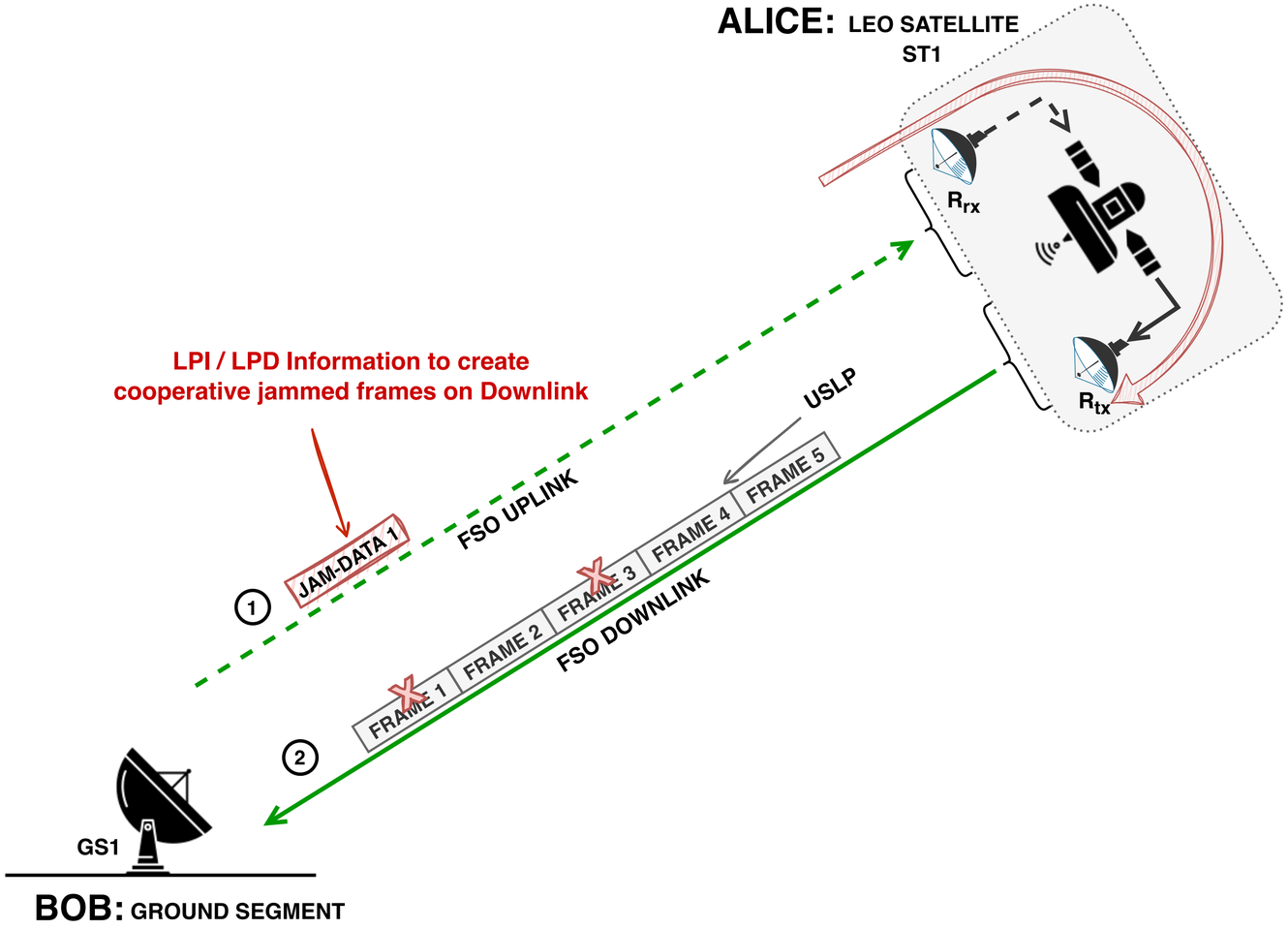
Spread spectrum watermarking **embeds a secondary signal (watermark) into a host signal using a pseudorandom spreading code**, allowing authorized receivers to extract it while providing robustness to interference.

For example, the watermark is constructed by using the **Direct Sequence Spread Spectrum (DSSS)** technique.



$$x'_S(i) = x_S(i) + \mu w(i)$$

System Model



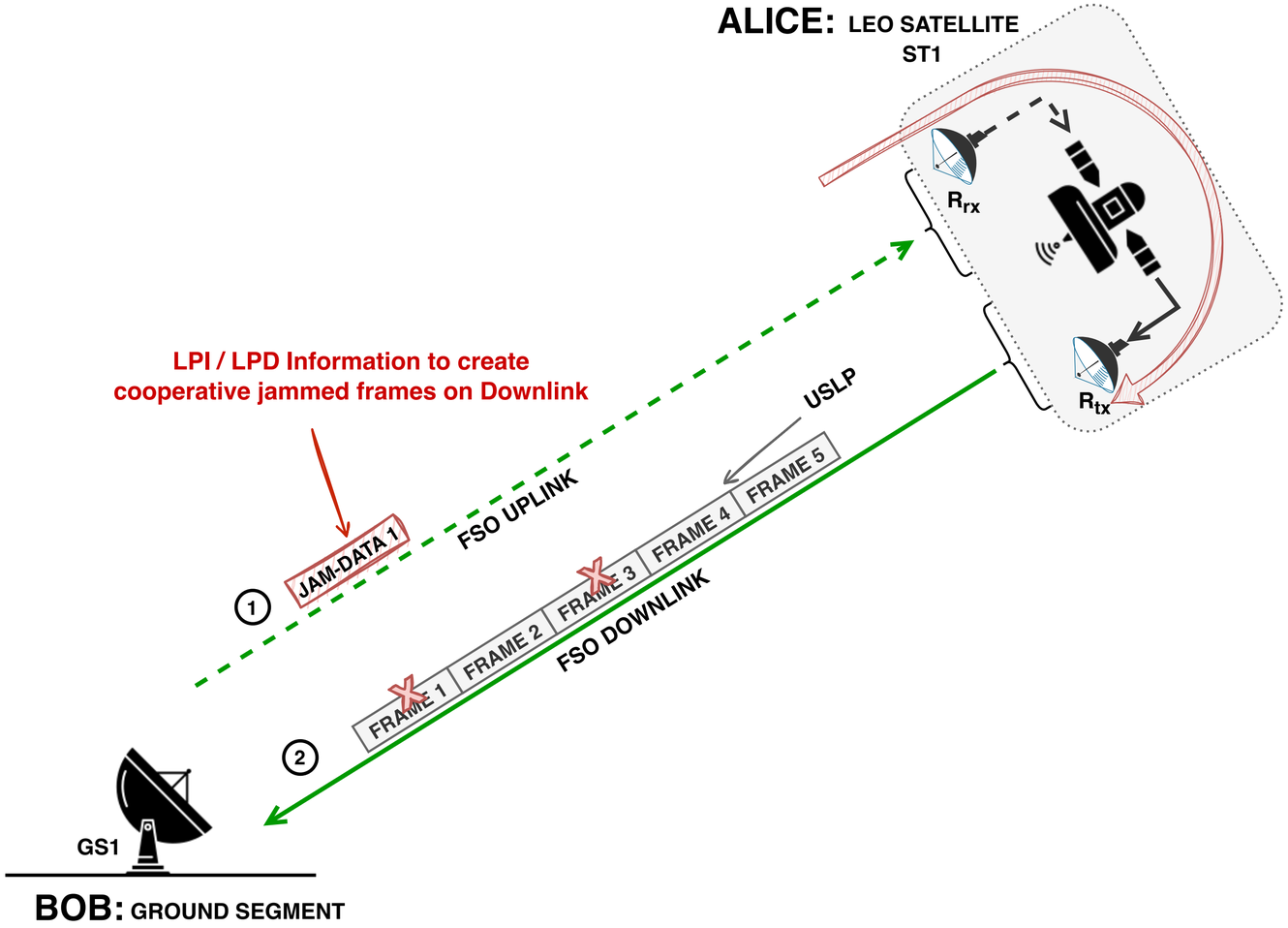
Objective:

Protect the FSO Downlink (**ALICE → BOB**)

Use case (reference architecture)

- **Free Space Optics (FSO)** Uplink/Downlink Communications
- **PHY LAYER:** Optical On-Off Keying modulation
- **RX:** Intensity Modulation/Direct Detection (IM/DD)
- **DATA LINK LAYER:** Unified Space Data Link Protocol (USLP)
  - Watermarked signal' samples embedded inside the **TFDF**.
  - This approach preserves **interoperability** with existing USLP and CCSDS-based infrastructure.

Watermarked Cooperative Jamming Algorithm

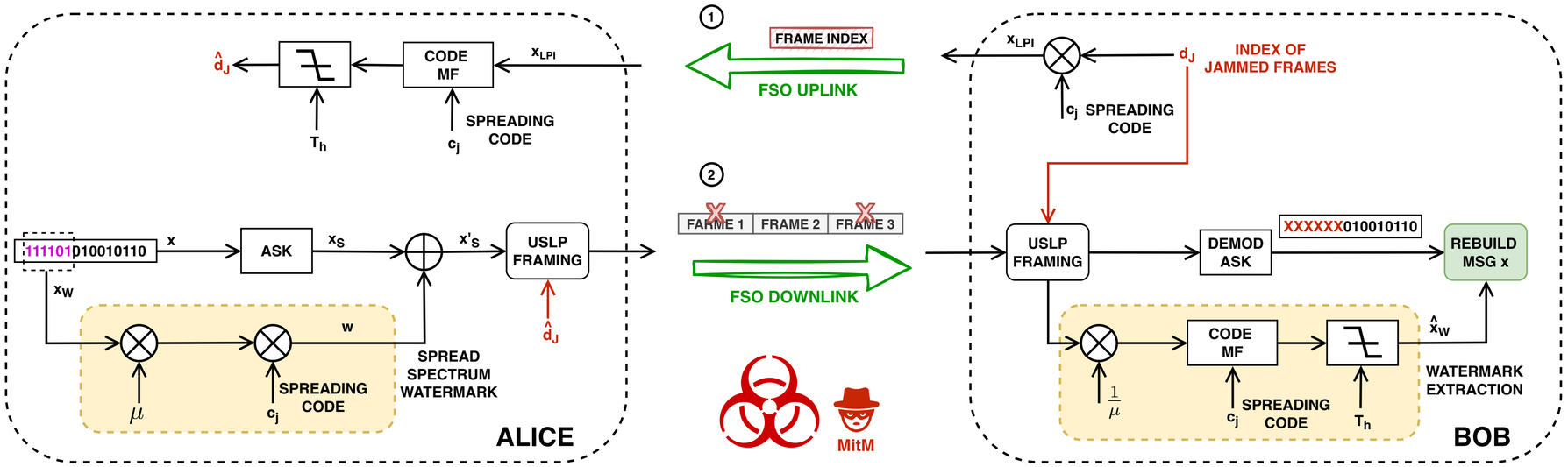


Algorithm 1: Watermarked Cooperative Jamming

procedure DOWNLINK SATCOM DEFENCE
- **Input**: x_S, c_W
- **Covert Communication (BOB)**: The legitimate receiver communicates to the legitimate transceiver the index of USLP (d_J) must be obfuscated in the downlink.
- **SS Watermarking (ALICE)**: The original message is modulated ASK. One part of the original message is first modulated with DSSS and then embedded into the host ASK signal.
- **Data Obfuscation and Transmission (ALICE)**: The payload of the USLP frames with index d_J is first obfuscated, and then the new data stream is sent to Bob.
- **Signal Processing at Receiver (BOB)**: The receiver knows d_J and can discard the USLP corrupted frames transmitted by Alice. The received signal is then processed by the ASK demodulator to recover the data, but due to the jamming, part of the received signal is now corrupted and unusable.
- **Watermark Extraction (BOB)**: The receiver extracts the SS watermark from the received signal by using a code-matched filter.
- **Symbol Rebuild (BOB)**: Knowing which bits are jammed by the receiver, i.e., Bob, can rebuild a clean symbol using information contained in the watermark.
- **Output**: x'_S

end procedure

Step (1): Covert Communication Channel (1/3)



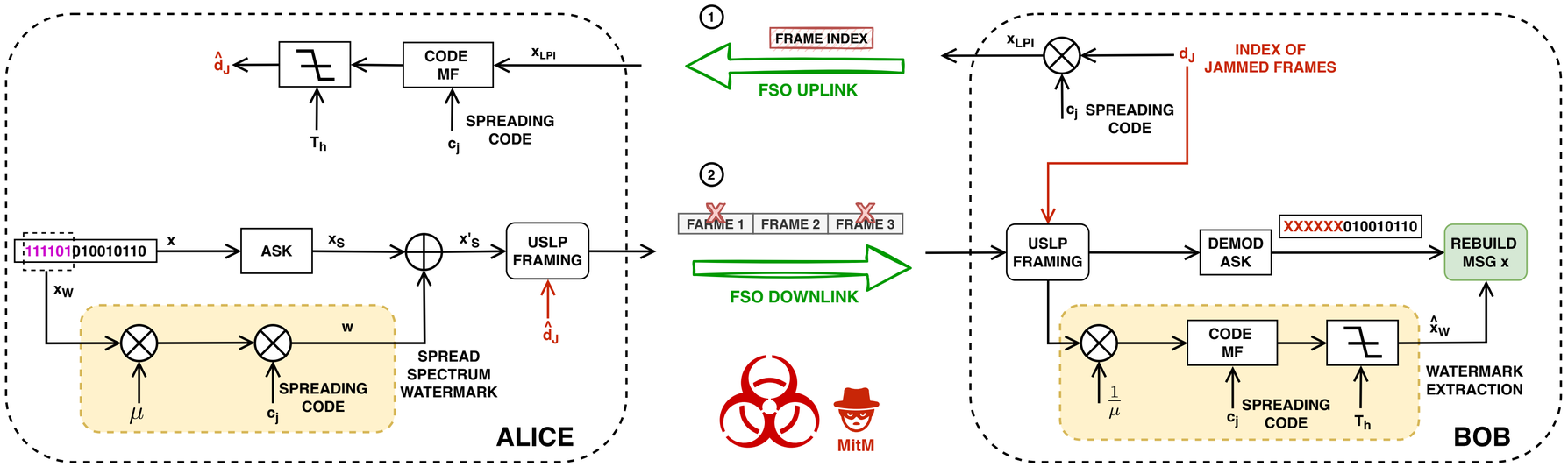
$$(\text{code},\ \text{index}) = \text{PRF}_{K_{\text{seed}}}\Big(\texttt{VCID} \,\|\, \texttt{MCFC}\,[\,\|\,\texttt{DIR}\,\|\,\texttt{GSID}\,]\Big)$$

The DSSS spreading code is derived using **Pseudo-Random Function (PRF) from a short seed Kseed and CCSDS/USLP counters** that ALICE and BOB already observe. **This seed-and-counter derivation avoids distributing long codes on-orbit.**

$$x_{\texttt{LPI}}(i) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_c-1} g(i - kT_b - jT_c)(c_L(i))_j (d(i))_k$$

Covert Communication: The legitimate receiver (BOB) communicates to the legitimate transceiver (ALICE) **the index of USLP (d(i)) must be obfuscated in the downlink.**

Step (1): Covert Communication Channel (2/3)



$$y_A(i) = \begin{cases} n_A(i), & (H_0 : \text{is true}) \\ h_{BA}(i)\, x_{\text{LPI}}(i) + n_A(i), & (H_1 : \text{is true}) \end{cases}$$

$$P_{\text{FA}} = P(\delta = H_1 \mid H_0),$$
$$P_{\text{MD}} = P(\delta = H_0 \mid H_1).$$

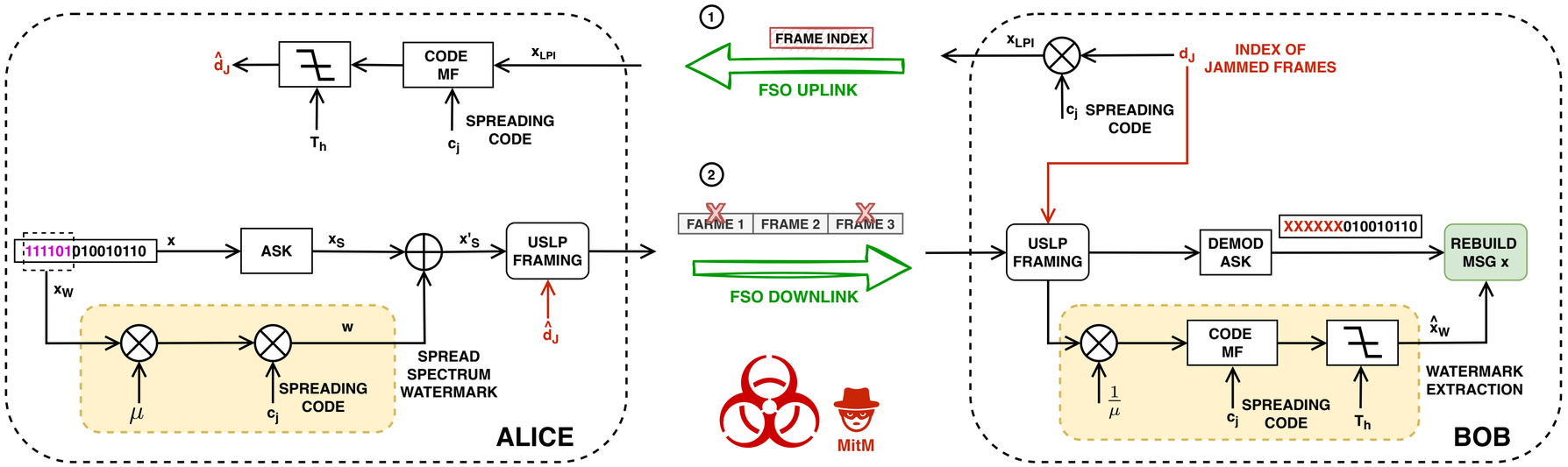
ADVERSARY classifies all observations on Bob's activities using the hypothesis testing :

- **H0:** Bob is silent, so Alice receives only noise $n_A(i)$.
- **H1:** Bob is transmitting $x_{LPI}(i)$, faded by $h_{BA}(i)$ and corrupted by noise $n_A(i)$.

Without any prior knowledge, two probabilities:

- **P_{FA}:** the chance the adversary declares "signal present" when H_0 is true (no signal).
- **P_{MD}:** the chance the adversary fails to detect Bob's signal when H_1 is true.

Step (1): Covert Communication Channel (3/3)



$$\mathcal{O}\sqrt{N}$$

$$p_0 \quad \text{under } H_0,$$
$$p_1 \quad \text{under } H_1.$$

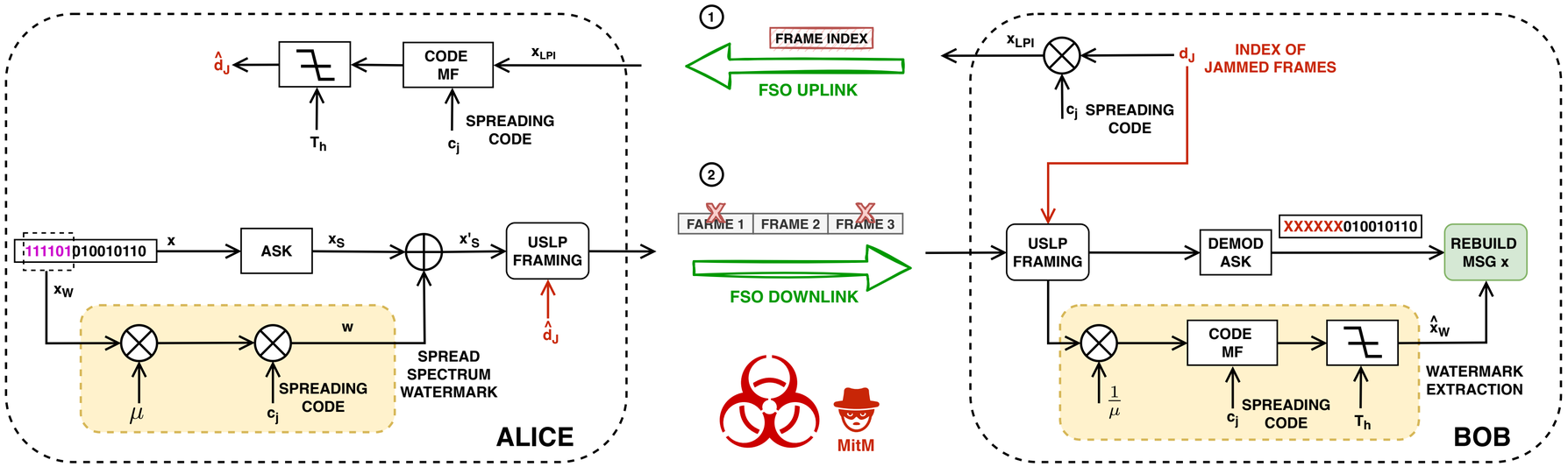
SQUARE ROOT LAW:

Intuition: the AWGN "square-root law" can hold to estimate the number of bits that Bob can exchange with Alice. Using LPI/LPD covert communication Bob can exchange $\sqrt{N}$ informative bits where N is the length of spread spectrum signal.

Probabilities of H_0 and H_1

If the distributions p_1, p_0 remain close enough, an adversary cannot reliably distinguish H_1 from H_0. With careful code design and extremely low power per symbol, this ensures throughput on the order of $\mathcal{O}\sqrt{N}$ bits.

Step (2): Downlink Protection (1/2)



NARROWBAND

SPREAD-SPECTRUM WATERMARKING

$$x'_S(i) = x_S(i) + \mu w(i)$$

$$y_M(i) = h_M(i)x'_S(i) + x_J(i) + n_M(i)$$

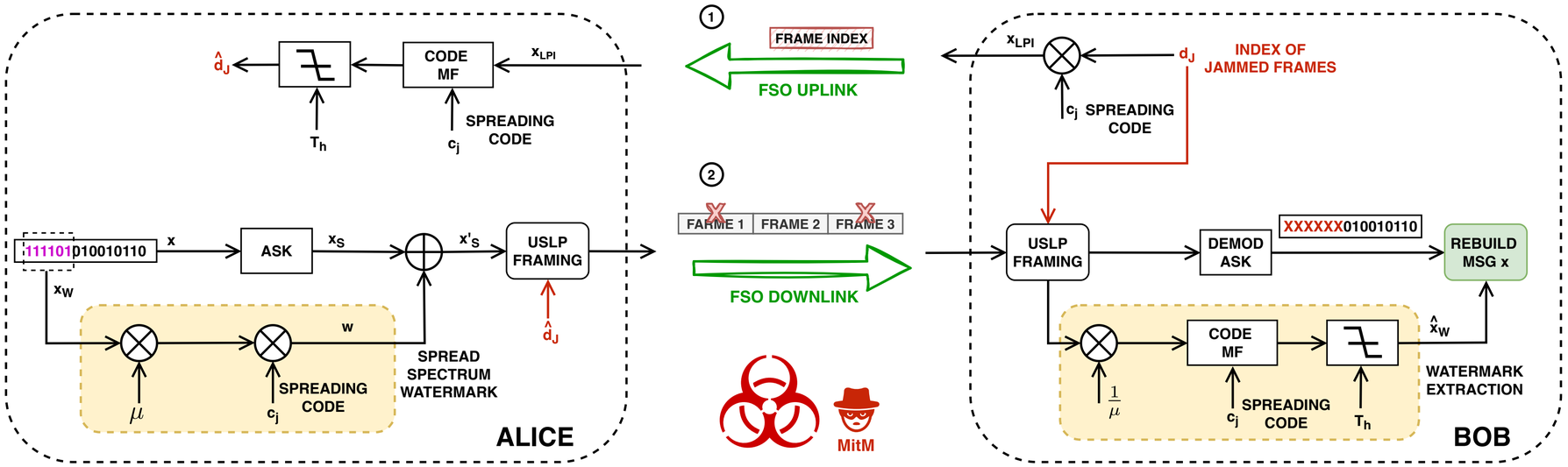
$$y_E(i) = h_E(i)x'_S(i) + x_J(i) + n_E(i)$$

Alice (Tx Satellite) and **Bob** (Rx Ground Station) **wish to exchange a secret message**, denoted by x (exchange the key).

Alice, transmits the watermarked x'_S signal via the FSO downlink main channel, while an eavesdropper (Eve) intercepts the same signal through the wiretap channel.

On the receiver side, **we assume that the frame obfuscation** (i.e., the effect of the cooperative jamming) **can be represented as an interference x_J.**

Step (2): Downlink Protection (2/2)



$$R_s = \max\{C_M - C_E, 0\} = \begin{cases} \log_2 \frac{1+\gamma_M}{1+\gamma_E}, & \text{if } \gamma_M > \gamma_E, \\ 0, & \text{if } \gamma_M \leq \gamma_E, \end{cases}$$

SECRECY RATE METRIC

$$\gamma_M = \frac{|h_M|^2 P_t^2}{\sigma_M^2 + \cancel{P_j^2}^{\,0}}$$

$$\gamma_E = \frac{|h_E|^2 P_t^2}{\sigma_E^2 + P_j^2}$$

Numerical Simulations

TABLE I: Simulation parameters.

Parameter	Value
$P_{\mathtt{tx}}$	17.5 dBm
$P_{\mathtt{req}}$	-35.5 dBm [1]
Wavelength	1550 nm
Satellite heigh	550 km [2]
Satellite distance	1000 km [3]
Spreading Code length (N)	$16, 32, 64, 128, 256$
Key length (K)	4096 bits
Bits for the Watermark (N_W)	$(8, 16, 32, 64, 128)$ bits
USLP Frame length	64 bits
Obfuscated frames (O_f)	up to 2 frames [4]
Watermark power ratio (ξ)	$0.1 \div 0.9$

[1] on-off keying modulation 10^{-12} BER.
[2] Uplink and downlink scenarios.
[3] ISL scenario.
[4] At most I can obfuscate the same number of bits that I use for watermarking.

OBJECTIVES

Verify through **Monte Carlo simulations** the **performance of covert communication** using LPD/LPD signals

Evaluate the secrecy rate we can achieve using cooperative jamming on USLP and SS watermarking

LINK MARGIN

The link margin quantifies, in decibels, **how much the received power exceeds the receiver sensitivity determined by the target BER** and modulation:

$$\Gamma_{\mathrm{dB}} = P_{\mathrm{rx,dBm}} - P_{\mathrm{req,dBm}}$$

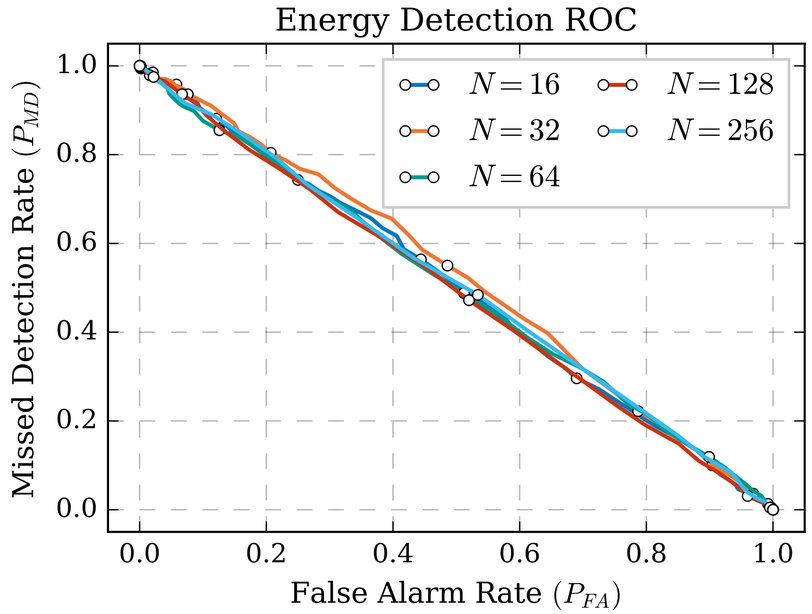
- $\Gamma = 0$: at sensitivity—just meets target BER
- $\Gamma > 0$: surplus margin—higher reliability
- $\Gamma < 0$: below threshold—BER degradation.

Γ summarizes system gains, losses, and impairments into a single metric.

Results: Receiver Operating Characteristic (ROC)

We assume the **adversary (Eve) does not know the precise spreading code used by Bob** to send his low-power DSSS signal.

This scenario reflects a more challenging detection environment for the adversary.



$$T_{\text{energy}} = \left| \frac{1}{N} \sum_{i=1}^{N} |y_A(i)|^2 \right|$$

The **diagonal** joining (PFA,PMD) = (1,0) and (0,1) **represents purely random guessing.**

The figure shows that, under both non-coherent strategies routinely assumed in the literature, the **eavesdropper's best achievable operating point lies arbitrarily close to random guessing**, validating the undetectability of the proposed covert side channel.

$$P_{\text{MD}} = 1 - \frac{\sum_{i=1}^{M_c} \mathcal{H}(\bar{T}_i)}{M_c}, \text{ if } H_1 \text{ is true}$$

H_1: *Bob is transmitting*

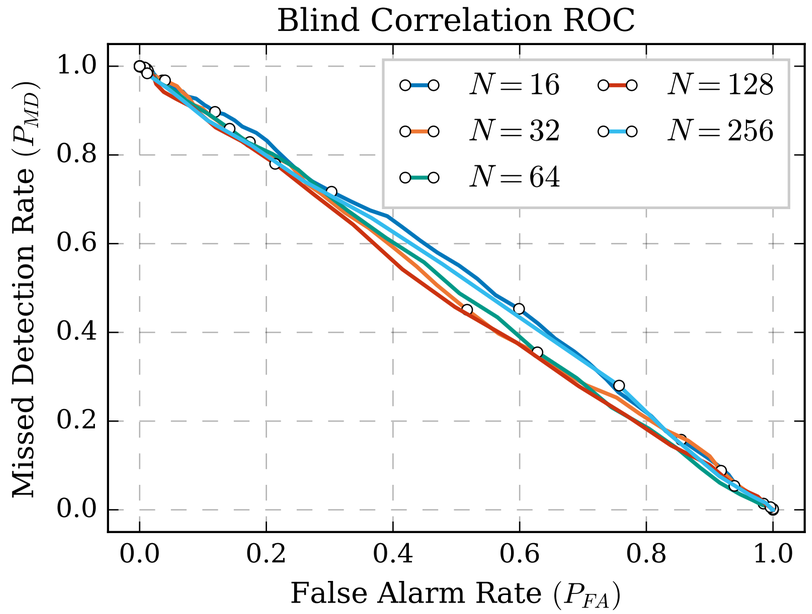
$$P_{\text{FA}} = \frac{\sum_{i=1}^{M_c} \mathcal{H}(\bar{T}_i)}{M_c}, \text{ if } H_0 \text{ is true}$$

H_0: *Bob is silent*

Results: Receiver Operating Characteristic (ROC)

We assume the **adversary (Eve) does not know the precise spreading code used by Bob** to send his low-power DSSS signal.

This scenario reflects a more challenging detection environment for the adversary.



$$T_{\text{corr}} = \left| \frac{1}{N} \sum_{i=1}^{N} y_A(i)\, \text{PN}_{\text{test}}(i) \right|$$

The **diagonal** joining (PFA,PMD) = (1,0) and (0,1) **represents purely random guessing.**

The figure shows that, under both non-coherent strategies routinely assumed in the literature, the **eavesdropper's best achievable operating point lies arbitrarily close to random guessing**, validating the undetectability of the proposed covert side channel.

$$P_{\text{MD}} = 1 - \frac{\sum_{i=1}^{M_c} \mathcal{H}(\bar{T}_i)}{M_c}, \text{ if } H_1 \text{ is true}$$

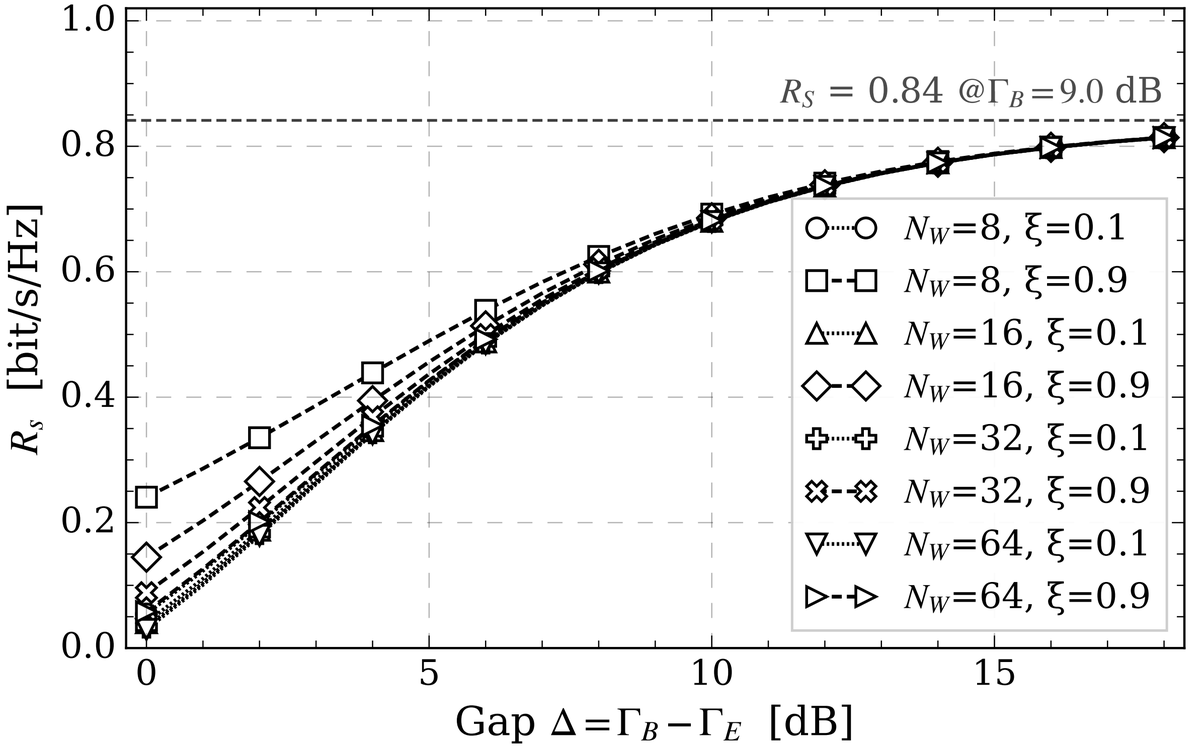
H_1: *Bob is transmitting*

$$P_{\text{FA}} = \frac{\sum_{i=1}^{M_c} \mathcal{H}(\bar{T}_i)}{M_c}, \text{ if } H_0 \text{ is true}$$

H_0: *Bob is silent*

Results: Secrecy Rate

Secrecy rate Rs versus gap $\Delta = \Gamma_B - \Gamma_E$ at fixed Γ_B (OOK downlink)



$O_f = 2$ *consistent with the USLP constraint that* ***the number of obfuscated bits does not exceed those protected by the DSSS watermark.***

In-band watermark noise: The DSSS watermark is embedded in-band with power ratio ξ and spreading code **N**

$$\gamma_E^{(\mathrm{wm})} = \frac{\gamma_E^{(0)}}{1 + \xi_{\mathrm{eff}} \gamma_E^{(0)}}, \qquad \xi_{\mathrm{eff}} = \frac{\xi}{N} \qquad \xi \triangleq \frac{P_{\mathrm{wm}}}{P_t}$$

Bob knows the watermark and the obfuscation index and cancels them

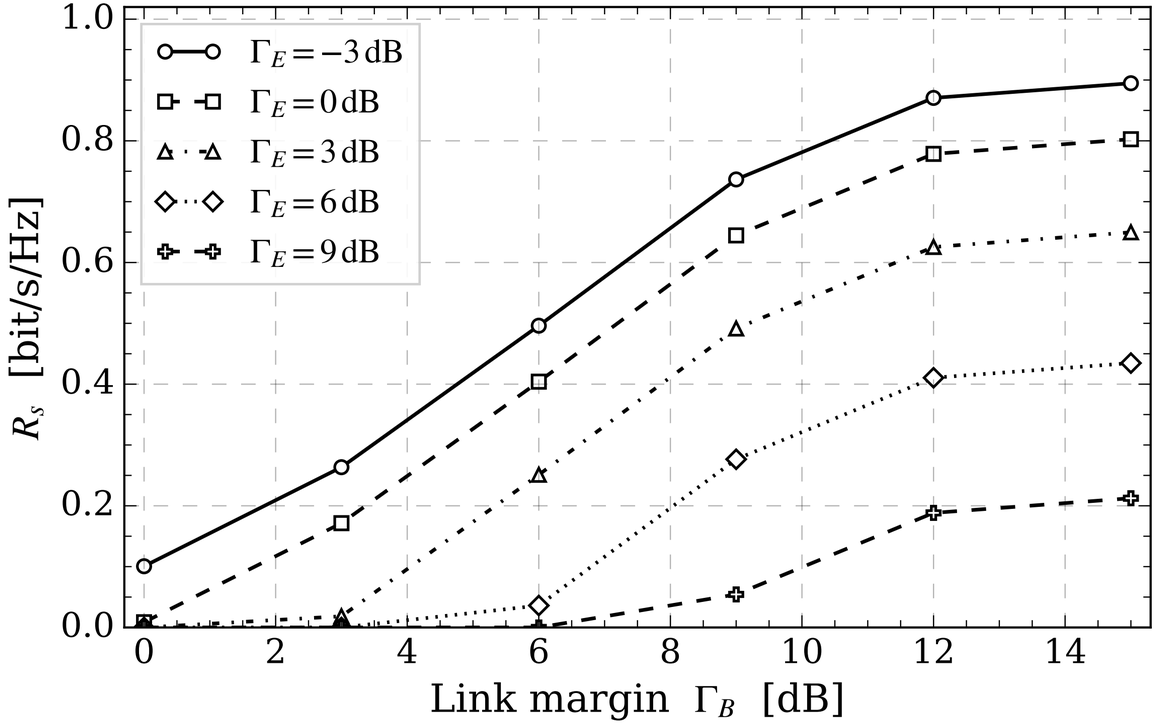
Cooperative obfuscation: Obfuscation replaces payload bits on selected frames, its effect appears at the bundle level via the erasure fraction $q = O_f/64$.

$$R_s = \left[C_M - (1 - q)\, C_E \right]^+$$

- Rs grows monotonically, asymptotically approaching the ceiling C_M set by Bob's margin.
- Stronger watermarking (ξ = 0.9) shifts the curves upward.

Results: Secrecy Rate

Secrecy rate Rs versus Γ_B (OOK downlink)



$O_f = 2$ *consistent with the USLP constraint that* ***the number of obfuscated bits does not exceed those protected by the DSSS watermark.***

$N_W = 16$

Effect of varying the attacker's Chanel.

Smaller Γ_E yield **higher R_s**.

Conclusions

This paper introduces a **novel physical and data link layer security approach that combines cooperative jamming with spread-spectrum watermarking**, specifically designed to enhance SATCOM confidentiality and enable secure key distribution in LEO-based constellations and upcoming 6G NTN systems.

ROC analyses for both energy-based detection and blind-correlation **attacks** showed that their **detection capability remains essentially indistinguishable** from random guessing even when the adversary tests multiple random spreading codes.

Simulations confirm the **secrecy rate improves with a better main channel and reaches good values** (e.g., 0.64 to 0.78 bit/s/Hz) under typical satellite margins, showing the method offers substantial secrecy gains without changing protocol or modulation.

Securing Satellite Key Distribution via Covert Channels: A Cooperative Jamming and Watermarking Approach

SECURITY FOR SPACE SYSTEMS (3S) 2025
NOV 04-06, 2025 - ESTEC in Noordwijk, The Netherlands

S. Soderi[*†‡], E. Casini[§], M. Conti[†‡]

[*]*IMT School for Advanced Studies, Lucca, Italy*

[†]*Cybersecurity National Laboratory, CINI - Roma, Italy*

[§]*ESA, European Space and Technology Center, ESTEC, Noordwjik, The Netherlands*

[‡]*University of Padova, Italy*

simone.soderi@imtlucca.it

Thanks for your attention!

WBPLSec in RF Channel