RESEARCH-ARTICLE

SpaceJam: Protocol-aware Jamming Attacks against Space Communications

EDD SALKIELD, University of Oxford, Oxford, Oxfordshire, U.K.

SEBASTIAN KÖHLER, University of Oxford, Oxford, Oxfordshire, U.K.

SIMON BIRNBACH, University of Oxford, Oxford, Oxfordshire, U.K.

MARTIN STROHMEIER, Armasuisse, Switzerland, Bern, BE, Switzerland

IVAN MARTINOVIC, University of Oxford, Oxford, Oxfordshire, U.K.

Open Access Support provided by:

University of Oxford

Armasuisse, Switzerland

Published: 30 June 2025

Citation in BibTeX format

WiSec 2025: 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks
June 30 - July 3, 2025
VA, Arlington, USA

Conference Sponsors:
SIGSAC

https://doi.org/10.1145/3734477.3734714
ISBN: 9798400715303

SpaceJam: Protocol-aware Jamming Attacks against Space Communications

Edd Salkield
edd.salkield@cs.ox.ac.uk
University of Oxford
Oxford, United Kingdom

Sebastian Köhler
sebastian.kohler@cs.ox.ac.uk
University of Oxford
Oxford, United Kingdom

Simon Birnbach
simon.birnbach@cs.ox.ac.uk
University of Oxford
Oxford, United Kingdom

Martin Strohmeier
martin.strohmeier@ar.admin.ch
armasuisse S+T
Zurich, Switzerland

Ivan Martinovic
ivan.martinovic@cs.ox.ac.uk
University of Oxford
Oxford, United Kingdom

Abstract

Motivated by the growing prevalence of increasingly advanced satellite jamming attacks, we introduce and systematically analyze protocol-aware jammers: the worst-case scenario that maximally exploits the protocol to deny service whilst remaining as difficult to detect as possible. This extends existing satellite jamming and anti-jamming literature, which to date considers only conventional jamming waveforms.

We find that protocol-aware jammers are significantly more effective than conventional jammers against all major standardized satellite protocols, including when anti-jamming countermeasures in the form of interleaving and adaptive coding and modulation are employed. This performance is possible since current protocols have a cyclic and predictable nature. We assess the required capabilities in terms of synchronization, and show that many of these performance gains can be realized even by completely desynchronized jammers.

We experimentally evaluate protocol-aware strategies against both a hardware and software receiver. The results show that over 15 dB of performance gains over Gaussian jamming are possible against all tested satellite protocols. Furthermore, we find that the attack can be optimized in simulation and deployed against the hardware receiver without performance degradation. We conclude with a discussion of countermeasures, primarily at the protocol level, to improve the availability of these systems.

CCS Concepts

• **Security and privacy** → **Denial-of-service attacks**; **Mobile and wireless security**; *Hardware attacks and countermeasures*; • **Networks** → **Mobile and wireless security**; **Very long-range networks**; *Physical links*; • **Hardware** → *Signal integrity and noise analysis.*

Keywords

Satellite security; denial of service; data-link jamming

WiSec 2025, Arlington, VA, USA

ACM ISBN 979-8-4007-1530-3/2025/06
https://doi.org/10.1145/3734477.3734714

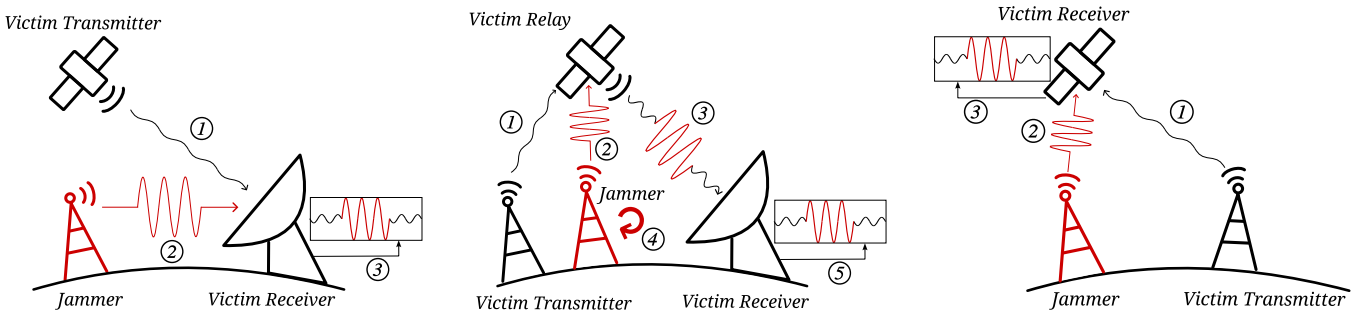
ACM Reference Format:
Edd Salkield, Sebastian Köhler, Simon Birnbach, Martin Strohmeier, and Ivan Martinovic. 2025. SpaceJam: Protocol-aware Jamming Attacks against Space Communications. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2025), June 30-July 3, 2025, Arlington, VA, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3734477.3734714

1 Motivation

The threat of jamming attacks against wireless communication channels—in which an attacker emits intentional interference in an attempt to disrupt successful data transmission—has been widely evaluated and the risks posed extensively classified. These attacks represent an increasing threat against satellite communications given their role as critical infrastructure. Furthermore, cheap commercial off-the-shelf (COTS) radio hardware means it is no longer sufficient to assume that any security is provided through inherent difficulties in accessing the required frequencies [1, 2]. As a result, modern jammers are no longer constrained to transmit only conventional jamming waveforms such as Gaussian noise, single tone modulated onto a carrier, or simple pulsed jamming, but can also optimize given knowledge of the particular protocol.

However to the best of our knowledge no current academic literature considers the threat of protocol-aware jammers against satellite communications. To date, the majority of works consider only protocol-unaware strategies such as AWGN and pulsed jamming, however the existence of more effective jammer waveforms has been posited [3–5]. The most related satellite jamming works optimize the jammer in the form of tuning the pulse rate, but stop short of considering further protocol-level improvements [5–8].

In other wireless systems such as WiFi, it has been found that protocol-aware jammers can achieve denial of service with many orders of magnitude less power than their protocol-unaware counterparts [9, 10]. The capabilities of the jammer have an important effect on their ability to exploit this knowledge. Reactive jammers, which specifically target frames which are "on the air", are capable of exploiting protocol knowledge, but require close proximity to the target to achieve the required synchronization level [11]. Clearly, accurately measuring the current frame and responding accordingly is difficult in a satellite setting where the jammer and receiver can be highly distant. We are interested in addressing this limitation given the unique properties of satellite data protocols, which are not random-access but instead have predictable timing properties.



(a) Downlink (b) Relay (c) Uplink

Figure 1: The three satellite system architectures considered in this work. From left to right: a) A satellite-originating downlink transmission, or relay network at the data-link layer or above. b) PHY-layer relay satellite, where the attacker jams the uplink to target a downlink receiver. c) TT&C uplink, where the attacker jams the uplink. The stages of the attack are marked with circled numbers and explained in Section 3.

Our objective in this work is to provide the first comprehensive overview of protocol-aware jammers against currently-deployed satellite communication systems. Whilst we focus on the widely-used standards as published by the standard bodies CCSDS and ETSI, this work is derived from fundamental principles which also apply in other cases (e.g. custom/proprietary protocols). In contrast to other works, we derive our jammer model from the fundamental units of failure, namely error correction and synchronization, and then work backward through the structure of the protocol to find the most efficient way of causing a failure. Intuitively, the degree to which the protocol structure can be taken advantage of depends on the level of synchronization of the jammer and the predictability of the protocol.

In summary, the main contribution of this work is to consider satellite jammers that, rather than transmitting protocol-unaware waveforms such as stochastic noise, can instead construct an adversarial waveform leveraging prior knowledge of the protocol, its structure, and how its components are processed by the receiver. More specifically, we make the following contributions:

- We systematize and assess jammers of different capabilities. We contrast these to existing work that only considers Gaussian pulsed jammers.
- We introduce novel techniques designed to stealthily deny service by taking advantage of the predictable structure of all major space protocols.
- We demonstrate through simulations and real world experiments the performance gains achievable, and that protocol-aware jammers outperform all previous techniques.
- Finally, we propose new countermeasures to mitigate the predictability of the structure, and therefore improve performance in the presence of jamming.

2 Related work

Jamming attacks against wireless systems have been well explored and evaluated in academic works, against many major classes of protocol. Since the performance of wireless systems in stochastic noise conditions is well understood, these results have been applied widely to evaluate the performance of protocol-unaware jammers [12–14]. Similarly to stochastic noise, a protocol-unaware jammer causes errors independently of the protocol's construction through e.g. *Additive White Gaussian Noise* (AWGN) or pulsed jamming.

A number of works have investigated more optimal jamming techniques which take advantage of the construction of the protocol, proposing a *reactive jammer* to synchronize to and destroy the signal. To date, these techniques have been applied in the context of multiple-access wireless channels which require reactive synchronization, but not in the unique context of satellite communications which are typically single-access and have a uniquely predictable structure, meaning synchronization is not necessarily required.

Broadly, papers on protocol-aware jamming techniques fall into two categories: a) information theoretic techniques which maximize the error rate in terms of physical symbols, and b) data-link level techniques which exploit higher level protocol constructs. We provide a comparative analysis between our work these other works in turn, and then finally consider related works in a satellite communication context.

2.1 Theoretically optimum jamming

Previous information theoretic work modeling jamming waveforms has demonstrated that there are substantial jamming performance gains to be made over conventional jamming strategies [15–18]. These works leverage knowledge of the physical-layer characteristics of the signal, especially the chosen modulation scheme, in order to maximize the symbol error rate. It has been shown that such a waveform is discontinuous, and relies on selectively targeting samples at the amplitude which optimizes the symbol error rate [19].

Although these strategies significantly reduce the average jammer power required to achieve given bit error rates, thus improving stealthiness, these works have only considered hard demodulators and ignore important practical aspects such as the error correcting code and protocol structure [19, 20]. Against many classes of soft error correcting systems, the best known jammer distribution is a pulsed jammer [6]. In contrast, our analytic model predicts the performance of a soft-demodulated forward error correction system

under the worst-case jammer, and evaluate the error correcting codes specifically standardized for use in satellite systems.

2.2 Data-link level and reactive jamming

Protocol-aware jammers which exploit data-link level knowledge are known to achieve large performance gains against their protocol-unaware counterparts. To exploit the protocol structure, several works suggest a reactive jammer to synchronize to the protocol and target certain structures [9, 11]. By targeting only the minimally required portion of each frame, a performance improvement of several orders of magnitude has been shown.

In contrast to existing works, which consider random access channels such as WiFi and Bluetooth, satellite links are designed for high latency and consist of a fixed length, repeating slot structure [21–23]. Therefore, whereas other data-link level jammers require a frame detection and synchronization mechanism to target individual frames, satellite jammers can instead exploit the known cyclic structure consisting of fixed length, repeating slots. Our evaluation focuses in particular on the gains possible by desynchronized jammers exploiting data-link knowledge without an additional synchronization mechanism.

Cyclic communication aspects were previously exploited in the context of WiFi, where an interleaver distributes adjacent bits into separate OFDM subcarriers [10]. The effect is that interference affecting several adjacent subcarriers is spread out and therefore is easier to correct. It was shown that a deinterleaving jammer can be constructed to target multiple subcarriers in order to concentrate the jammer pulses, and which results in a higher frame error rate. Only frame-level synchronization is required. We propose and evaluate a similar deinterleaving jammer architecture, but instead targeting the specific (A)-PSK symbol interleaver proposed for satellite systems.

2.3 Satellite signal jamming

Surprisingly, no current academic work considers the application of protocol-aware jammers to current space communication standards. Instead, nearly all existing satellite work focuses on GNSS systems such as GPS, which are code-division shared channels designed for position, navigation, and tracking rather than data transport [24, 25]. Therefore these results do not generalize well to all other satellite protocols which are designed under different constraints: in particular not being code-division but rather transmitting arbitrary data in a frame structure [2].

The most directly related work considers the vulnerability of current satellite uplink protocols to pulsed AWGN jammer waveforms, and was critical in the selection of the protocol structure and error correcting codes standardized today by CCSDS [6]. Whilst this work does briefly consider how the pulsed duty cycle can be optimized for a given system, the analysis does not extend to data-link level jamming. Furthermore, whilst interleaving is evaluated as an anti-jamming countermeasure, the undoing of the interleaver to further maximize performance was not considered.

3 Background

In this paper, we consider the three most prevalent satellite system architectures: satellite-originating downlink transmissions, physical-layer relay satellites, and telemetry, tracking, and control (TT&C) uplink transmissions originating from a ground station. Figure 1 depicts each of them under attack by a protocol-aware jammer. In this section, we describe each of these link architectures in these attack scenarios, as well as the protocols corresponding to each architecture.

3.1 Satellite System Architecture

3.1.1 Downlink. Figure 1a shows a satellite transmitting data on the downlink to a receiving ground station ①. To prevent the ground station from receiving the data, a jammer transmits an interfering signal targeting the ground station ②. The combined signal is then received by the ground station, preventing the successful reception of the satellite data ③. This scenario also applies to the last hop of a relay network which operates at the data-link layer or above, as the satellite reencodes and remodulates the data on board rather than relaying the physical signal.

3.1.2 Relay. A physical-layer relay satellite is used in Figure 1b to relay the signal transmitted by a ground station ① to a different, receiving ground station. In this case, no processing is done on the satellite. The satellite merely acts as a "bent pipe" and retransmits the waveform on the downlink exactly as it received it on the uplink. The jammer exploits this property and injects their jamming signal on the uplink ②. The victim and the attack signal both reach the satellite, and the combined signal is retransmitted to the ground station ③. The jammer can receive the downlink signal as well and use it to fine tune the attack. By carefully observing the downlink while adjusting the jamming signal, they can achieve full synchronization with the victim signal ④. The combined signal is then received by the ground station, preventing the successful reception of the satellite data ⑤.

3.1.3 Uplink. Figure 1c shows a satellite receiving telecommands from a transmitting ground station on the uplink ①. To prevent the satellite from receiving the telecommands, a jammer transmits an interfering signal targeting the satellite ②. The combined signal is then received by the satellite, preventing the successful reception of the telecommands ③. This scenario also applies to the first or intermediate hops of a relay network which operates at the data-link layer or above.

3.2 Protocols

Due to the different link characteristics and requirements for each architecture, a number of different physical-layer satellite protocols have been developed. The three main protocols in current use are CCSDS Telemetry (used in the *downlink* architecture for government missions and scientific missions), Telecommand (used in the *uplink* architecture for control of the spacecraft), and DVB-S2 which is widely used for broadband and television and thus primarily broadcast via *relay*.

Whilst in both protocol families many of the specifics such as the choice of error correcting codes are left for the mission designer and operator to decide, nevertheless all of the protocols consist of common elements. Specifically, all of these protocols feature forward error corrected data blocks which encode the message, alongside a synchronization preamble which enables the receiver to

lock onto and begin decoding the message. Other optional protocol features include idle time which is implemented at the physical layer in CCSDS Telecommand, and physical layer signaling codes (PLSC) which communicate the parameters of the data block to allow link adaption during the mission in DVB-S2.

Applications provide data in the form of Transfer Frames which are then fragmented, packed, and padded into the physical-layer frames. Since the physical link is designed for a single transmitter only, access for multiple users or payloads is provided at the Transfer Frame level. Because only a single transmitter is expected, each protocol is laid out in a predictable structure, with each physical-layer frame being fixed length, back-to-back, and exhibiting exactly the same properties.

From the perspective of a protocol-aware jammer, this inherent predictability serves as a unique advantage. In the relay setting, where the jammer can continuously monitor their phase alignment with respect to the signal, synchronization can be maximally exploited. We are also interested in understanding the behavior of less synchronized threat actors.

4 Threat Model

The goal of the adversary is to deny service at the lowest possible power level. We are therefore primarily interested in targeting the error correcting code, which is critical for successfully receiving the data, or alternatively the synchronization preamble delimiting the frames. We assume that the protocol structure is known to the jamming adversary; where this is not apparent from publicly-available standards documents, recent work on the SpaceX Starlink protocol has demonstrated that reverse engineering the signals themselves is possible [26].

Intuitively, protocol knowledge can be exploited to a greater effect by adversaries which are fully synchronized to the victim signal. We are also interested in exploring the extent to which less synchronized jammers can exploit this knowledge. Thus we consider the following fundamental synchronization levels: *desynchronized*, in which no attempt to synchronize is made, *frame synchronized* in which regions of the protocol such as preambles can be jammed independently, and *synchronized* in which the jammer can lock on to the victim signal on a per-symbol basis.

We also consider the degree of knowledge about the data itself that the jammer can exploit in addition to the structure of the protocol. Whilst typically the victim message cannot be known beforehand, the jammer can have *full knowledge* of other predictable segments which have fixed, or nearly fixed, values. Whereas high levels of synchronization and knowledge are generally considered impractical in wireless systems [27], many satellite systems act as physical-layer relays, thus enabling precise synchronization to exploit this knowledge. This was discussed further in Subsection 3.1.2.

We also make a number of practical assumptions: that the attacker has access to Software Defined Radio (SDR) hardware alongside a suitable upconverter, amplifier, and antenna; and that all relevant protocol details including the frequency band, data rate, modulation scheme, error correcting code, protocol structure, and the presence of interleaving are known. The specifications for many satellites are publicly available, and can otherwise be reverse-engineered [26, 28].

5 Protocol-Aware Jammer Overview

A protocol-aware jamming attack proceeds as follows: the victim satellite and jammer both transmit a signal in the direction of the receiver, and are received relative power ratio JSR, with the channel introducing noise at the signal-to-noise power ratio SNR. These values are determined by physical-layer factors including the transmit power, antenna gain, physical distance between transmitter and receiver, the bandwidth, channel conditions, and multipathing effects. Further distortions such as multipathing are also present, but we consider these out of scope since they depend on the specifics of a given system and its environment.

The receiver synchronizes by correlating for the synchronization preamble, resulting in I/Q samples corresponding to physical-layer frames arriving at the demodulator and decoder. These physical-layer frames are finally unpacked into Transfer Frames. Thus the two fundamental stages at which failures can be induced are *modulation and coding* and *synchronization*: if either step fails, the Transfer Frame is not recovered. The overall effect of the protocol-aware jammer depends on how effectively these failures can be induced with respect to the protocol structure, including anti-jamming countermeasures, and under different capabilities.

In the following, we consider how a protocol-aware jammer can optimize performance, defined in terms of error rate per unit power, with respect to the protocol structure. We first show how the jammer can be optimized with respect to the two fundamental failure points: *modulation and coding* and *synchronization*. We justify this with respect to an analytic model that predicts the performance of the system when prior knowledge of the relevant waveform segment is available. We then introduce novel key techniques for exploiting these failure points within the protocol, even when the anti-jamming countermeasures of interleaving and adaptive coding and modulation are employed.

5.1 Modulation and Coding

Data recovery from the satellite channel fundamentally depends on the error correcting decoder successfully decoding the data. A jammer introduces errors when the received signal is sufficiently distant from its original position that the decoder cannot correct it. Thus the error rate in the presence of jamming depends strongly on the chosen modulation and coding of the system, as well as the parameters of the jammer waveform itself.

We consider two key cases: *full knowledge* where the jammer is aware of the transmitted message beforehand, and *zero knowledge* where the message is unknown. Whilst in general the data within the transmission cannot be known beforehand, the full knowledge case is realistic when considering predictable error-corrected headers.

5.1.1 Full Knowledge. We first consider the strongest adversary by assuming that the jammer knows the encoded message à priori, and is also synchronized to the message. Thus, the jammer is capable of arbitrarily manipulating the received location of the samples and can pick the ideal sequence of symbol shifts to cause denial of service. Whilst this technique is discussed in related works, to the best of our knowledge the performance characteristics have not been formalized [29].

Suppose the satellite transmits message m by encoding and modulating it into signal $\mathbf{s}_m = code(mod(m))$. The decoder succeeds if the received signal $\mathbf{r} = \mathbf{s}_m + \mathbf{j} + \mathbf{n}$ is closer to $\mathbf{s}_m$ than to any alternative signal $\mathbf{s}_{m'}$, where $m' \neq m$. The received signal consists of three components: the satellite signal $\mathbf{s}_m$, the jammer signal $\mathbf{j}$, and the channel noise $\mathbf{n}$.

Under optimum (Maximum-Likelihood) soft decoding, every signal is decoded to the nearest codeword in Euclidean space $\mathbb{R}^n$ [30]. Instead of canceling the signal, the ideal jammer strategy is instead to identify the message m' where $\mathbf{s}_{m'}$ is closest to $\mathbf{s}_m$, and construct $\mathbf{j}$ to shift from $\mathbf{s}_m$ to $\mathbf{s}_{m'}$.

We formalize this by deriving the distance between the received signal $\mathbf{r}$ and the error boundary between $\mathbf{s}_m$ and $\mathbf{s}_{m'}$, with respect to the channel noise power per symbol N_0/E_s, and jammer signal $\mathbf{j}$:

$$\text{dist}_{m\to m'}(\mathbf{j}, N_0/E_s) = \frac{\mathbf{d}\cdot\mathbf{j}}{||\mathbf{d}||_2} + \mathcal{N}(0, \frac{1}{2}N_0/E_s) - \frac{||\mathbf{d}||_2}{2} \quad \text{where } \mathbf{d} = \mathbf{s}_{m'} - \mathbf{s}_m \tag{1}$$

This expresses that the distance distribution is governed by three components: the length of the jammer signal as projected along $\mathbf{d}$, the noise distribution, and the shortest distance to the plane dividing $\mathbf{m}$ from $\mathbf{m}'$ which is half the length of $\mathbf{d}$.

The error probability is then given as follows:

$$\begin{aligned}\mathbb{P}_{m\to m'}(\mathbf{j}, N_0/E_s) &= P\left[\ \text{dist}_{m\to m'}(\mathbf{j}, N_0/E_s) > 0\ \right] \\ &= P\left[\frac{\mathbf{d}\cdot\mathbf{j}}{||\mathbf{d}||_2} + \mathcal{N}(0, \frac{1}{2}N_0/E_s) > \frac{||\mathbf{d}||_2}{2}\right]\end{aligned} \tag{2}$$

Clearly the error is maximized when the jammer component is projected along $\mathbf{s}_{m'} - \mathbf{s}_m$. Therefore jammer performance is the highest for protocols where the distance between $\mathbf{s}_m$ and $\mathbf{s}_{m'}$ is as small as possible. There are two factors which influence this distance: the Hamming distance of the code, and the layout of the constellation.

Weaker codes, which are characterized by smaller minimum Hamming distances, are therefore more vulnerable. Denser modulations, which are characterized by smaller average distances between constellation points, are also more vulnerable. The smallest possible distance between two codewords can then be found with respect to $\rho_{\min}$, the minimum equivalent power per bit within the constellation:

$$||\mathbf{s}_m - \mathbf{s}_{m'}||_2 = \sqrt{d_{\min}\cdot\rho_{\min}} \tag{3}$$

The ρ is given by the square of half the Euclidian distance between two points on the I/Q plot of the constellation, normalized by the number of bits. This can be interpreted as the minimum Jammer-to-Signal power ratio required, per bit, to deny service in the limiting case of zero receiver noise. In BPSK/QPSK, each bit is demodulated independently so only one power level is possible: $\rho_{min} = \rho_{max} = 0.00 / -3.01$ dB respectively. The bit mappings of denser constellations are not independent [31], leading to a range of possible power levels. For instance, QAM-256 has $\rho_{\min} = -22.30$ dB and $\rho_{\max} = 1.22$ dB. The values of ρ for the different constellation schemes standardized by CCSDS and DVB-S2 are provided in Appendix Table 3. Interestingly, whilst on average less power is required to jam denser constellations, the worst case can require more power. This is because, while the closest points in the constellation are closer, the furthest points are also further.

5.1.2 Zero Knowledge. Where the jammer does not know the encoded message beforehand, the best known jammer distribution is a pulsed jammer [6]. Such a jammer is defined by two key parameters, the average power P_J and pulse rate r. The signal alternates between the peak power level, calculated as P_J/r, and zero. In contrast to related works, in which fixed values of these parameters are evaluated, we are interested in finding the ideal parameters per modulation and code combination.

Additionally, whereas related works only consider pulsed Gaussian jammers, we consider the full range of symbol distributions possible depending on the synchronization capability of the jammer [6]. Specifically, when a jammer is desynchronized to the symbols they undergo an unpredictable rotation in I/Q space relative to the victim signal. In Figure 2 we illustrate this effect on the received symbol in I/Q space, with the hard decision boundary between the correct and incorrect symbols in gray. Since the contribution of the jammer's sample to the error rate depends only on the component in the direction between these symbols, it can be seen that much of the desynchronized jammer power is wasted in shifting the symbol in an orthogonal or opposite direction.

5.2 Receiver Synchronization

Alongside modulation and coding, the other fundamental failure point is synchronization. To successfully recover a frame, the receiver correlates the signal for the presence of a known preamble, and takes the highest correlation peak [32]. When a sequence of preambles is received, receiver lock is established so the receiver now only correlates for the highest peaks arriving with the correct timing. Therefore, despite being effective against other protocols, preamble spoofing is largely ineffective in denying service once receiver lock has been established [33]. We assume the strongest receiver, in which the jammer must destroy the existing preambles.

The correlation, which is implemented using a matched filter, can also be understood as minimizing Euclidean distance between the received signal $\mathbf{r}$ and the known preamble signal $\mathbf{p}$. The error probability is then given by modifying Equation 2:

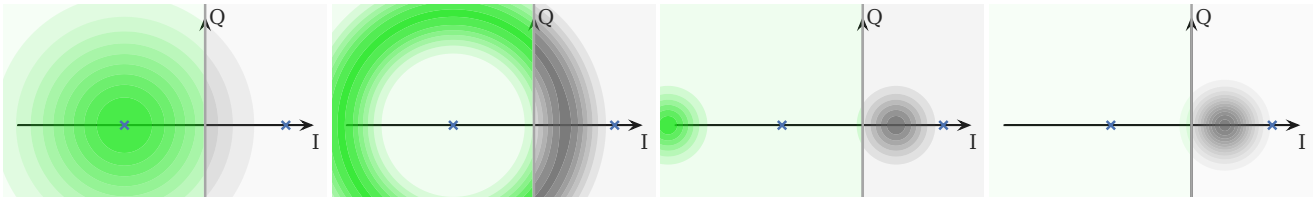
$$\mathbb{P}_e(\mathbf{j}, N_0/E_s, t) = P\left[\frac{-\mathbf{p}\cdot\mathbf{j}}{||\mathbf{p}||_2} + \mathcal{N}(0, \frac{1}{2}N_0/E_s) > \frac{||\mathbf{p}||_2}{2} - t\right] \tag{4}$$

Where t is the correlation threshold above which preamble detection succeeds.

Since the error rate is directly related to the component of the jammer signal in the direction of $-\mathbf{p}$, this confirms that the most effective jammer in this context is digital signal cancellation. Where the jammer is not synchronized, but instead frame synchronized, the preamble can instead be targeted by one of the jammer distributions from Figure 2. Entirely desynchronized jammers are unlikely to be effective against the preamble, which is by design more robust than the modulation and coding against continuous noise signals [32].

5.3 Protocol Structure

Treating the errors that occur at the decoder and synchronizer as building blocks, we now show how the ideal protocol-aware jammer can be constructed to take advantage of the structure of the protocol. Specifically, we account for the framing of the preamble and data segments and how Transfer Frames are packed into the physical-layer frames. We also consider the presence of interleaving



(a) Gaussian noise **(b) Desynchronized** **(c) Synchronized** **(d) Full knowledge**

Figure 2: IQ diagrams of the BPSK constellation; shading shows the effect caused by the jammer. The green region represents correct bits under hard demodulation. $Eb/N0 = 6$ dB**,** $J0/Eb = 3$ dB**.**

as an anti-jammer countermeasure. In each case, we find that the communication structure is sufficiently predictable and periodic that significant gains can be made.

5.3.1 Physical-layer frame layout. In addition to the error corrected data and preamble structures, the physical-layer frame may also consist physical-layer signaling codes (PLSC) and idle time. The average power requirements of a protocol-aware jammer are therefore determined not only by the vulnerability of each structure to jamming, but also by the ability of the jammer to predict the time of arrival of each structure, and the proportion of the time spent in each structure. We note that the CCSDS Telecommand, CCSDS Telemetry, and DVB-S2 protocols all exhibit a fixed physical-layer frame structure since satellite systems typically allocate a dedicated channel per transmitter. In contrast to random-access systems where multiple transmitters operate concurrently on a single channel, desynchronized pulsed jammers can also optimize for this by transmitting pulses at random within the time interval of a frame, tuning the pulse rate to compensate for the timing uncertainty.

We can analyze the possible jammer gains with respect to the *frame layout ratio* which expresses the proportion of time spent in each structure. When expressed in dB this is equivalent to the jammer performance gain for exploiting this knowledge. We calculate these ratios for a selection of CCSDS and DVB-S2 protocol variants in Table 1, considering the preamble, physical-layer signaling code (PLSC), and data region.

5.3.2 Transfer Frame Fragmentation. To obtain the final error performance experienced by applications, we finally consider how Transfer Frames of potentially variable lengths are fragmented, padded, and packed into the physical-layer frames [6]. Since the Transfer Frames contain an error-detecting checksum but lack error correction capability, the failure of just a single fragment contained within a physical-layer frame is sufficient to destroy the entire Transfer Frame. The performance then depends on the number of fragments which the Transfer Frame is split across. We express this as the codeword-to-frame ratio (CFR). Protocols with a higher CFR are more vulnerable to protocol-aware jamming, as proportionally fewer of the physical-layer frames need to be targeted in order to deny service.

We note in particular that a desynchronized periodic jammer should achieve similar performance to even a synchronized jammer. This is because Transfer Frame fragments are packed deterministically resulting in a periodic layout of vulnerable segments every CFR multiplied by the time period of a physical layer frame.

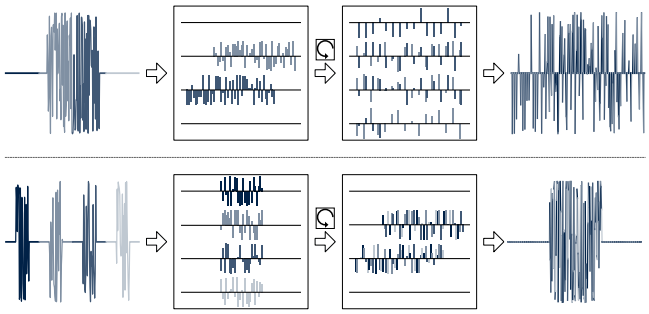


Figure 3: The effect of a deterministic row-column interleaver on two jamming signals, demonstrating its key weakness to protocol-aware jamming. Top: a naïve pulsed signal is spread out. Bottom: a protocol-aware waveform compensates for the interleaving effect, and is instead concentrated.

While the specific CFR differs per mission, we can evaluate the range of possible ratios based on the minimum and maximum possible values permitted by the standards. The minimum is clearly 1; we tabulate the maximum in Table 1 based on the maximum permissible Transfer Frame lengths from the CCSDS standards. Since DVB-S2 frames contain long data blocks and therefore do not often require fragmentation, for these we consider only $CFR = 1$.

5.3.3 Interleaving. To address the performance issues due to frame fragmentation, block-level interleaving schemes have been proposed which spread error bursts across multiple consecutive codewords [6]. These interleavers are designed to provide the maximum protection against burst errors by deterministically maximizing the spread of the symbols across long sequences of dependent physical-layer frames.

However, since the proposed interleaver algorithms are entirely deterministic, they can be undone by a synchronized jammer. The best performing interleaver is *row-column* which is implemented with a square buffer: data at the transmitter is read into the buffer in rows and read out in columns. The inverse operation is applied at the receiver. Whereas this spreads out a pulsed signal uniformly across multiple physical-layer frames, a jammer which transmits periodically according to the columns is concentrated by the interleaver back into a pulse, which can now more easily cause errors in a single physical-layer frame. This effect is illustrated in Figure 3, which plots the effect of a pulsed and deinterleaved signal passing through the row-column interleaver.

Table 1: Summary of the physical-layer frame layout of common satellite protocols, and the proportion of time spent in each structure. This corresponds to a gain in dB for frame-synchronized jammers which target only a particular structure. Where Codeword-to-Transfer Frame Ratio (CFR) is high, targeting just one codeword per frame is sufficient to deny service; this is possible for even desynchronized jammers. CFR is calculated using the maximum Telecommand Transfer Frame size of 1019+5 octets and maximum Telemetry Transfer Frame size of 65536 octets [34, 35]. † indicates that for DVB-S2, the ratio of time per frame segment depends on the constellation, since PLSC are $\pi/2$-BPSK modulated independent of the data modulation [36].

Protocol			Segments (*length* [bit] / *gain* [dB])			
Specification	Variant	CFR max.	Preamble	PLSC	Data	Total length
Telecommand *CCSDS 231.0*	PLOP-1	128× / −21.07 dB	64 bit / −8.45 dB	N/A	128 bit / −5.44 dB	448 bit
	PLOP-1	32× / −15.05 dB	64 bit / −10.41 dB	N/A	512 bit / −1.38 dB	704 bit
	PLOP-2	128× / −21.07 dB	64 bit / −7.10 dB	N/A	128 bit / −4.09 dB	328 bit
	PLOP-2	32× / −15.05 dB	64 bit / −9.60 dB	N/A	512 bit / −0.57 dB	584 bit
Telemetry *CCSDS 131.0*	$k=4096$ $r=1/2$	128× / −21.07 dB	64 bit / −21.11 dB	N/A	8192 bit / −0.03 dB	8256 bit
	$k=4096$ $r=2/3$	128× / −21.07 dB	64 bit / −19.87 dB	N/A	6144 bit / −0.05 dB	6208 bit
	$k=4096$ $r=4/5$	128× / −21.07 dB	64 bit / −19.08 dB	N/A	5120 bit / −0.05 dB	5184 bit
DVB-S2 *ETSI EN 302 308-1*	Normal frame	1× / 0 dB	26 symb / −31.02 dB	64 symb / −27.11 dB	64 800 bit / −0.05 dB	< 32 890 symb†
	Short frame	1× / 0 dB	26 symb / −24.98 dB	64 symb / −21.07 dB	16 200 bit / −0.07 dB	< 8190 symb†

We note that furthermore the row-column algorithm is *cyclic*: to be concentrated by the interleaver, the jammer needs only transmit in a duty cycle according to the columns; synchronization is not required. Provided that the duty cycle is maintained, even a fully desynchronized jammer can overcome the effects of the interleaver.

6 Evaluation

In Section 5, we considered how the data and preamble structures within the frame can be targeted by protocol-aware jammers in order to deny service. We then discussed how the overall waveform can be optimized with respect to the protocol structure and jammer synchronization capabilities. We now evaluate these techniques end-to-end against specific protocols, through simulations on software decoders and real-world experiments on a hardware receiver.

Throughout the analysis, Jammer-to-Signal Ratio (*JSR*), Signal-to-Noise Ratio (*SNR*), and Frame Error Rate (*FER*) are our primary metrics. The particular values of *JSR* and *SNR* can be easily derived for a particular context given aspects of the wireless environment, such as the antenna gain, transmit power, and distances between jammer and receiver. Whilst repeating the mathematics here is out of scope for this work, the process is identical as in the satellite spoofing context discussed in other works [2]. We also note that these metrics abstract over other specific aspects of the environment such as non-Gaussian noise components and local multipathing effects. Since these must be evaluated individually for each context, we consider this out of scope.

6.1 Simulations

We begin by evaluating the performance of a jammer optimized to target either the modulation and coding, or the synchronization structures within the frame; these are the fundamental points at which the jammer can induce failure. For each, we optimize the parameters of the jammer to maximize error performance under different synchronization capabilities.

6.1.1 Monte Carlo Simulation. We first generate a signal which targets the relevant structure. For modulation and coding, we generate a random binary message of size k which is then encoded into blocks of size n according to the chosen error correcting code. These blocks are then modulated into the chosen constellation. For receiver synchronization, we instead generate the preamble defined by the relevant CCSDS or ETSI standard document.

For each given jammer power P_J, we generate pulsed signals by varying the pulse rate $r \in [1/n, 1]$ according to the rates permitted by the number of symbols in the block. The jammer and victim signals are combined in a channel model, which adds a phase offset determined by the jammer's synchronization capability, and also −15 dB of channel noise relative to the signal[1]. Under desynchronization we consider the worst case phase alignment by offsetting the phase of each jammer symbol at random, for every symbol.

The resulting signal is finally processed by either a high performance soft demodulation and decoder, or a preamble correlator, both implemented in software [38]. Whereas the correlator is single-pass, soft demodulators are typically iterative algorithms. We select the "approximate min-star" run to 100 iterations for CCSDS codes in accordance with the simulations in the CCSDS standard documents, and 25 iterations for the DVB-S2 codes in accordance with common receiver implementations [39].

When simulating the decoder, we assume that the receiver is synchronized and locked onto the victim signal, meaning that any errors are solely due to decoder errors.

6.1.2 Modulation and Coding. The results of this analysis are graphed as heatmaps in Appendix Figure 6, which compares the error rates between a CCSDS telecommand code, a high rate CCSDS telemetry code, and a standard rate DVB-S2 code, under desynchronized and synchronized capabilities. The telecommand code is significantly more robust, with a code rate of 1/2, as compared to

[1]Noise values of −16 to −5 dB are typical for this sort of analysis [37]. We picked a −15 dB noise level to ensure that the weakest protocol still performs well, allowing us to comparatively assess the contribution of the jammer across protocols.

the others with a rate of 4/5; this indicates that 1/2 of the telecommand bits are redundant, as compared to 1/5 for the others. Taking the error rate maximizing parameters at each power level, we can find the ideal pulsed jammer for the synchronized and desynchronized cases. The ideal full knowledge jammer is bound by applying Equation 2 from Section 5.

Figure 4 (top) compares these error curves for each jammer capability under both BPSK (left) and QPSK (right), fixing the protocol as CCSDS Telecommand as an example. As expected, in general jammers with stronger capabilities are able to achieve greater performance. Interestingly, the synchronized jammer has almost identical performance to the desynchronized jammer under QPSK, whereas the synchronized jammer is $\sim$ 3 dB more effective against BPSK, roughly a 2× improvement in absolute terms. The reason for this can be seen in Figure 2: in BPSK a desynchronized jammer can shift orthogonally to the modulation scheme, whereas in QPSK every I/Q dimension is used and so this is not possible.

6.1.3 Synchronization. We now evaluate protocol-aware jamming strategies against the synchronization preamble by applying Equation 4 from Subsection 5.2. Unlike the data, the preamble is always known beforehand by design so we do not evaluate the zero-knowledge but synchronized capability.

In Figure 4 (bottom) we compare the JSR required to destroy the synchronization preamble defined across the different standards (left) and as modulated into different constellations (right). In contrast to CCSDS where the preamble is modulated along with the data, the DVB-S2 preambles are identical leading to variable and consistent performance respectively. The synchronized jammer gains are especially evident as compared to the desynchronized and Gaussian cases: the synchronized error rates consistently rise at $\sim$ 5 dB less power, and asymptotically approach 100 % error as opposed to 50 %. This is because, whereas the synchronized jammer can consistently destroy every preamble, a jammer with random phase shifts the received signal toward and away from the threshold with equal probability.

6.1.4 End-to-end Evaluation. Using these jammer performance characteristics derived for the data and preamble structures, we now calculate the expected jammer performance when applying the techniques which account for the protocol structure as described in Section 5.3. The key results are in Table 2, where we provide a performance comparison of optimized protocol-aware jammers against a selection of different protocols, covering CCSDS telecommand uplink, and CCSDS telemetry downlink, and DVB-S2 downlink. We go on to verify these values through real-world experiments in the following section.

The columns refer to different jammer strategies which increase in capability from left to right. The rows refer to different protocols, which are defined by the standard, code and minimum Hamming distance, Codeword-to-Frame ratio CFR, and preamble length d_{pre}. Within each row we consider jamming either code blocks or the preamble. Each cell contains both the Jammer-to-Signal power ratio required to achieve the given Frame Error Rate (FER) which is either approximately 100 % or 50 %[2], and the gain relative to the

[2]In this context, approximately is defined to within 1 %. This is necessary since the modulation and coding, and synchronization error rate curves asymptotically approach but never truly reach 0.5 or 1.

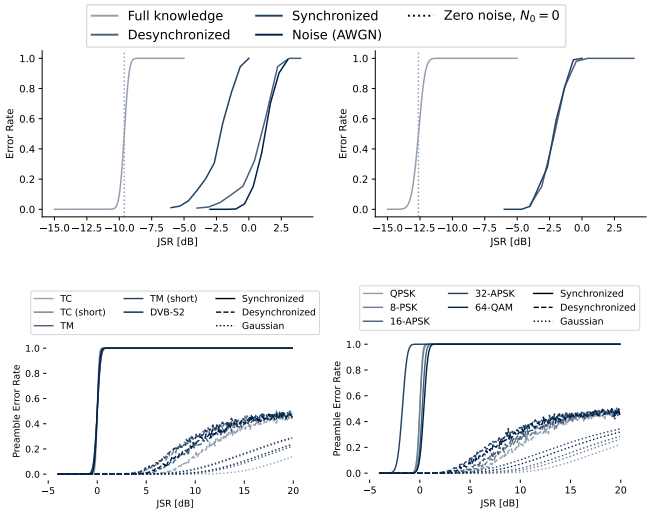


Figure 4: Top: Performance comparison of optimized jamming strategies against CCSDS TC $(128, 64)$ **code blocks, under BPSK (top left) and QPSK (top right). Bottom: Performance against the sync preamble, varying preamble type under BPSK (bottom left) and modulation scheme for the TM preamble (bottom right). Synchronized jammers achieve ideal performance.**

previous capability which is bracketed. We pay attention specifically to the values in bold, which highlight large gains of $>$ 3 dB and correspond to a power reduction of $>$ 2× in absolute terms. For consistent comparison, we set $CFR = 16$ as an example value for the CCSDS protocols, and leave $CFR = 1$ for DVB-S2 as justified in Subsection 5.3.2.

We note first of all that within the desynchronized capability, which makes no attempt to synchronize, selecting the optimal pulse rate and then deinterleaving leads to performance gains against the code blocks of 3.11 to 13.48 dB as compared to a Gaussian jammer. Of this, deinterleaving contributes 7.20 to 9.76 dB over the previously considered simpler pulsed signals [6]. We find that against the preamble it is essentially impossible to meaningfully cause errors, which typically requires $\sim$ 30 dB more power to cause an equivalent error rate. This is a worst-case analysis for the jammer since we consider the strongest receiver (see Subsection 5.2).

Under frame synchronization, where the jammer can target specific frame segments but is not synchronized to the symbol level, specific frame segments can be targeted in accordance with Table 1. This results in a 5.44 dB performance improvement for Telecommand (as seen in the *Frame Sync* column) which has a low frame layout ratio owing to the comparatively little time spent communicating the data. This same improvement applies to the preamble such that causing preamble errors is now feasible, but still requires more power than causing an equivalent error rate in the decoder.

Under synchronization, the power required to jam the preamble drops significantly given that the waveform of the preamble is already known. Additionally under Full Knowledge, where the code block is also known in advance, a similar performance improvement of at least 8.87 dB is seen. The target which maximizes performance

Table 2: Performance comparison of optimized protocol-aware jammers under different protocols and jammer capabilities, all values in dB. Two jammer objectives are considered in terms of the desired Frame Error Rate (FER): 99% and 50%. Bracketed values relative to previous cell; bold values draw attention to particularly significant results. † marks $d_{\min}$ estimate found by searching.

Protocol	Target	FER	Desynchronized			Frame sync	Synchronized	Full knowledge
			Gaussian	Pulsed Symb.	Deinterleaved			
CCSDS TC (128, 68) $CFR = 16$; BPSK $d_{\min} = 14$ [32]; $d_{\text{pre}} = 64$ bit	Code	∼100%	1.00 *(-)*	0.44 *(-0.56)*	-8.93 ***(-9.37)***	-14.37 ***(-5.44)***	-17.48 ***(-3.11)***	-26.35 ***(-8.87)***
	Code	∼50%	0.33 *(-)*	-2.22 *(-2.55)*	-11.98 ***(-9.76)***	-17.42 ***(-5.44)***	-20.54 ***(-3.12)***	-29.41 ***(-8.87)***
	Preamble	∼100%	- *(-)*	- *(-)*	- *(-)*	- *(-)*	-8.51 *(-)*	-8.51 *(+0.00)*
	Preamble	∼50%	52.94 *(-)*	27.94 ***(-25.00)***	27.94 *(+0.00)*	19.49 ***(-8.45)***	-11.57 ***(-31.05)***	-11.57 *(+0.00)*
CCSDS TM r = 4/5 $CFR = 16$; QPSK $d_{\min} = 27$ † [40]; $d_{\text{pre}} = 64$ bit	Code	∼100%	-4.85 *(-)*	-8.48 ***(-3.63)***	-15.68 ***(-7.20)***	-15.73 *(-0.05)*	-16.33 *(-0.60)*	-37.18 ***(-20.85)***
	Code	∼50%	-5.25 *(-)*	-9.09 ***(-3.84)***	-18.73 ***(-9.64)***	-18.78 *(-0.05)*	-19.39 *(-0.61)*	-40.24 ***(-20.85)***
	Preamble	∼100%	- *(-)*	- *(-)*	- *(-)*	- *(-)*	-21.15 *(-)*	-21.15 *(+0.00)*
	Preamble	∼50%	46.94 *(-)*	19.94 ***(-27.00)***	19.94 *(+0.00)*	0.85 ***(-19.08)***	-24.20 ***(-25.05)***	-24.20 *(+0.00)*
DVB-S2 r = 4/5 $CFR = 1$; QPSK $d_{\min} = 32$; $d_{\text{pre}} = 26$ symb	Code	∼100%	-4.89 *(-)*	-8.00 ***(-3.11)***	-8.00 *(+0.00)*	-8.05 *(-0.05)*	-8.17 *(-0.12)*	-29.67 ***(-21.50)***
	Code	∼50%	-5.00 *(-)*	-10.00 ***(-5.00)***	-11.05 *(-1.05)*	-11.10 *(-0.05)*	-11.23 *(-0.13)*	-32.73 ***(-21.50)***
	Preamble	∼100%	- *(-)*	- *(-)*	- *(-)*	- *(-)*	-30.17 *(-)*	-30.17 *(+0.00)*
	Preamble	∼50%	48.85 *(-)*	20.85 ***(-28.00)***	20.85 *(+0.00)*	-10.17 ***(-31.02)***	-33.23 ***(-23.05)***	-33.23 *(+0.00)*
DVB-S2 r = 9/10 $CFR = 1$; QPSK $d_{\min} = 32$; $d_{\text{pre}} = 26$ symb	Code	∼100%	-6.78 *(-)*	-10.89 ***(-4.11)***	-10.89 *(+0.00)*	-10.94 *(-0.05)*	-11.57 *(-0.63)*	-29.67 ***(-18.10)***
	Code	∼50%	-6.89 *(-)*	-9.89 ***(-3.00)***	-13.94 ***(-4.05)***	-13.99 *(-0.05)*	-14.62 *(-0.63)*	-32.73 ***(-18.11)***
	Preamble	∼100%	- *(-)*	- *(-)*	- *(-)*	- *(-)*	-30.17 *(-)*	-30.17 *(+0.00)*
	Preamble	∼50%	48.85 *(-)*	20.85 ***(-28.00)***	20.85 *(+0.00)*	-10.17 ***(-31.02)***	-33.23 ***(-23.05)***	-33.23 *(+0.00)*

is the preamble for DVB-S2, and the code block for the CCSDS protocol variants.

6.2 Real-world Experiments

Until this point, we have used software simulations to evaluate system performance. We now validate the applicability of these simulations to predict the actual performance of a hardware receiver implementation in the real world.

6.2.1 Experiment Setup. Our hardware testbed consists of two USRP N210 SDRs, one representing the satellite and the other the jammer, connected to a DVB-S2 satellite television. We installed a DC blocker and 30 dB attenuator between the SDR and television to avoid damage to the circuit [41]. The SDRs are connected by a MIMO cable, and so can operate desynchronized under independent clocks or synchronized under the same clock.

The experiment proceeds as follows: a clean physical layer DVB-S2 waveform is generated which represents the victim signal, and mixed with channel noise. This signal encodes an MPEG stream containing a 440 Hz sine wave. We identify successful jamming by correlating for this frequency in the television's audio output over a 1 s measurement.

For each jammer type and tested modulation and coding, we binary search over the jammer-to-signal power levels *JSR* to find the threshold at which signal loss is observed. We test both $-\infty$ and -15 dB of added noise to match the simulations in Subsection 6.1. For each combination, we repeat each 1 s measurement 10 times, aiming for a 100 % error rate. We allow the receiver to reacquire "locked" state every time the signal is lost. The television states of signal loss can also be seen visually, shown in the Appendix Figure 7.

6.2.2 Results. The results of this analysis are plotted in Figure 5, in which we compare the power level required to deny service for each capability, broken down by the different jammer capabilities. The different colored bars represent modulation and coding variants; the vertical red lines compare the performance predicted by the simulations. Solid bars are zero noise, and the hashed bars are -15 dB of added noise. As expected, the high-precision software decoder outperforms the hardware receiver, since it fails at a higher JSR power level than the hardware.

The simulated performance for the synchronized jammer, which was derived from the analytic theory from Subsection 5.1.1, matches the performance of the synchronized jammer to a high precision. The preamble jamming is marginally more effective than PLSC data jamming, which accords with Table 2. For the other jammer classes, the required power to achieve jamming is higher in simulation than against the hardware. These experiments confirm that in all cases, the jammer can achieve significant performance improvements of at least 15 dB by optimizing for the protocol structure, and that this performance is worse or the same as the simulations suggest.

7 Countermeasures

We have found significant improvements in jammer performance against all major classes of space protocols, and under all jammer capabilities by exploiting the predictable and repeating underlying structure of the protocol. Although jamming attacks can never be truly prevented, nevertheless by increasing the unpredictability of the signal the performance gains of protocol-aware jamming can be reduced.

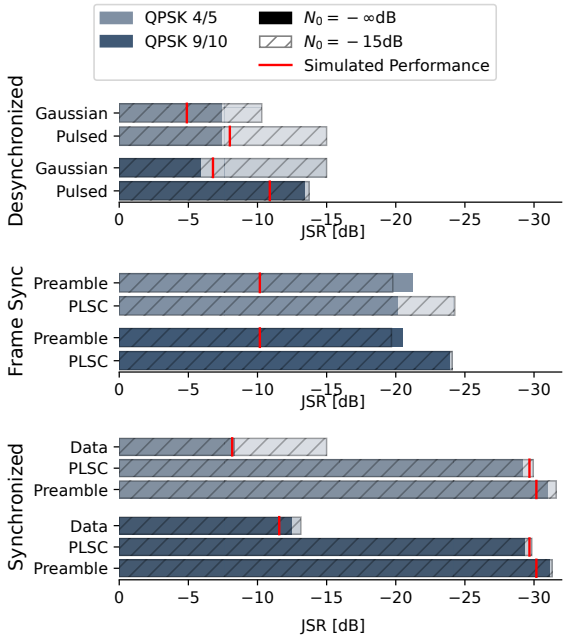


Figure 5: Real-world DVB-S2 performance comparison under desynchronized, frame synchronized, and synchronized jammer capabilities. Values are Jammer-to-Signal ratio in dB; lower (longer bar) is a more performant jammer. Different colors distinguish different choices of modulation and coding, striped bars have −15 dB of noise. Within each capability, significant performance gains can be made; the vertical dotted line shows the predicted threshold under optimal SOF jamming.

7.1 Current Countermeasures

7.1.1 Jammer State Information. Decoder performance can be improved in the presence of jamming by including information about the likely state of the jammer in each sample. It is generally considered that the ideal situation is when the receiver can accurately estimate the variance of the jammer's signal [6]. This has been found to improve the performance of the receiver in pulsed noise jamming channels, but there remain open questions over the level of improvement that could be expected from a synchronized jammer which does not have to transmit Gaussian samples. Furthermore, we see in Table 2 that the largest gains are to be made by exploiting the protocol structure: this is still possible even if JSI is applied to each individual codeblock.

7.1.2 Cryptographic Spread Spectrum. In cryptographic spread spectrum, the spreading sequence is determined via a shared secret; several works have considered its application to securing space links [42, 43]. In addition to making the signal difficult or impossible to detect by those without the spreading code, it has been shown that the operation of despreading causes the jammer samples to be reduced to a Gaussian distribution [6]. Whilst this is a helpful mechanism, we again note that the primary contributor to protocol-aware jamming gains is not the jammer distribution but rather the ability to predict the timing of the signal structure. This is still possible under cryptographic spread spectrum if the underlying protocol is periodic and predictable.

7.1.3 Secure Link Adaption. In principle adaptive coding and modulation abilities provide a level of defence against jammers, since the link can be adapted dynamically to match the current channel conditions. DVB-S2 is an example of a protocol which supports adaptive configurations. However, adaptive systems are required to communicate the channel condition in-band, which can therefore be targeted by the jammer. Our experiment results in Figure 5 show that targeting the PLSCODE of DVB-S2 yields high performance under both *Frame Synchronized* and *Synchronized* capabilities. Furthermore, a recent work has shown that implementing link adaption can open the system to attacks through the feedback channel [44].

7.2 Cryptographic Interleaving

In order to mitigate the gains possible due to awareness of the protocol structure, we propose the application of a cryptographic interleaver. In contrast to the deterministic row-column interleaver design (see Figure 3), this pseudo-randomly scrambles the bits. Cryptographic interleaving in this manner has been shown to be effective in the mitigation of protocol-aware jamming in other wireless protocols, as well as to provide a degree of data secrecy [9, 45]. Provided that the scrambling sequence is sufficiently long to cover all physical-layer frames which convey all fragments of a Transfer Frame, this completely prevents a jammer from exploiting the internal structure of the protocol.

Our results in Table 1 and Figure 5 enable us to assess the performance of this countermeasure by comparing jammers which cannot deinterleave, the *Pulsed Symbols* capability, to the *Synchronized* capability. We see that the robustness of the system can be improved by at least 18 dB in all assessed protocols in simulation, and 15 dB from the hardware experiments.

8 Conclusion

We have demonstrated that protocol-aware jamming attacks are a plausible threat against space communications which can exploit the cyclic and predictable nature of the protocol to deny service at significantly reduced power levels as compared to conventional jamming. We assessed CCSDS Telemetry and Telecommand protocols, as well as DVB-S2, across the three major architectures of uplink, downlink, and relay satellite systems and demonstrated that at least 15 dB of jammer performance improvements are present across all tested classes. This represents a significant shift in the threat model of current satellite jamming and anti-jamming literature, which ubiquitously assumes protocol-unaware classes. We validated our approach through real-world experiments on a hardware DVB-S2 receiver, and found that the real system performed worse or the same against all attack classes, as compared to the simulated values. These results underline the risks of designing protocols and receivers with only a Gaussian noise model in mind.

In conclusion, the findings of this study underscore the significant threat posed by protocol-aware jamming attacks on satellite communications and highlight the need for countermeasures to mitigate vulnerabilities inherent in standardized space protocols.

References

[1] Johannes Willbold, Moritz Schloegel, Robin Bisping, Martin Strohmeier, Thorsten Holz, and Vincent Lenders. 2024. VSAsTer: Uncovering Inherent Security Issues in Current VSAT System Practices. In *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 288–299.

[2] Edd Salkield, Marcell Szakály, Joshua Smailes, Sebastian Köhler, Simon Birnbach, Martin Strohmeier, and Ivan Martinovic. 2023. Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 341–352.

[3] Samuel Lefcourt, Nathaniel Gordon, Hanting Wong, and Gregory Falco. 2022. Space cognitive communications: Characterizing radiofrequency interference to improve digital space domain awareness. In *2022 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 1–7.

[4] Ryan H Mitch, Ryan C Dougherty, Mark L Psiaki, Steven P Powell, Brady W O'Hanlon, Jahshan A Bhatti, and Todd E Humphreys. 2011. Signal characteristics of civil GPS jammers. In *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, 1907–1919.

[5] Marco Baldi, Franco Chiaraluce, Roberto Garello, Nicola Maturo, I Aguilar Sanchez, and Stefano Cioni. 2015. Analysis and performance evaluation of new coding options for space telecommand links-Part I: AWGN channels. *International Journal of Satellite Communications and Networking*, 33, 6, 509–525.

[6] Marco Baldi, Franco Chiaraluce, Roberto Garello, Nicola Maturo, I Aguilar Sanchez, and Stefano Cioni. 2015. Analysis and performance evaluation of new coding options for space telecommand links–part II: jamming channels. *International Journal of Satellite Communications and Networking*, 33, 6, 527–542.

[7] Nele Noels and Marc Moeneclaey. 2017. Performance of advanced telecommand frame synchronizer under pulsed jamming conditions. In *2017 IEEE International Conference on Communications (ICC)*, 1–6. doi:10.1109/ICC.2017.7996555.

[8] Nele Noels and Ignacio Aguilar Sánchez. 2019. Towards improved satellite telecommand link availability. *International Journal of Satellite Communications and Networking*, 37, 4, 360–369.

[9] Guolong Lin and Guevara Noubir. 2005. On link layer denial of service in data wireless LANs. *Wireless Communications and Mobile Computing*, 5, 3, 273–284.

[10] Triet Dang Vo-Huu, Tien Dang Vo-Huu, and Guevara Noubir. 2016. Interleaving jamming in Wi-Fi networks. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec)*, 31–42.

[11] Matthias Wilhelm, Ivan Martinovic, Jens B Schmitt, and Vincent Lenders. 2011. Short paper: Reactive jamming in wireless networks: How realistic is the threat? In *Proceedings of the fourth ACM conference on Wireless network security*, 47–52.

[12] Thomas Kraus, Roland Bauernfeind, and Bernd Eissfeller. 2011. Survey of in-car jammers-analysis and modeling of the RF signals and IF samples (suitable for active signal cancelation). In *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, 430–435.

[13] Beatrice Motella, Simone Savasta, Davide Margaria, and Fabio Dovis. 2011. Method for assessing the interference impact on GNSS receivers. *IEEE Transactions on Aerospace and Electronic Systems*, 47, 2, 1416–1432.

[14] David L Adamy. 2021. *EW 105: Space Electronic Warfare*. Artech House.

[15] Akshay Kashyap, Tamer Basar, and R Srikant. 2004. Correlated jamming on MIMO Gaussian fading channels. *IEEE Transactions on Information Theory*, 50, 9, 2119–2123.

[16] RJ McEliece and WE Stark. 1981. An information theoretic study of communication in the presence of jamming. In *ICC 1981; International Conference on Communications, Volume 3*. Vol. 3, 45–3.

[17] Shlomo Shamai and Sergio Verdu. 1992. Worst-case power-constrained noise for binary-input channels. *IEEE Transactions on Information Theory*, 38, 5, 1494–1511.

[18] Suat Bayram, N Denizcan Vanli, Berkan Dulek, Ilhan Sezer, and Sinan Gezici. 2012. Optimum power allocation for average power constrained jammers in the presence of non-Gaussian noise. *IEEE Communications Letters*, 16, 8, 1153–1156.

[19] SaiDhiraj Amuru and R Michael Buehrer. 2015. Optimal jamming against digital modulation. *IEEE Transactions on Information Forensics and Security*, 10, 10, 2212–2224.

[20] SaiDhiraj Amuru and R Michael Buehrer. 2014. Optimal jamming strategies in digital communications—Impact of modulation. In *2014 IEEE Global Communications Conference*. IEEE, 1619–1624.

[21] 2023. TM SYNCHRONIZATION AND CHANNEL CODING. CCSDS. (Sept. 2023). Retrieved May 14, 2025 from https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01//131x0b5.pdf.

[22] Dan Veeneman. 2021. IRIDIUM CERTUS Technical Details. Retrieved: 2023-10-04. Decode Systems, (2021). http://www.decodesystems.com/iridium.html.

[23] 2021. TC SYNCHRONIZATION AND CHANNEL CODING. CCSDS. (July 2021). Retrieved May 14, 2025 from https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01//231x0b4e1.pdf.

[24] Alan Grant, Paul Williams, Nick Ward, and Sally Basker. 2009. GPS Jamming and the Impact on Maritime Navigation. *The Journal of Navigation*, 62, 2, 173–187. doi:10.1017/S0373463308005213.

[25] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. 2011. On the Requirements for Successful GPS Spoofing Attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (CCS '11). Association for Computing Machinery, Chicago, Illinois, USA, 75–86. ISBN: 9781450309486. doi:10.1145/2046707.2046719.

[26] Todd E Humphreys, Peter A Iannucci, Zacharias Komodromos, and Andrew M Graff. 2022. Signal Structure of the Starlink Ku-Band Downlink. *arXiv preprint arXiv:2210.11578*.

[27] Daniel Moser, Vincent Lenders, and Srdjan Capkun. 2019. Digital radio signal cancellation attacks: an experimental evaluation. In *Proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 23–33. http://lenders.ch/publications/conferences/wisec19_1.pdf.

[28] Johannes Willbold, Franklyn Sciberras, Martin Strohmeier, and Vincent Lenders. 2024. Satellite cybersecurity reconnaissance: Strategies and their real-world evaluation. In *2024 IEEE Aerospace Conference*. IEEE, 1–13.

[29] Norbert Ludant and Guevara Noubir. 2021. SigUnder: a stealthy 5G low power attack and defenses. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 250–260.

[30] Claude E Shannon. 1959. Probability of error for optimal codes in a Gaussian channel. *Bell System Technical Journal*, 38, 3, 611–656.

[31] Jon Hamkins. 2010. Performance of low-density parity-check coded modulation. In *2010 IEEE Aerospace Conference*. IEEE, 1–14.

[32] TM Synchronization. 2021. CCSDS 230.1-G-3: Channel Coding—Summary of Concept and Rationale. *Report Concerning Space Data System Standard. Informational Report CCSDS*.

[33] Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic. 2023. Brokenwire : Wireless Disruption of CCS Electric Vehicle Charging. In *30th Annual Network and Distributed System Security Symposium NDSS, 2023*.

[34] 2021. TC SPACE DATA LINK PROTOCOL. CCSDS. (Oct. 2021). Retrieved May 14, 2025 from https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01/232x0b4e1c1.pdf.

[35] 2021. TM SPACE DATA LINK PROTOCOL. CCSDS. (Oct. 2021). Retrieved May 14, 2025 from https://ccsds.org/wp-content/uploads/gravity_forms/5-448e85c647331d9cbaf66c096458bdd5/2025/01/132x0b3.pdf.

[36] ETSI Standard EN. 2014. 302 307-1 V1.4.1: Digital Video Broadcasting (DVB). *Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2), European Telecommunications Standards Institute, Valbonne, France*.

[37] European Telecommunications Standards Institute. 2014. EN 302 307-1 - V1.4.1 - Digital Video Broadcasting (DVB); Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications; Part 1: DVB-S2. Tech. rep. EN 302 307-1 V1.4.1. European Telecommunications Standards Institute, 1–80.

[38] Daniel Estévez. 2023. ldpc-toolbox: A Rust crate with utilities to aid in LDPC code design. https://github.com/daniestevez/ldpc-toolbox. Accessed: 2025-05-14. (2023).

[39] Ahmet Inan. 2018. LDPC: Playing with Low-density parity-check codes. https://github.com/xdsopl/LDPC. Accessed: 2025-03-15. (2018).

[40] Brian K Butler and Paul H Siegel. 2013. Bounds on the minimum distance of punctured quasi-cyclic LDPC codes. *IEEE Transactions on Information Theory*, 59, 7, 4584–4597.

[41] 2017. Transmitting DVB-S2 with GNU Radio and an USRP B210. Ettus Research. Retrieved Dec. 11, 2023 from https://kb.ettus.com/Transmitting_DVB-S2_with_GNU_Radio_and_an_USRP_B210.

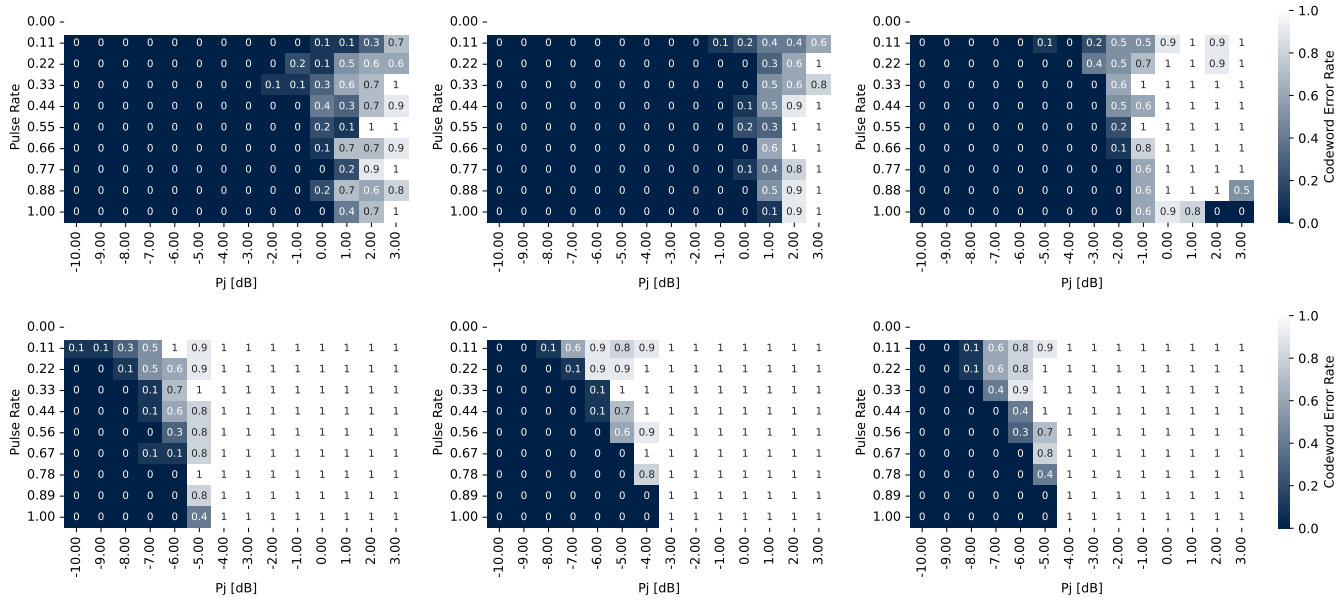
[42] Ignacio Aguilar Sanchez. 2012. On the protection of future telecommunication mission operations. In *2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*. IEEE, 1–6.

[43] L. Simone, G. Fittipaldi, and I. Aguilar Sanchez. 2011. Fast acquisition techniques for very long PN codes for On-Board Secure TTC transponders. In *2011 - MILCOM 2011 Military Communications Conference*, 1748–1753. doi:10.1109/MILCOM.2011.6127563.

[44] Edd Salkield, Sebastian Köhler, Simon Birnbach, and Ivan Martinovic. 2024. Security risks of adaptive coding and modulation in space systems. In *2024 Security for Space Systems (3S)*. IEEE, 1–10.

[45] Triet D Vo-Huu and Guevara Noubir. 2015. Mitigating rate attacks through crypto-coded modulation. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 237–246.

Appendix



(a) Gaussian (b) Desynchronized (c) Synchronized

Figure 6: The effect of a pulsed jamming strategy on individual FEC Codewords under zero knowledge jamming, as jammer power *JSR* and Pulse Rate vary; lighter color is a higher error rate indicating jammer success. Top: *CCSDS 231.0* Telecommand with code rate $r = 1/2$ and modulation BPSK; bottom: *CCSDS 232.0* Telemetry with code rate $r = 4/5$ and modulation QPSK. Pulsed jamming strategies cause the highest error rates at the lowest JSR with the exception of a desynchronized jammer against telecommand (top left), which uses a highly robust code. This aligns with previous pulsed jammer analysis [6].

Table 3: The minimum and maximum equivalent power per bit for various constellation types defined for space protocols, and the required Jammer-to-Signal power ratio to target these bit flips. As expected, denser constellations require less power to jam on average, but interestingly the maximum power may go up depending on the specific selected bits within the constellation.

	BPSK	QPSK	8-PSK	8-APSK	16-APSK	32-APSK	16-QAM	64-QAM	128-QAM	256-QAM
$\rho_{\min}$ [dB]	0.00	-3.01	-8.34	-14.14	-11.89	-16.01	-10.00	-16.23	-26.02	-22.30
ρ_{avg} [dB]	0.00	-3.01	-4.59	-4.39	-5.77	-6.72	-5.81	-7.59	-8.15	-8.87
$\rho_{\max}$ [dB]	0.00	-3.01	-0.69	2.51	0.76	1.89	-0.46	0.67	1.94	1.22

Figure 7: The satellite TV in three states: receiving a clear signal, approaching the limit of signal loss, and signal loss.

Acknowledgments

We would like to thank armasuisse Science and Technology for their support. Sebastian was supported by the Royal Academy of Engineering and the Office of the Chief Science Adviser for National Security under the UK Intelligence Community Postdoctoral Research Fellowships programme. Simon was supported by the Government Office for Science and the Royal Academy of Engineering under the UK Intelligence Community Postdoctoral Research Fellowships scheme.