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

Simone Soderi*†‡ *Senior Member, IEEE,* Enirco Casini§, Mauro Conti†‖‡ *Fellow, IEEE,*
*IMT School for Advanced Studies Lucca, Lucca, Italy,
‡Cybersecurity National Laboratory, CINI - Roma, Italy
simone.soderi@imtlucca.it
§European Space Agency, European Space and Technology Center, ESTEC, Noordwjik, The Netherlands
enrico.casini@esa.int
† University of Padua, Department of Mathematics, Padua, Italy
‖ Örebro University, AI, Robotics and Cybersecurity Center (ARC), Sweden
conti@math.unipd.it

***Abstract*—As Non-Terrestrial Networks (NTNs) move toward integration with 6G infrastructures, Low Earth Orbit (LEO) satellite constellations become central to delivering ubiquitous global connectivity. Recent cyberattacks targeting space systems and the rapid expansion of LEO satellite technology have heightened the need to address emerging vulnerabilities and design robust countermeasures. To this end, we propose a novel data link–layer security scheme combining cooperative jamming with watermark-based covert signaling, specifically developed to facilitate secure key distribution in satellite communications. Our approach leverages a Low Probability of Intercept (LPI) covert channel to securely communicate frame indices designated for intentional obfuscation through friendly jamming. Concurrently, a spread-spectrum watermark embedded within the payload enables authorized receivers to efficiently recover jammed bits without the overhead of frequent cryptographic rekeying. The proposed solution integrates seamlessly into existing CCSDS-compliant satellite protocols, ensuring backward compatibility and minimal hardware disruption. Numerical simulations, including detailed Free Space Optical (FSO) link budget analyses, demonstrate robust secrecy performance, significantly mitigating risks of eavesdropping and man-in-the-middle attacks. Utilizing a shared spreading code, this watermarked cooperative-jamming approach provides a secure, agile, and resource-efficient method suitable for future satellite networks.**

***Index Terms*—satellite communication, security, watermarking, ISL, FSO.**

I. Introduction

As the global community moves toward 6G networks, satellite communication systems are set to become a pivot of the emerging Non-Terrestrial Networks (NTNs). By interconnecting Geostationary (GEO), Medium Earth Orbit (MEO), and Low Earth Orbit (LEO) satellites with terrestrial infrastructure, NTNs will ensure near-ubiquitous connectivity—even in remote regions—while delivering high-speed, low-latency links for telecommunications, IoT, and beyond.

LEO satellite constellations, in particular, are revolutionizing connectivity by enabling high-speed Internet, navigation, and remote sensing [1]. With the advent of commercial networks, e.g., SpaceX's Starlink or OneWeb, space access barriers have diminished, yet the security posture of such systems has not always kept pace [2], [3]. In particular, while many standardized frameworks and waveforms are widely employed in LEO networks, adversaries can exploit vulnerabilities in onboard firmware, ground software stacks, or the data link layer. Recent events, such as the close approach of Russia's Luch-5Kh satellite to the U.S. Intelsat-39 [4], have further underscored the risk of malicious activities when external satellites can maneuver into proximity and attempt physical-layer intrusion or espionage.

Real incidents highlight the gravity of these threats. A notable example is the 2022 KA-SAT disruption [5], which stemmed from a ground-segment intrusion that disabled large numbers of consumer terminals (i.e., not an RF-layer over-the-air attack). For RF-layer threats specifically (uplink jamming, spoofing, signal hijacking), the academic literature documents practical attack vectors [6], [7]; our work targets precisely this RF/optical over-the-air surface with a watermark-assisted, receiver-undoable obfuscation mechanism. If essential protective features are absent, adversaries might intercept unprotected downlink signals over large Radio-Frequency (RF) footprints or attempt to breach optical links in more targeted FSO scenarios. Even partial compromises of software-defined networking components can expose critical data or yield control over satellite operations. Another pressing issue is spoofing attacks, where adversaries forge SATCOM signals to impersonate ground stations or satellites. By injecting falsified telemetry data or unauthorized commands, attackers can manipulate satellite operations, compromise network integrity, and disrupt legitimate communication flows [8]. This attack poses serious risks to mission-critical applications and requires enhanced authentication mechanisms to ensure secure transmission.

This paper proposes a novel data link–layer strategy that harnesses both *cooperative jamming* and *signal watermarking* to enhance confidentiality and facilitate *secure key distribution* in modern LEO networks (see Figure 1). We seamlessly embed

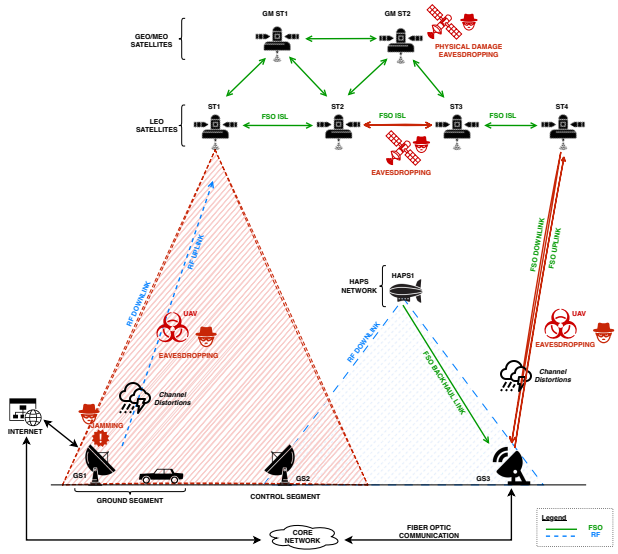


Fig. 1: RF and FSO NTN architecture and potential attacks on wireless links.

these techniques into existing link-layer frames—avoiding major hardware changes or protocol overhauls—so legitimate users can differentiate intended signals from adversarial interference. Rather than replacing traditional encryption, our cooperative jamming and watermarking framework augments it at a lower stack level, adding an adaptive, software-driven layer of security in resource-constrained satellite environments.

In contrast to standard cryptographic solutions alone, the proposed data link enhancements tackle vulnerabilities that arise when encryption keys or upper-layer methods can be bypassed or jammed. Our solution aims to integrate with software-defined modems found in many LEO constellations, proposing a more robust, proactive defense. SATCOM employs both RF and Free Space Optics (FSO) channels. At the same time, FSO beams can offer narrower coverage than RF, and a lack of strong security mechanisms can still leave systems open to adversaries. Ultimately, our adaptive, software-based mechanism impedes eavesdropping and spoofing threats under a wide range of LEO operating conditions and supports broader 6G NTN objectives by safeguarding critical satellite links.

Motivation. Strong encryption protects data but requires frequent key exchanges due to fast-moving satellites, introducing computational overhead and key management complexity [9]. While effective in mitigating certain threats, physical-layer security often demands specialized antennas, power-intensive processing, or proprietary hardware modifications, making it impractical for cost-effective satellite networks [8]. By *Physical Layer Security (PLS)* we mean mechanisms that leverage the waveform/channel/receiver processing to reduce detectability or information leakage independently of cryptographic secrecy (e.g., Low Probability Interception (LPI)/Low Probability Detection (LPD) signaling, interference shaping, artificial noise). Our approach is complementary to conventional cryptography, not a replacement: encryption and authentication remain feasible and widely deployed; however, operational realities (on-orbit rekeying cadence, compromised terminals, detectability constraints, or contested spectrum) motivate an additional, waveform-level layer that degrades the eavesdropper even when ciphertext is present or keys are static. The proposed watermark-assisted cooperative obfuscation adds such a layer while preserving USLP interoperability.

We propose a two-level approach to address these limitations: cooperative jamming at the data link layer and watermarking for information reconstruction. Our proposal aims to minimize modifications of existing satellite systems, making them attractive for a quicker and less risky implementation. This paper integrates LPI and LPD communications mechanisms to exchange information in a way that is difficult to attack by jamming the content of Unified Space Link Protocol (USLP) frames. We deliberately mark and obfuscate a subset of USLP frames; Bob knows the index and cancels/repairs them, whereas Eve sees effective erasures on those frames and watermark-induced interference on the rest. On the other hand, watermarking incorporates lightweight authentication markers into communication frames, enabling rapid detection of forged or tampered signals. By integrating these techniques, our approach increases resilience against jamming and spoofing without requiring hardware changes, making it suitable for large-scale satellite networks.

Contribution. To the best of our knowledge, this is the first SATCOM study that combines *cooperatively scheduled, receiver-undoable* jamming with *in-band physical-layer watermarking* to counter Man-in-the-Middle (MitM)-class interception while remaining compatible with CCSDS/USLP framing. In particular, our proposal:

- *Focuses on Secure Key Exchange:* Rather than relying on advanced encryption suites with frequent keying, we protect the SATCOM's key distribution phase through a low-overhead combination of jamming and watermarking. This approach avoids the constant need to create or refresh complex cryptographic keys.
- *Minimizes Transmission Alterations:* We embed watermark signals at the data link layer without visibly altering the main waveform from an adversary's perspective. As a result, a passive observer examining the spectrum observes no noticeable change, rendering it extremely difficult to identify which portions of the signal are obfuscated.
- *Employs Cooperative Jamming Strategically:* The legitimate transmitter and receiver collaborate to selectively mask parts of the downlink. Because the receiver knows which bits are jammed, it can easily reconstruct the original data, while any unauthorized party is effectively locked out.
- *Avoids Major Hardware or Protocol Modifications:* By inserting the watermark and jamming indicators into standard CCSDS frames, we remain backward compatible with existing RF or FSO platforms, requiring no extensive changes to the underlying communication hardware.

Overall, the proposed framework offers an agile and resource-friendly layer of security for satellite networks, particularly suited for high-demand scenarios where cryptographic overhead might otherwise be impractical. By mixing cooperative jamming with cleverly placed watermarks, we ensure a robust method to protect critical key exchanges from MitM threats while keeping the overall communications architecture largely intact.

Organization. The rest of the paper is organized as follows. The rest of the paper is structured as follows. Section II surveys existing satellite security solutions and how they relate to cooperative jamming. Section III briefly recalls the concepts useful for understanding the paper. Section IV outlines our system assumptions, including the USLP-based data link. Section V describes the watermarked cooperative jamming algorithm for secure key distribution. Section VII provides numerical results that support this research. In Section VIII, we discuss how to apply the method to the case of RF-based SATCOMs and possible limitations. Finally, Section IX concludes the paper by discussing our findings.

II. Related Works

Modern SATCOM networks, particularly LEO constellations and inter-satellite links, face an array of sophisticated threats, including jamming, spoofing, and infiltration of onboard software [5], [2]. On the uplink side, adversaries may seize command channels or deploy Software-Defined Radios (SDRs) to transmit falsified telemetry and manipulate satellite operations [10], [11]. Conversely, downlinks remain susceptible to eavesdropping over broad footprints or targeted, high-power jamming attacks [12], [1]. Although FSO crosslinks can have narrower beams and lower intercept probability, beam misalignment, and firmware-level impersonations are still feasible [13], [14]. Moreover, many small-satellite designs incorporate Commercial Off-The-Shelf (COTS) hardware and open-source software, expanding the risk of supply-chain or insider intrusions [3].

China's growing readiness to challenge U.S. space dominance further elevates the urgency for enhanced SATCOM security. In recent years, Beijing has engaged in record satellite launches and demonstrated advanced technologies, from grappling arms to orbital debris-removal systems, that could be repurposed for sabotage or for maneuvering near other spacecraft [15]. Such proximity would allow an adversary to intercept free-space optical transmissions, underscoring the high importance of communications defense. Conventional cryptographic solutions alone may not suffice, as side-channel or jamming-based assaults can bypass cryptographic layers if key management is weak or the data link itself is underprotected [16].

Several mitigation techniques have thus emerged in the literature. Early efforts centered on spoofing detection, anti-jamming strategies, and signal authentication [5]. For example, Giuliari *et al.* document how low-cost denial-of-service exploits undermine LEO network performance [12]. Other studies focus on the vulnerabilities introduced by SDR-based interception or manipulation [2]. Cryptographic authentication methods, such as AES variants or post-quantum cryptography, offer strong protection but introduce extensive computational overhead and complicated key management [9]. Physical-layer security mechanisms, for instance, spread spectrum or frequency hopping, help combat jamming yet often impose bandwidth inefficiencies [17]. Meanwhile, *signal watermarking* embeds unique signatures in transmissions to detect spoofing [8], and friendly jamming can mask legitimate signals from eavesdroppers, albeit requiring fine synchronization to avert unintended performance degradations [17]. Other approaches leverage adversarial learning for real-time anomaly detection, though these systems need continuous training against evolving threat models [18].

A fundamentally different method is Quantum Key Distribution (QKD), which employs FSO or fiber-based quantum channels for key sharing [19], [20]. Despite its theoretical promise, QKD faces formidable challenges, particularly in LEO networks, due to atmospheric attenuation, stringent beam pointing requirements, and device miniaturization constraints that hinder widespread deployment [21]. Consequently, purely cryptographic or purely quantum-based schemes alone may not fully address security gaps in modern satellite architectures.

Our work builds on these lines of inquiry by integrating data-link *cooperative jamming* and *watermarking* into an overarching SATCOM security framework. Instead of relying exclusively on computational cryptography, we embed lightweight obfuscation and markers within standard frames, enabling rapid detection and response to malicious activities without substantial hardware modifications. This solution complements encryption-based defenses and offers an agile mechanism to protect key distribution and data integrity in LEO-based satellite communications.

RF emitter-fingerprinting and hardware-based device identification provide orthogonal defenses that require no explicit watermark and have seen growing attention in the satellite domain. Our focus here is on optical/RF waveform-level obfuscation and LPI/LPD coordination; integrating watermark-based secrecy with emitter fingerprinting is a promising avenue for future work.

III. Background

This section outlines the key concepts necessary to understand our proposal. It mainly introduces physical layer techniques, data link protocols, and jamming techniques.

Physical Layer Security. Transmission Security (TRANSEC) ensures hostile entities cannot readily detect, intercept, or exploit communication signals. Within satellite networks, TRANSEC techniques have LPI and LPD characteristics as they distribute the signal over a wider bandwidth, lowering the overall power spectral density and complicating any interception attempts. Spread spectrum waveforms, in particular, have long been the basis for achieving LPI/LPD in critical or military communications [22]. Examples include Cyclic Code Shift Keying (CCSK) [23] and rapid Sidelobe Time

Modulation (SLTM) [24]. By boosting the processing gain and often resorting to higher frequency bands, these approaches can significantly reduce the chances of signal detection and interception [25]. Spatial diversity at the transmitter side can add further resilience [26], while careful modulation and power control balance anti-jamming strength by minimizing a detectable signature [27]. In addition, antenna patterns with low sidelobes are often incorporated, helping to limit signal leakage to unintended directions and thereby strengthening LPD capabilities [28].

Space Data Link Protocol. Although LPD/LPI concepts ensure hidden or hard-to-detect transmissions, the underlying link-layer framing and security mechanisms are equally important elements of TRANSEC in modern satellite networks. The Unified Space Data Link Protocol (USLP) [29], proposed by the Consultative Committee for Space Data Systems (CCSDS), offers a flexible frame format for data transfer and supports additional fields that allow for the selective integration of security features. A typical USLP transfer frame begins with a primary header containing the protocol version, frame length specifications, and flags for bypass or sequence control. The heart of the frame is the Transfer Frame Data Field (TFDF), which may incorporate higher-layer services (such as different packet services) or optional headers for multiplexing. Designers can also include security-related fields before the payload data or append them within the TFDF to accommodate encryption, authentication tags, or other protection schemes that do not necessitate hardware modifications. USLP aims to unify spatial data link protocols under one general structure, making it a good candidate for the architecture presented in this paper.

Jamming. Although spread spectrum methods ensure a lower probability of signal detection, adversaries may still attempt to capture signals if they isolate and process faint transmissions. To prevent such interception, *cooperative jamming* introduces a purposeful injection of structured interference by legitimate satellite nodes. Unlike adversarial jamming, which disrupts reliable communications, cooperative jamming [30] is carefully coordinated so legitimate receivers, holding the appropriate synchronization or decoding references, can effectively remove or subtract the injected signals from the desired transmission. An eavesdropper, lacking these references, cannot filter out the jamming component and thus fails to reconstruct the original data.

The combination of spread spectrum signaling and cooperative jamming proves especially beneficial when integrated at the data link layer through optional watermarking within USLP frames. The watermarking further helps authenticate legitimate frames while the jamming reduces the clarity of intercepted signals, increasing the difficulty of any unauthorized analysis. This layered yet integrated approach — consisting of physical layer engineering, link-layer framing, and active interference management — provides a robust, flexible countermeasure against passive eavesdropping and more aggressive attacks, thereby strengthening the overall security of the satellite communication link.

IV. System Model

This section presents the reference architecture and link budget analysis for an FSO satellite communication system covering ISLs and uplink/downlink paths to ground stations. Although our subsequent threat mitigation primarily targets the downlink, the same formalism—amended to account for atmospheric differences—can be adapted to uplinks or ISLs. We propose minimal modifications to existing constellations by leveraging widely adopted Optical On-Off Keying (O3K), intensity modulation/direct detection (IM/DD) at the physical layer, and standardized data-link framing via the USLP. This combination harnesses FSO's high directionality and LPI/LPD features while preserving backward compatibility with widely deployed CCSDS-based satellites.

A. Optical Link Budget Analysis

In an Inter Satellite Link (ISL) scenario, the laser beam propagates through near-vacuum conditions, so atmospheric losses are typically negligible. The received power, $P_{\mathtt{rx}}^{\mathtt{ISL}}$ in dBm, may be written as

$$\begin{aligned} P_{\mathtt{rx}}^{\mathtt{ISL}} =& P_{\mathtt{tx}} + OE_{\mathtt{tx}} + OE_{\mathtt{rx}} + G_{\mathtt{tx}} + G_{\mathtt{rx}} + \\ & - LP_{\mathtt{tx}} - LP_{\mathtt{rx}} - L_{\mathtt{PS}}, \end{aligned} \tag{1}$$

where $P_{\mathtt{tx}}$ is the transmit power in dBm, $OE_{\mathtt{tx}}$ and $OE_{\mathtt{rx}}$ represent optical efficiencies, $G_{\mathtt{tx}}$ and $G_{\mathtt{rx}}$ capture transmitter/receiver antenna gains in dB, and $LP_{\mathtt{tx}}$ and $LP_{\mathtt{rx}}$ are pointing losses (in dB) due to misalignment. The term $L_{\mathtt{PS}}$ denotes the free-space path loss associated with the satellites' separation and the carrier wavelength [31]. Since there is no atmospheric channel, pointing loss is often the most critical parameter in ensuring sufficient received signal power.

In the case of uplink and downlink, the link budget includes atmospheric absorption and scattering for optical transmissions traversing the Earth's atmosphere. The received power in dBm, denoted by $P_{\mathtt{rx}}^{\mathtt{UDL}}$, is:

$$\begin{aligned} P_{\mathtt{rx}}^{\mathtt{UDL}} =& P_{\mathtt{tx}} + OE_{\mathtt{tx}} + OE_{\mathtt{rx}} + G_{\mathtt{tx}} + G_{\mathtt{rx}} + \\ & - LP_{\mathtt{tx}} - LP_{\mathtt{rx}} - L_{\mathtt{PG}} - L_{\mathtt{abs}} - L_{\mathtt{sca}}. \end{aligned} \tag{2}$$

Here, $L_{\mathtt{PG}}$ is the free-space path loss from ground station to satellite, commonly computed as $20\log_{10}\big(\lambda/(4\pi\, d_{GS})\big)$ [31], where λ is the wavelength and $d_{\mathtt{GS}}$ is the ground-to-space distance. Absorption losses ($L_{\mathtt{abs}}$) typically remain small at infrared bands around 1550 nm [32], while scattering losses ($L_{\mathtt{sca}}$) arise from aerosols, fog, and other particles in the troposphere [33]. Depending on local meteorological conditions, these phenomena can significantly degrade the link margin, so operators often include fade margins and adaptive coding or power control to maintain reliable connectivity. Pointing errors remain relevant because even a small misalignment can result in large geometric losses.

Equations (1) and (2) highlight the principal factors shaping optical link budgets in satellite communications. For ISLs, pointing losses dominate while atmospheric attenuation is negligible, whereas uplink/downlink paths through the troposphere demand careful modeling of absorption and scattering.

In practice, mission teams select transmit power, antenna sizes, and error-correction schemes based on these loss terms and the desired quality of service under dynamic conditions, such as cloud cover, precipitation, or orbital geometry.

B. USLP Framing with an O3K Physical Layer

This work employs USLP frames over an optical O3K scheme under IM/DD. USLP provides a flexible transfer frame, beginning with a *Primary Header* that includes a Transfer Frame Version Number, a 16-bit Spacecraft Identifier (SCID), flags for source/destination and multiplexing, and up to 65 536 octets of frame length. These fields allow multiple data channels (virtual channels) and sub-channels (MAP IDs) to share the same physical link without requiring separate hardware paths.

If Space Data Link Security (SDLS) is enabled, a *Security Header* may follow to embed cryptographic parameters. The main Transfer Frame Data Field (TFDF) then carries user data up to 65 529 octets, optionally segmented or limited to a shorter length for space mission requirements. A short Operational Control Field (OCF) can be added for command link control or security reporting, and an optional Frame Error Control Field (FECF) may conclude the frame to detect residual errors.

In our proposal, the new security-related data reside within the USLP Transfer Frame's payload region, i.e., the TFDF. Rather than altering fundamental header fields or requiring non-standard subheaders, we embed any additional information—such as watermarking codes, collaborative jamming markers, or authentication tokens—directly in the payload area. This approach preserves interoperability with existing USLP and CCSDS-based infrastructure since end systems can continue parsing frames according to the standard primary header and data field headers without changes to the surrounding protocol logic. Embedding data in the USLP payload thus provides a minimally invasive method to introduce advanced security measures while retaining full compatibility across diverse mission profiles.

Implementation considerations and interoperability. On the space segment, our design is implementable as a lightweight baseband add-on in FPGA/DSP cores. Where software-defined radios or reconfigurable modems are available, the watermark embed/extract and frame-indexing blocks can be deployed via firmware updates. No changes to optics, pointing, or front-end linearity are required; power draw is negligible compared with the laser transmitter. On the ground segment, the receiver performs successive-interference cancellation using the shared code and erasure index. Because the scheme keeps the USLP framing intact and overlays the watermark in-band at the physical layer, it preserves interoperability with CCSDS USLP and O3K mappings and is compatible with incremental on-orbit updates where firmware reconfiguration is feasible.

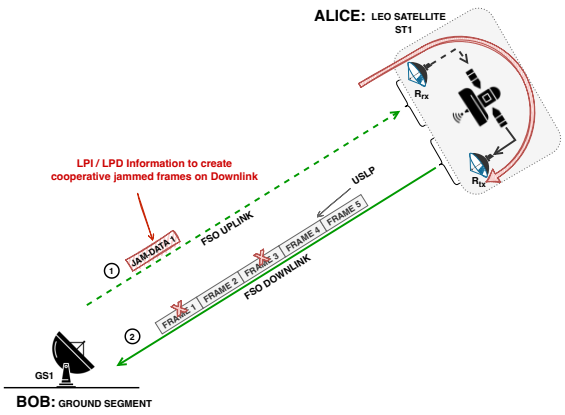


Fig. 2: SATCOMs downlink defense proposal with data link-based cooperative jamming. Step (1) LPI/LPD message contains the information to build the cooperative jamming; step (2) downlink with USLP frames obfuscated.

V. Secure Key Distribution through a Watermarked Cooperative Jamming Algorithm

We propose a receiver-assisted defense that fuses a covert LPI/LPD exchange with data-link obfuscation. In step (1) (Figures 2 and 3), a Direct Sequence Spread Spectrum (DSSS) watermark acts as a covert control channel that conveys the obfuscation index. In step (2), the downlink payload is transmitted with the watermark *in-band* and a subset of USLP frames is deliberately obfuscated (cooperative jamming). Bob shares the spreading code and index, cancels the watermark, and discards/restores the marked frames; Eve lacks both and thus faces watermark-induced interference on clean frames and effective erasures on the obfuscated ones. This differs from WBPLSec [34] by making the interference *cooperatively scheduled* and *undoable* at the legitimate receiver while remaining protocol-compatible with USLP.

The watermark spreading code and the frame–obfuscation index are derived *implicitly* using a Pseudo-Random Function (PRF) from a short seed K_{seed} and CCSDS/USLP counters that both ends already observe. For example, we can assume,

$$(\text{code, index}) = \text{PRF}_{K_{\text{seed}}}\Big(\texttt{VCID} \,\|\, \texttt{MCFC}\,[\,\|\,\texttt{DIR} \,\|\, \texttt{GSID}\,]\Big), \tag{3}$$

where VCID is the Virtual Channel ID and MCFC the (Master) Channel Frame Count; optional fields (direction, ground-station/beam ID) avoid collisions across segments. No explicit bundle identifier is transmitted on the air. This seed-and-counter derivation avoids distributing long codes on-orbit, enables lightweight rotation (per beam/region or per mission phase), and keeps USLP/O3K framing unchanged.

Without loss of generality, in this section, we utilize the downlink use case, but we could apply the same to uplink and ISL communications. Our scheme defends downlink transmissions in two main stages, as illustrated in Figure 2. Algorithm 1 leverages signal-processing techniques under the assumption that both the transmitter and receiver share a standard spread-

ing code (for instance, a Hadamard sequence [22]). One way to establish this code is to use a pre-arranged mathematical function so each party can derive the same sequence from minimal parameters, thus avoiding frequent key exchanges typical of standard encryption. Once this spreading code is in place, the legitimate parties generate an LPI signal and a spread-spectrum watermark to obfuscate sensitive data. An eavesdropper lacking knowledge of the spreading code cannot remove the friendly jamming or detect the watermark. Meanwhile, the receiver can selectively strip out the interference to reconstruct crucial downlink portions, achieving robust protection without burdensome key distribution overhead.

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

A. Step (1): Covert Communications Channel

Consider a covert link from Bob to Alice across an optical medium subject to Mie-scattering fading.

Using the PRF in (3), the bundle identifier is *implicit*; hence, the on-air overhead reduces to a very short, low-power *covert DSSS header*

$$m = \big\langle \text{Index},\ \text{AuthTag} \big\rangle. \tag{4}$$

For example, for $O_f = 2$ obfuscated frames out of 64, the index requires only $\lceil \log_2 \binom{64}{2} \rceil = 11$ bits (or fewer if the admissible pair set is restricted). An authentication tag (e.g., 16 b) binds the index to the current counters to prevent replay/desynchronization. The header is spread with length N at low duty cycle; *Alice* despreads, verifies the tag, and schedules the indicated frames for obfuscation in the upcoming 4 096-bit bundle. No USLP fields are modified—the header rides entirely at the physical layer alongside the O3K mapping. (In Step (2), *Bob* cancels the watermark and discards/repairs the marked frames on reception.)

At the i-th time instant, Bob may send a (low-power) symbol $x_{\text{LPI}}(i)$ such as a DSSS signal that can be expressed as

$$x_{\text{LPI}}(i) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_c-1} g(i - kT_b - jT_c)(c_L(i))_j (d(i))_k, \tag{5}$$

where $(d(i))_k$ is the *k*-th data bit of the signal that contains the index of jamming information, $(c_L(i))_j$ represents the *j*-th chip of the orthogonal pseudo-noise (PN) sequence, $g(i)$ is the pulse waveform, T_c is the chip length, and $T_b = N_c T_c$ is the bit length.

The channel gain $h_{BA}(i)$ models the Mie-based attenuation or random fading on the optical path, and $n_A(i)$ is the additive noise (shot noise, background light, etc.) at Alice's receiver. Here, $y_A(i)$ is the *i*-th sample observed at Alice

$$y_A(i) \ = \ \begin{cases} n_A(i), & (H_0 : \text{is true}) \\ h_{BA}(i)\, x_{\text{LPI}}(i) \ + \ n_A(i), & (H_1 : \text{is true}) \end{cases} \tag{6}$$

and we describe the adversary's perspective as a hypothesis-testing problem with two hypotheses:

- H_0: *Bob is silent*, so Alice receives only noise $n_A(i)$.
- H_1: *Bob is transmitting* the (low-power) symbol $x_{\text{LPI}}(i)$, faded by $h_{BA}(i)$ and corrupted by noise $n_A(i)$.

An adversary (i.e., Eve) tries to detect whether the sequence $\{y_A(i)\}$ corresponds to H_0 or H_1. Define two probability distributions over $\{y_A(i)\}$:

$$p_0 \ \text{ under } H_0, \quad p_1 \ \text{ under } H_1. \tag{7}$$

The adversary applies a decision rule $\delta(\{y_A(i)\}) \in \{H_0, H_1\}$ to minimize some cost. The key metrics for covert communications are:

$$P_{\text{FA}} \ = \ P(\delta = H_1 \mid H_0), \quad P_{\text{MD}} \ = \ P(\delta = H_0 \mid H_1). \tag{8}$$

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

To maintain *covert* communication, the distributions p_0 and p_1 must be "close enough" so that *any* detection test keeping the false alarm probability P_{FA} low necessarily incurs a high misdetection probability P_{MD} (and vice versa). In practical terms:

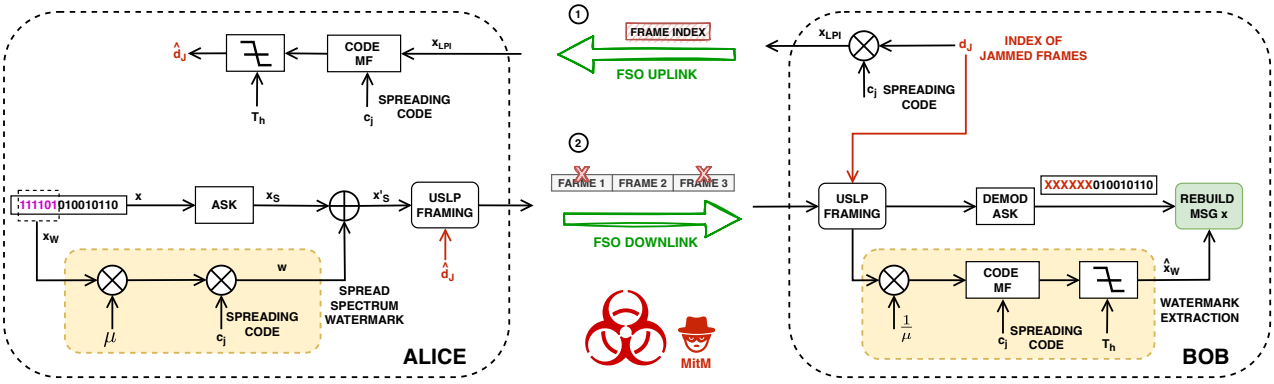


Fig. 3: SATCOM defense based on cooperative data link jamming and spread spectrum watermarking.

- If the adversary tries to keep P_{FA} low (i.e., rarely declaring "signal present" under uncertainty), then P_{MD} becomes large (the adversary misses the real signal most of the time).
- If the adversary tries to keep P_{MD} low (catch nearly every real signal), then P_{FA} becomes large (frequent false alarms even under noise).

If Bob transmits the low-power signal $\{x_{\text{LPI}}(i)\}$ so weak that

$$y_A(i) \approx n_A(i) \quad \text{with high probability,} \tag{9}$$

then the distribution p_1 under H_1 (i.e., Bob is transmitting) becomes almost indistinguishable from the noise-only distribution p_0. Thus, an adversary employing a Likelihood-Ratio Test (LRT) is forced to accept either a large P_{FA} (frequent false alarms) or a large P_{MD} (frequent misses) if they attempt to detect Bob's signal.

Although the channel is not strictly AWGN (because $h_{BA}(i)$ is random), the AWGN "square-root law" [35] intuition can hold to estimate the number of bits that Bob can exchange with Alice. Indeed, following the square root law, Bob can transmit using LPD communication up to $\mathcal{O}\sqrt{N}$ informative bits in a noisy channel (where N is the length of the binary modulated signal generated with LPD). In other words, 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.

Equation (6) formalizes the discrete-time samples of Alice's received signal $y_A(i)$ under H_0/H_1. Random Mie fading enters via $h_{BA}(i)$, and $x(i)$ is kept low power for covertness. The adversary's false alarm/miss probabilities $(P_{\text{FA}}, P_{\text{MD}})$ in (8) characterize detectability. By ensuring the distributions under (H_0, H_1) remain close, Bob can maintain a covert link under non-AWGN conditions.

B. Step (2): Downlink Protection

This section provides a mathematical formulation for the downlink protection (i.e., step (2) in Figure 3), assuming a non-degraded wiretap channel model [36] for signals representation. We took inspiration from the WBPLSec [34] algorithm for watermarked signal management, but with the important innovation of the jamming method, which is one of the contributions of this paper.

Suppose that Alice (transmitter in Figure 3) and Bob (receiver in Figure 3) wish to exchange a *secret message*, denoted by x, in preparation for secure communications they plan to conduct later. This message is first modulated by Amplitude Shift Keying (ASK) and can be expressed as

$$x_S(i) = \begin{cases} A_a \sqrt{\dfrac{2}{T_{hs}}} \cdot cos(2\pi f_{hs} i), & \text{for } 0 \le i \le T_{hs}, \\ 0, & \text{elsewhere,} \end{cases} \tag{10}$$

where A_a is the amplitude, T_{hs} is the symbol time and f_{hs} is the frequency of the modulated signal.

Following the classical spread spectrum approach outlined in [37], the embedding process relies on ASK to produce a host signal from the secret x. A subset of that secret, denoted N_W, is then utilized to form the SS watermark (i.e., x_W) and mark the host signal x_S via spread spectrum. Hence, the SS watermark is given by

$$w(i) = \sum_{k=-\infty}^{+\infty} \sum_{j=0}^{N_c-1} g(i - kT_b - jT_c)(c_W(i))_j (x_W(i))_k, \tag{11}$$

where $(x_W(i))_k$ is the k-th data bit of the watermark signal, $(c_W(i))_j$ represents the j-th chip of the orthogonal PN sequence, $g(i)$ is the pulse waveform, T_c is the chip length, and $T_b = T_{hs} = N_c T_c$ is the bit length. Whereas we utilize the first equation for watermarking defined by Cox *et al.* [38] to formally define the watermarked signal as follows

$$x'_S(i) = x_S(i) + \mu w(i), \tag{12}$$

where $x_S(i)$ is the i-th sample of the ASK signal [22], μ is the scaling parameter and $w(i)$ is the SS watermark.

The legitimate user, 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 Bob's side, we assume that the frame obfuscation (i.e., the effect of the cooperative jamming) can be represented

as an interference x_J. The legitimate receiver applies Algorithm 1 for the correct reconstruction of the secret message or key sent by Alice.

We denote the i-th sample of the received signal at Bob and Eve, respectively, be:

$$y_M(i) = h_M(i)x'_S(i) + x_J(i) + n_M(i), \tag{13}$$

$$y_E(i) = h_E(i)x'_S(i) + x_J(i) + n_E(i), \tag{14}$$

where h_M, h_E are the channel's gains. x'_S is the data signal, x_J is the jamming signal, n_M and n_E are the complex zero-mean Gaussian noise with variance σ^2. Without loss of generality in the rest of the paper, we assume that $\mathbb{E}[|\boldsymbol{x}_S|^2] = 1$ and $\mathbb{E}[|\boldsymbol{x}_J|^2] = 1$.

VI. Secrecy Rate

This work adopts the secrecy rate (R_s) as a metric to evaluate PLS performance. The secrecy rate is the specific transmission rate (bits per second, for example) at which a system sends confidential data while ensuring that an eavesdropper can derive negligible information about the message.

Since the proposed algorithm relies on cooperative intentional interference, we must introduce the Signal-to-Interference Plus Noise Ratio (SINR). The SINR at Bob's side is given by

$$\gamma_M = \frac{|h_M|^2 P_t^2}{\sigma_M^2 + \cancelto{0}{P_j^2}}, \tag{15}$$

where P_t is the transmitted optical power, P_j is the jamming optical power, and σ_M^2 is the background noise spectral density.

The SINR at Eve's side is given by

$$\gamma_E = \frac{|h_E|^2 P_t^2}{\sigma_E^2 + P_j^2}. \tag{16}$$

As already discussed, Bob (the legitimate receiver) is the only one responsible for generating the frame obfuscation on the optical links, which means he knows precisely which bits have been corrupted. Consequently, it becomes feasible to eliminate the interference term from equation (15), mirroring the successive interference cancellation approach frequently employed in the literature. This selective disturbance removal effectively disrupts the interceptor's detection efforts, leaving Bob's data intact.

When modelling FSO channels as described in Section IV-A, the secrecy rate (R_s) for non-degraded Gaussian wiretap channels [36] under these conditions can be expressed as

$$R_s = \max\{C_M - C_E, 0\} = \begin{cases} \log_2 \frac{1+\gamma_M}{1+\gamma_E}, & \text{if } \gamma_M > \gamma_E, \\ 0, & \text{if } \gamma_M \leq \gamma_E, \end{cases} \tag{17}$$

where $C_M = \log_2(1+\gamma_M)$ is the channel capacity from Alice to Bob, i.e., the main channel, and $C_E = \log_2(1+\gamma_E)$ is the channel capacity from Alice to Eve, i.e., the eavesdropper's channel.

VII. Numerical results

In this section, we aim to verify through Monte Carlo simulations the performance of covert communication using LPD/LPD signals (i.e., step (1)). Still, we also want to evaluate the secrecy rate we can achieve using cooperative jamming on USLP and SS watermarking (i.e., step (2)).

A. Modeling assumptions and normalization for simulations

We map link margin (in dB) to chip-wise Signal-to-Noise Ratio (SNR) via

$$\gamma \triangleq \gamma_{\text{ref}}\, 10^{\Gamma/10}, \qquad \gamma_{\text{ref}} = 1. \tag{18}$$

Hence, the main-channel SNR is $\gamma_M = 10^{\Gamma_B/10}$ and Eve's nominal SNR (absent watermark) is $\gamma_E^{(0)} = 10^{\Gamma_E/10}$; the hardware/process gap is $\Delta = \Gamma_B - \Gamma_E$. This choice fixes the SNR scale at the receiver sensitivity P_{req}; if an absolute calibration is preferred, replace $10^{\Gamma/10}$ with $\gamma_{\text{ref}}\, 10^{\Gamma/10}$.

In-band watermark and cooperative obfuscation. The DSSS watermark is embedded *in-band* with power ratio

$$\xi \triangleq \frac{P_{\text{wm}}}{P_t}, \tag{19}$$

and spreading length N. Bob knows both the watermark and the obfuscation index and cancels them (successive–interference cancellation), so his SINR is unaffected. In our simulations, the *obfuscation power* P_j replaces payload bits on selected frames (logical/cooperative jamming) and is therefore *not* modeled as additional radiated noise; its effect is captured at bundle level by the fraction q below. For Eve, the watermark acts as self–scaled interference; the effective SINR is modeled as

$$\gamma_E^{(\text{wm})} = \frac{\gamma_E^{(0)}}{1 + \xi_{\text{eff}}\gamma_E^{(0)}}, \qquad \xi_{\text{eff}} = \frac{\xi}{N}. \tag{20}$$

OOK error and capacity model. With OOK non-coherent detection, the bit-error probability is

$$p(\gamma) = \tfrac{1}{2}\,\text{erfc}\Big(\sqrt{\gamma/4}\Big). \tag{21}$$

We use the *symbols* C_M and C_E for the main/eavesdropper capacities:

$$C_M = 1 - H_2\big(p(\gamma_M)\big), \qquad C_E = 1 - H_2\big(p(\gamma_E^{(\text{wm})})\big). \tag{22}$$

Bundle-level secrecy rate with frame obfuscation. We consider a 4096-bit USLP bundle (64 frames $\times$ 64 bits). If O_f frames are deliberately obfuscated (e.g., $O_f = 2$), then a fraction $q = \frac{O_f}{64}$ of frames is useless for Eve (capacity zero on those frames), while Bob recovers them perfectly via the watermark index. Averaging over the bundle gives the secrecy spectral efficiency

$$R_s = \big[\, C_M - (1-q)\, C_E \,\big]^+, \tag{23}$$

which is the formula used in our numerical simulations. Setting $q = 0$ recovers the case without explicit frame-erasure averaging on Eve.

B. Attacker Model to covert communication: Unknown Spreading Code

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 since direct correlation (i.e., matched filtering) is no longer straightforward.

We use binary antipodal chip sequences from the Walsh–Hadamard set of length $N = 2^m$ [22]. Let $M_1 = [1]$ and, for $m \geq 1$, build M_{2N} via the Sylvester recursion $M_{2N} = \begin{bmatrix} M_N & M_N \\ M_N & -M_N \end{bmatrix}$. Each spreading code is a row $\mathbf{c}$ of M_N mapped to $\{\pm 1\}$ and normalized to unit energy ($\tilde{\mathbf{c}} = \mathbf{c}/\sqrt{N}$); rows are mutually orthogonal ($M_N M_N^\top = N I_N$). The attacker does not know which row is in use.

In this stage, Bob must send a secret key of length K bits to Alice under LPD conditions. We follow the square-root law by setting $K = \mathcal{O}(\sqrt{N})$ so that transmitting $\sqrt{N}$ bits within a DSSS waveform of length N remains covert. The simulation proceeds as follows:

We consider two strategies, assuming the adversary does *not* know the true PN sequence:

- *Energy Detection:* The detector computes

$$T_{\text{energy}} = \left| \frac{1}{N} \sum_{i=1}^{N} \left| y_A(i) \right|^2 \right|, \tag{24}$$

  and decides H_1 if $T_{\text{energy}} > \tau_{\text{energy}}$. A wideband, low-power signal may remain below the noise floor, degrading detection performance.
- *Blind Correlation:* The detector tries many candidate codes. For each candidate PN_{test}, it forms

$$T_{\text{corr}} = \left| \frac{1}{N} \sum_{i=1}^{N} y_A(i)\, \text{PN}_{\text{test}}(i) \right|, \tag{25}$$

  and declares H_1 if any peak exceeds a threshold τ_{corr}. Because N is large and Bob's PN is unknown (and can be changed frequently), this search becomes infeasible or yields a high miss probability unless the adversary accepts many false alarms.

We use a Monte Carlo procedure with M_c independent trials to evaluate an adversary's detection performance. The adversary then attempts to detect the presence of our LPD signal either via energy detection (using threshold τ_{energy}) or correlation (using threshold τ_{corr}).

Then, for a given threshold η, the FA and MD probabilities can be written as

$$P_{\text{FA}} = \frac{\sum_{i=1}^{M_c} \mathcal{H}(\bar{T}_i)}{M_c}, \text{ if } \ H_1 \text{ is true}, \tag{26}$$

$$P_{\text{MD}} = 1 - \frac{\sum_{i=1}^{M_c} \mathcal{H}(\bar{T}_i)}{M_c}, \text{ if } \ H_0 \text{ is true}, \tag{27}$$

where M_c is the number of Monte Carlo experiments. And $\mathcal{H}(\bar{T})$ denotes the Heaviside step function as

$$\mathcal{H}(\bar{T}) = \begin{cases} 1, & \bar{T} < \eta, \\ 0, & \bar{T} \geq \eta. \end{cases} \tag{28}$$

TABLE I: Simulation parameters.

Parameter	Value
P_{tx}	17.5 dBm
P_{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.

Our results show that when the PN sequence is unknown, and N is large, the attacker faces a high misdetection probability unless accepting a large false alarm rate. Meanwhile, knowing the watermark keys, the legitimate receiver can reconstruct $\sqrt{N}$ bits of covert data with minimal risk of detection by an adversary performing only blind or energy-based detection.

Figure 4 and Figure 5 show the Receiver Operating Characteristic (ROC) (i.e., P_{FA} versus P_{MD}) for an eavesdropper attempting to detect the LPD covert channel in an uplink scenario. Table I summarizes the main simulation parameters.

Within every panel, the *upper* subplot corresponds to Eve's attack strategy: Figure 4(a) the energy detector and Figure 5(a) the blind-correlation (code-guessing) detector that tests $G = 8$ random spreading codes. Curves are parametrized by the length N of the Hadamard spreading sequence $\{16, 32, 64, 128, 256\}$; longer codes approach the diagonal. The diagonal joining $(P_{\text{FA}}, P_{\text{MD}}) = (1, 0)$ 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.

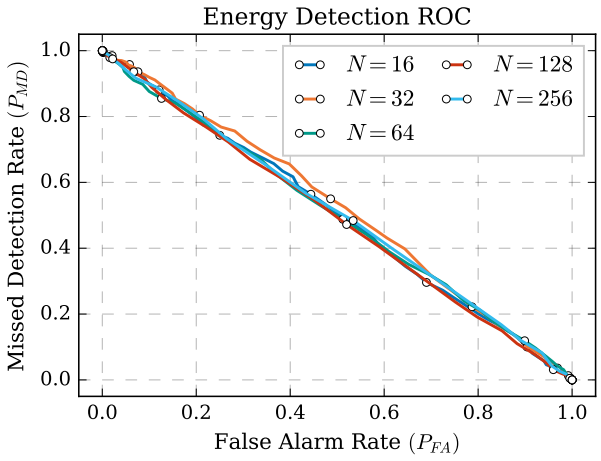
C. Numerical Simulations for Secrecy Rate Under Payload Obfuscation

We now outline how to simulate the secrecy rate (17) after performing "payload obfuscation" on select USLP frames, leveraging the link-budget equations for ISL and Uplink/Downlink (UDL) scenarios. Instead of a literal "jamming power," Alice modifies (obfuscates) certain payload bits, which effectively increases the Bit Error Rate (BER) for any eavesdropper lacking the obfuscation index. Bob knows precisely which frames are obfuscated and can reconstruct them using the watermark, so the main channel remains at low BER, while the eavesdropper's channel suffers.

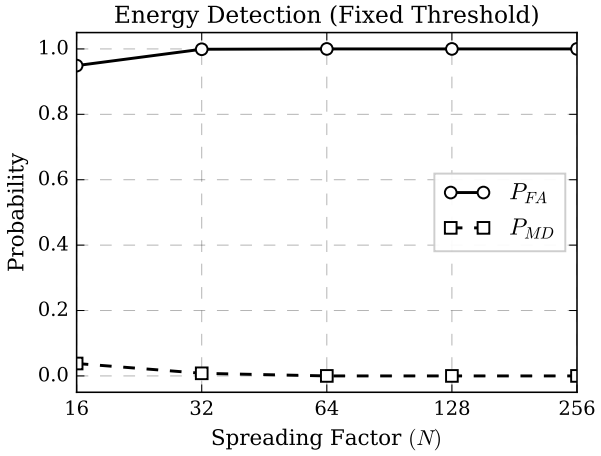
We use Section IV-A's equations (1) and (2) to compute the received power in dBm, $P_{\text{rx}}^{\text{ISL}}$ or $P_{\text{rx}}^{\text{UDL}}$. The ISL scenario has a minimal atmospheric effect but potentially significant pointing losses. In the UDL scenario, we incorporate Mie scattering and atmospheric absorption, so $h_M(i), h_E(i)$ vary based on local parameters.

When Alice decides to *obfuscate* a USLP frame (based on the "index" Bob provides in step (1)), she deliberately alters the payload bits, e.g. by injecting errors or scrambling those bits. Bob, however, knows which frames are obfuscated and uses the watermark to recover the original payload. Unaware of this index, an eavesdropper sees a higher BER on those frames.

Eve attempts to decode each USLP frame. Eve's BER depends on normal SNR or link margin for non-obfuscated frames. Eve's BER is significantly worse for obfuscated frames because the payload bits are systematically corrupted. Hence, from Eve's perspective, the "effective" SNR (or capacity) is degraded. Meanwhile, Bob recovers these frames with negligible penalty because he *knows* which bits are deliberately corrupted and can undo them via the watermark.

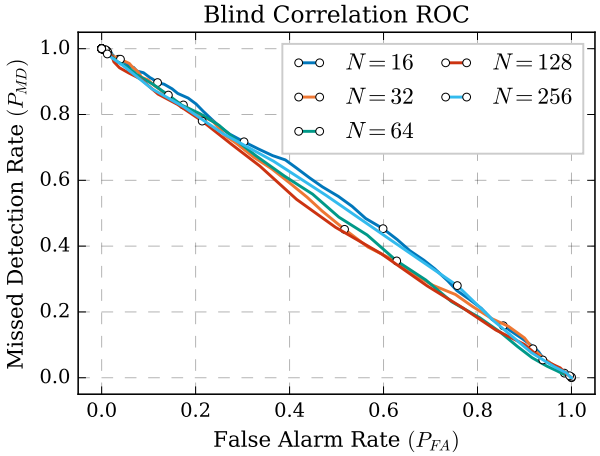


(a) Receiver operating characteristic curve for FSO uplink.

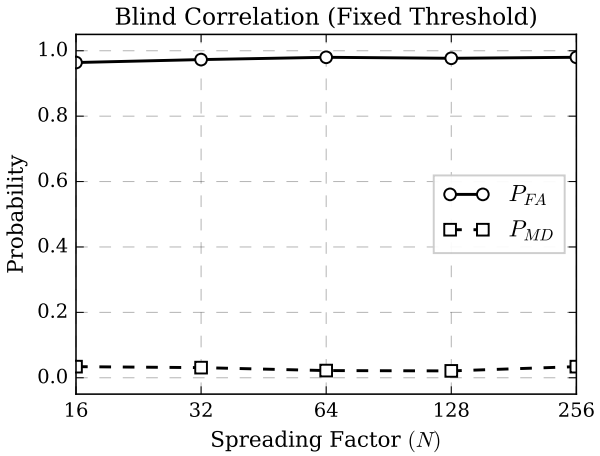


(b) Probability pattern.

Fig. 4: Attacker performance when using an energy detection strategy on an FSO uplink which employs an LPD signal.



(a) Receiver operating characteristic curve for FSO uplink.



(b) Probability pattern.

Fig. 5: Attacker performance when using a blind correlation strategy on an FSO uplink which employs an LPD signal.

We consider the OOK optical downlink (550 km, cirrus attenuation) with a 4096-bit USLP bundle (64 frames, 64 bits each). Two frames are deliberately obfuscated (cooperative jamming), while a DSSS watermark is embedded *in-band* and perfectly cancelled at Bob. Let Γ_B and Γ_E denote the link margins (in dB) of Bob and Eve; the hardware/process gap is $\Delta = \Gamma_B - \Gamma_E$. We denote the main/eavesdropper capacities by C_M and C_E, respectively (as per the OOK/BSC model stated at the beginning of Section VII).

In our simulations, the *obfuscation power* P_j replaces payload bits on selected frames and is therefore *not* modeled as additional radiated noise; its effect appears at the bundle level via the erasure fraction $q = \frac{O_f}{64}$. The in-band DSSS watermark uses power P_{wm} with ratio $\xi = P_{\text{wm}}/P_t$ and spreading length N. Bob knows the watermark and the obfuscation index and cancels them (successive–interference cancellation), so his SINR is unaffected. For Eve, the watermark acts as self-scaled

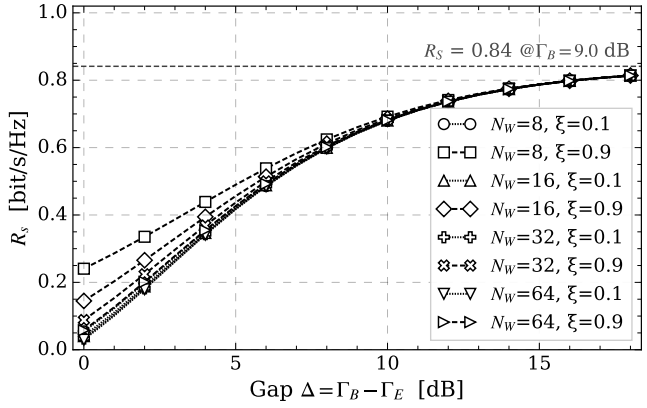


Fig. 6: Secrecy rate R_s versus gap $\Delta = \Gamma_B - \Gamma_E$ at fixed Γ_B (OOK downlink). Two watermark power ratios $\xi \in \{0.1, 0.9\}$; curves indexed by N. The horizontal line marks C_M at the chosen Γ_B.

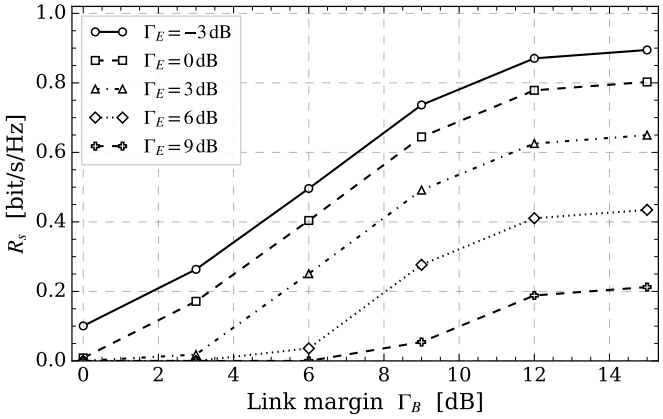


Fig. 7: Gap-family for $N = 16$: R_s versus Bob's margin Γ_B, with curves indexed by Eve's margin Γ_E (OOK downlink, cirrus). Increasing Γ_B (or reducing Γ_E) drives R_s toward C_M.

interference; her effective SINR follows Eq. (20).

If O_f of the 64 frames are obfuscated (here $O_f = 2$), Eve loses the fraction $q = \frac{O_f}{64}$ of useful frames; the bundle secrecy spectral efficiency is given by Eq. (23).

Figure 6 plots R_s versus the gap Δ at fixed $\Gamma_B = 9\,\text{dB}$, for two watermark intensities $\xi \in \{0.1, 0.9\}$ and several N_W. As Δ increases, $\gamma_E^{(\text{wm})}$ in (20) shrinks and R_s grows monotonically, asymptotically approaching the ceiling C_M set by Bob's margin. Stronger watermarking ($\xi = 0.9$) shifts the curves upward.

Figure 7 shows the *gap-family* at $N = 16$: the abscissa is Γ_B and each curve fixes Eve's margin Γ_E (hence Δ increases along the x-axis). The curves are monotone in Γ_B and saturate toward C_M; for the same Γ_B, larger watermark intensity or smaller Γ_E yield higher R_s. In both figures, we set $O_f = 2$ (i.e., $q = \frac{2}{64}$), consistent with the USLP constraint that the number of obfuscated bits does not exceed those protected by the DSSS watermark.

VIII. Discussion and Limitations

Our numerical study models the physical layer as chip-wise AWGN, with link margin Γ mapped to per-chip SNR via $\gamma = 10^{\Gamma/10}$. The in-band watermark that Eve observes is captured by an average interference loading $\xi_{\text{eff}} = \xi/N$, whereas cooperative obfuscation is modeled at the bundle level as an erasure fraction $q = \frac{O_f}{64}$ (Bob cancels both via successive-interference cancellation). We do not include hardware non-idealities (e.g., shot-noise/thermal-noise transitions, Analog-to-Digital Converter (ADC) quantization and clipping), tight synchronization, and MAC-timing constraints. Despite these simplifications, the reported R_s-versus-gap curves are monotone and repeatable across the tested margins and spreading lengths, providing a conservative indicator of the achievable secrecy gain.

Our proposed method leverages a LPI covert channel to securely transmit critical information regarding which satellite communication frames must be obfuscated. This covert channel operates below the noise threshold, enabling legitimate terminals to exchange data reliably without alerting potential eavesdroppers.

A key advantage of embedding obfuscation decisions within an LPI channel is that the transmitted signal appears indistinguishable from standard background noise from an adversary's perspective, limited to conventional spectrum analysis. No detectable spectral anomalies arise because the jamming pattern is driven by internal signal-processing routines rather than modulation or transmission power changes. Consequently, an adversary cannot detect unusual signaling behavior or deduce the underlying frame-obfuscation scheme. This ensures that critical frames remain protected without giving adversaries insights into the employed defensive measures or patterns.

The energy cost of this method compared to traditional data protection techniques, such as encryption, will be analyzed in the future. As already demonstrated in some situations, watermarking and jamming primitives can have lower power consumption than cryptographic techniques such as AES [39].

It is essential to note that, because the proposed method abstracts from the hardware that comprises the satellite transceiver, it can also be applied to RF-based SATCOM.

IX. Conclusions

This paper introduces a novel 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. Leveraging a covert side channel for communicating the indices of frames selected for obfuscation and embedding watermark signals using a shared spreading code, our scheme ensures that legitimate receivers effectively negate friendly interference and reliably recover obfuscated keys and data. Importantly, our method integrates seamlessly into existing CCSDS/USLP protocols, achieving strong security enhancements without significant hardware upgrades or protocol disruptions.

Numerical evaluations demonstrated robust security under realistic attack conditions. Specifically, 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. This result underscores the practical undetectability of our proposed covert channel, ensuring secure and stealthy key exchanges in SATCOM environments.

Furthermore, the link-budget–driven simulations for the optical downlink confirm that the secrecy spectral efficiency R_s increases monotonically with the Bob–Eve gap Δ and saturates at the main-channel ceiling C_M set by Bob's margin. Using a representative downlink margin $\Gamma_B = 9\,\mathrm{dB}$, two obfuscated USLP frames ($O_f = 2$), and an in-band DSSS watermark, we observe $R_s \simeq 0.64\,\mathrm{bit\,s^{-1}Hz^{-1}}$ at $\Delta \approx 9\,\mathrm{dB}$ for $N = 8$ (and up to $R_s \simeq 0.78\,\mathrm{bit\,s^{-1}Hz^{-1}}$ by $\Delta \approx 12\,\mathrm{dB}$), while larger spreads moderately reduce the achievable rate due to the effective loading $\xi_{\mathrm{eff}} = \xi/N$. These results, obtained without altering USLP framing or the O3K mapping, support the practicality of watermark-assisted cooperative obfuscation on current SATCOM stacks.

Overall, the presented cooperative jamming and watermarking paradigm provides a powerful yet practical means to securely distribute cryptographic keys over SATCOM links, offering substantial improvements in secrecy, efficiency, and stealth compared to conventional cryptographic approaches. The approach promises agile, software-driven protection against sophisticated adversaries, positioning it as a valuable contribution to next-generation satellite communication security.

REFERENCES

[1] A. Lalbakhsh, A. Pitcairn, K. Mandal, M. Alibakhshikenari, K. P. Esselle, and S. Reisenfeld, "Darkening Low-Earth Orbit Satellite Constellations: A Review," *IEEE Access*, vol. 10, pp. 24 383–24 394, 2022.

[2] B. Lin, W. Henry, and R. Dill, "Defending small satellites from malicious cybersecurity threats," in *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, 2022, pp. 479–488.

[3] N. Tieby, J. Khoury, and E. Bou-Harb, "Characterizing and analyzing leo satellite cyber landscape: A starlink case study," in *ICC 2024 - IEEE International Conference on Communications*, 2024, pp. 1352–1357.

[4] Avia.Pro, "Russian satellite Luch-5X approaches American communications satellite Intelsat 39," Apr 2025, https://avia-pro.net/news/rossiyskiy-sputnik-luch-5h-priblizhaetsya-k-amerikanskomu-sputniku-svyazi-intelsat-39 [Accessed: (April 2025)].

[5] R. Peled, E. Aizikovich, E. Habler, Y. Elovici, and A. Shabtai, "Evaluating the security of satellite systems," 2023. [Online]. Available: https://arxiv.org/abs/2312.01330

[6] F. Rawlins, R. Baker, and I. Martinovic, "Death by a thousand cots: Disrupting satellite communications using low earth orbit constellations," *arXiv preprint arXiv:2204.13514*, 2022.

[7] R. Bisping, J. Willbold, M. Strohmeier, and V. Lenders, "Wireless Signal Injection Attacks on VSAT Satellite Modems," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 6075–6091. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/bisping

[8] M. Y. Abdelsadek, A. U. Chaudhry, T. Darwish, E. Erdogan, G. Karabulut-Kurt, P. G. Madoery, O. Ben Yahia, and H. Yanikomeroglu, "Future Space Networks: Toward the Next Giant Leap for Humankind," *IEEE Transactions on Communications*, vol. 71, no. 2, pp. 949–1007, 2023.

[9] M. Giordani, F. Ardizzon, L. Crosara, N. Laurenti, and M. Zorzi, *The Role of Non-terrestrial Networks: Features and Physical-Layer Security Concerns*. John Wiley & Sons, Ltd, 2024, ch. 13, pp. 275–303. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394170944.ch13

[10] B. Lin, W. Henry, and R. Dill, "Defending small satellites from malicious cybersecurity threats," in *International Conference on Cyber Warfare and Security*, vol. 17, no. 1, 2022, pp. 479–488.

[11] R. Singh, I. Ahmad, and J. Huusko, "The role of physical layer security in satellite-based networks," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2023, pp. 36–41.

[12] G. Giuliari, T. Ciussani, A. Perrig, and A. Singla, "ICARUS: Attacking low earth orbit satellite networks," in *2021 USENIX Annual Technical Conference (USENIX ATC 21)*. USENIX Association, Jul. 2021, pp. 317–331. [Online]. Available: https://www.usenix.org/conference/atc21/presentation/giuliari

[13] G. Baselt, M. Strohmeier, J. Pavur, V. Lenders, and I. Martinovic, "Security and privacy issues of satellite communication in the aviation domain," in *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon)*, vol. 700, 2022, pp. 285–307.

[14] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," *IEEE Photonics Journal*, vol. 7, no. 2, pp. 1–14, 2015.

[15] S. News, "U.S. Space Force official warns of rising Chinese threats," Dec 2024, https://spacenews.com/u-s-space-force-official-warns-of-rising-chinese-threats/ [Accessed: (April 2025)].

[16] G. Jang, B. You, and H. Jung, "A survey on physical layer security schemes in satellite networks," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 2022, pp. 1213–1215.

[17] S. Gecgel and G. K. Kurt, "Intermittent jamming against telemetry and telecommand of satellite systems and a learning-driven detection strategy," in *Proceedings of the 3rd ACM Workshop on Wireless Security and Machine Learning*, ser. WiseML '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 43–48. [Online]. Available: https://doi.org/10.1145/3468218.3469041

[18] P. Yue, J. An, J. Zhang, J. Ye, G. Pan, S. Wang, P. Xiao, and L. Hanzo, "Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 3, pp. 1604–1652, 2023.

[19] P. V. Trinh, A. T. Pham, A. Carrasco-Casado, and M. Toyoshima, "Quantum key distribution over fso: Current development and future perspectives," in *2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama)*, 2018, pp. 1672–1679.

[20] M. Sabani, I. Savvas, D. Poulakis, and G. Makris, "Quantum key distribution: Basic protocols and threats," in *Proceedings of the 26th Pan-Hellenic Conference on Informatics*, ser. PCI '22. New York, NY, USA: Association for Computing Machinery, 2023, p. 383–388. [Online]. Available: https://doi.org/10.1145/3575879.3576022

[21] P. Zhang, J. Sagar, E. Hastings, M. Stefko, S. Joshi, and J. Rarity, "End-to-end demonstration for cubesatellite quantum key distribution," *IET Quantum Communication*, vol. 5, no. 3, pp. 291–302, 2024. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/qtc2.12093

[22] J. G. Proakis, *Digital communications*. Boston: McGraw-Hill, 2008.

[23] G. Dillard, M. Reuter, J. Zeiddler, and B. Zeidler, "Cyclic code shift keying: a low probability of intercept communication technique," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 39, no. 3, pp. 786–798, 2003.

[24] J. Zhao, S. Qiao, J. H. Booske, and N. Behdad, "Low Probability of Intercept/Detect (LPI/LPD) Secure Communications Using Antenna Arrays Employing Rapid Sidelobe Time Modulation," *IEEE Transactions on Antennas and Propagation*, vol. 72, no. 8, pp. 6448–6463, 2024.

[25] A. Glenn, "Low probability of intercept," *IEEE Communications Magazine*, vol. 21, no. 4, pp. 26–33, 1983.

[26] A. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[27] M.-K. Tsay, C.-H. Liao, C.-S. Shyn, and T.-Y. Yang, "Simultaneous AJ and LPD Evaluations for Secure Communication," in *MILCOM 2007 - IEEE Military Communications Conference*, 2007, pp. 1–6.

[28] R. Dybdal and K. Soohoo, "LPI/LPD Detection Sensitivity Limitations," in *2014 IEEE Military Communications Conference*, 2014, pp. 1657–1662.

[29] CCSDS, "Recommendation for Space Data System Standards: Unified Space Data Link Protocol," CCSDS 732.1-B-3, June 2024. [Online]. Available: https://ccsds.org/

[30] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[31] ITU-R, "S.1590 : Technical and operational characteristics of satellites operating in the range 20-375 THz ," https://www.itu.int/rec/R-REC-S.1590-0-200209-I/en [Accessed: (October 2024)].

[32] ——, "P.1621 : Propagation data required for the design of Earth-space systems operating between 20 THz and 375 THz," https://www.itu.int/rec/R-REC-P.1621-2-201507-I/en [Accessed: (October 2024)].

[33] ——, "P.1622 : Prediction methods required for the design of Earth-space systems operating between 20 THz and 375 THz," https://www.itu.int/rec/R-REC-P.1622-1-202208-I/en [Accessed: (October 2024)].

[34] S. Soderi and R. De Nicola, "6G Networks Physical Layer Security Using RGB Visible Light Communications," *IEEE Access*, vol. 10, pp. 5482–5496, 2022.

[35] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of Reliable Communication with Low Probability of Detection on AWGN Channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2013.

[36] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[37] H. Malvar and D. Florencio, "Improved spread spectrum: a new modulation technique for robust watermarking," *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 898–905, Apr 2003.

[38] I. J. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673–1687, Dec 1997.

[39] G. Costa, P. Degano, L. Galletta, and S. Soderi, "Formally verifying security protocols built on watermarking and jamming," *Computers & Security*, vol. 128, p. 103133, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823000433