SideDish: Low-Cost Anti-Spoofing Countermeasure for Satellite Data Communications

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

Louis-Emile Ploix
louisemile.ploix@gmail.com
University of Oxford
Oxford, United Kingdom

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

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

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

Abstract

Satellite systems are increasingly vulnerable to spoofing attacks at the physical layer, where adversaries use inexpensive radio equipment to interfere with and replace legitimate signals. While cryptographic countermeasures are common in other wireless systems, their adoption in new space programs is slow due to concerns about the associated implications on robustness, cost, weight, power, and the challenges of updating existing systems.

In this paper we introduce SideDish, a novel anti-spoofing countermeasure that combines a secondary receiver colocated at the satellite receiver with decoded signal comparison to detect out-of-beam unauthentic interference. The system is retrofittable into existing ground station deployments, cheap by using only low-cost components, and is robust against denial of service attacks.

We verify this through simulations and real-world experiments that show SideDish spatially constraints attackers by between 70 % to 99.84 % in the angular domain, even considering scattering effects of the primary antenna. Targeting SideDish to deny service is not feasible within practical constraints, requiring microsecond-order timing accuracy to overcome.

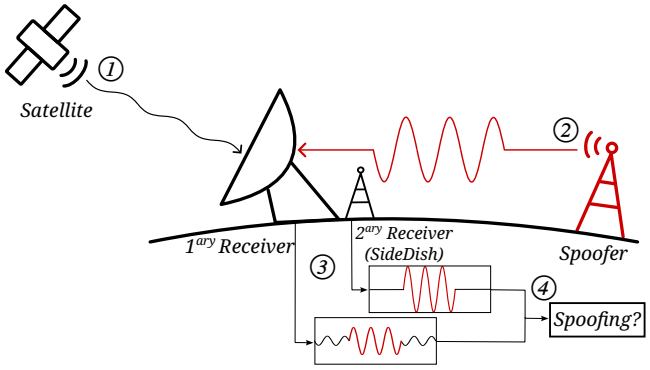


Figure 1: SideDish when faced with a spoofing attack. The satellite (1) transmits a downlink signal which arrives coincident with out-of-beam spoofing signal (2). To overshadow the primary receiver, the spoofer must compensate for both the antenna gain effects and the presence of the existing signal, so it is received at the secondary receiver at higher power (3). The Spoofing/Not Spoofing decision is made by comparing the decoded data from these two signals (4).

1 Motivation

Today, satellite systems are increasingly depended upon as critical infrastructure, providing communication, navigation, and observation services within civil, scientific, and government applications. Therefore, these systems are increasingly valuable targets for attacks, with recent examples including the remote disabling of satellite modems in the war in Ukraine [15], the hijacking of DVB-S2 (television and data signals) for propaganda distribution [16], and the over 310,000 flights affected by GPS spoofing in 2024 [25]. These and other systems are widely vulnerable to unsophisticated wireless spoofing attacks, which are enabled by a lack of cryptographic authentication at the data link layer [2], and open the door for further attacks against downstream systems which rely upon their data [21]. It has been shown that satellite data downlink signals are especially at risk from ground-based attackers, which do not have to maintain presence within the satellite receiver's line of sight and can be equipped with cheap off-the-shelf equipment.

Although cryptographic authentication is now ubiquitous in other wireless systems, many space programs remain slow to adopt these security measures where the risk and impact of wireless interference is understood to be outweighed by the implications on mission cost and robustness, launch weight, and power budget.

This is leading to both new and old systems which are set to remain vulnerable throughout long mission lifespans, even as the threat landscape is rapidly shifting. As a result, satellite spoofing attacks have received significant academic interest in applications including hijacking VSAT [2], television [6], and Earth observation systems [21]. Spoofing is a particular threat against dedicated ground stations equipped with highly directional antenna dishes, which are centralized, stationary targets where adversaries can disrupt many satellites. Whilst antenna directionality arguably provides an elementary level of authentication since attackers positioned out of the main beam must compensate with higher power (an increased capability), the benefit is small since RF amplifiers are cheaply available [22]. Currently-available signal monitoring solutions are highly sophisticated and able to monitor interference across a wide bandwidth, but are orders of magnitude more expensive than the unsophisticated strategies and cheap hardware sufficient to spoof these systems.

In this paper, we introduce SideDish, a retrofittable and cheap spoofing detection system for satellite downlink communications. This system can provide a form of authentication as part of a wider system that rejects data classified as spoofing, even in the absence of cryptographic measures. The system consists only of cheaply available components installed at the ground station: an omnidirectional secondary antenna colocated with the directional satellite dish, connected to a secondary receiver system (cf. Figure 1). By comparing the data decoded by the primary and secondary receivers, out-of-beam spoofing attempts can be identified and rejected without requiring any custom signal processing techniques. This upgrades authenticity from the rudimentary level arguably provided by the directional dish alone by requiring the attacker either operate in the direct line of sight between the satellite and ground station, or else with two coordinated transmitters at carefully chosen locations.

We provide both a theoretic and real-world analysis of this countermeasure, paying particular attention to attacks which target the countermeasure to deny authentication. Our evaluation considers the system end-to-end using high-precision antenna gain measurements from a near-field range, an extensive parameter search of protocol decoder behavior under different overshadowing conditions, and results from spoofing experiments in a real-world urban environment. Our results show that SideDish spatially constrains the attacker such that spoofing is detected for 70 % to 99.84 % of possible attacker positions. Denial of authentication attacks are not feasible within practical constraints as the receiver system is precise enough to bound the expected timestamps of decoded signals.

2 Related Work

Retrofittable authentication for legacy wireless systems is commonly required when protocol-level cryptographic authentication is unavailable or can not be introduced for compatibility constraints. For satellite, and particularly GNSS systems, the most relevant prior work in this area can be grouped into three broad categories: (a) *single receiver signal-observable methods*, (b) *angular domains security methods*, and (c) *auxiliary-sensor and EMI-inspired methods*.

2.1 Single-receiver Signal-observable Methods

A first line of work detects spoofing by monitoring quantities already exposed by commodity receivers such as lock state, received power, Doppler shift, or other demodulator observables [18, 3]. More advanced signal analysis for this purpose includes correlation-shape monitoring, statistical hypothesis tests, signal-quality monitoring, fingerprinting, and signature-based techniques (cf. [10] for an overview). For instance, the multiple-access nature of the channel has been used to detect multiple carrier signals using the same code sequence, the predictability of both message contents and timing to verify receiver signals, and the comparison of the computed location from multiple nearby receivers [27]. Ranganathan et al. showed that the presence of multiple carrier signals can be used to determine spoofing in a GNSS setting [19]

Adams et al. [1] specifically consider operational RF interference monitoring at satellite ground stations. They show that persistent monitoring can characterize the local interference environment and distinguish likely RFI from legitimate downlink activity using features such as center frequency and cross-polarization ratio.

The broader GNSS literature contains many examples of such defenses, but as shown by prior work, a sufficiently capable adversary can match expected signal characteristics, transmit before receiver lock is established, or perform a seamless takeover of the receiver state [27]. SideDish differs from these systems by relying not on signal characteristics extracted from a single receiver, but instead on a secondary receiver colocated with the ground station. For a full overview of this popular research area, we refer to [23].

2.2 Angular-domain Security Methods

A second family of defenses exploits spatial information, aiming to address seamless takeovers by monitoring for signal characteristics that indicate transmission at an unexpected incident angle. Security is provided by defining angular-domain bounds for the authentic signal, thus restricting the viable attacker locations. This security approach is well-established, for instance in directional modulation schemes such as Antenna Subset Modulation, which provide secrecy against eavesdropping attackers operating outside of a specified angular domain [29, 12].

Angular-domain security methods can be classified into Angle of Arrival (AoA) and Time Difference of Arrival (TDoA).

Typical AoA methods compare the received signal power from multiple different antennas. In Amplitude Comparison Monopulse, multiple antenna gain patterns are considered together, with the power level asymmetry between them used to determine the signal direction [4, 11]. SideDish similarly compares the relative gain of the signal received between the directional dish and a single omnidirectional secondary antenna. However, a disadvantage of this approach is that location misclassification can be caused if the attacker can replay the signal from a different direction at a controlled power, leading to denial of authentication. MUSIC (Multiple Signal Classification) can be used to overcome this challenge by using an antenna array to search for steering vectors that lie in the subspace for each signal, thereby improving AoA measurement [4]. SideDish instead overcomes this challenge with reduced complexity through TDoA-based filtering.

In TDoA, the received signal time is compared at multiple antenna positions to determine the AoA. The use of TDoA for satellite authenticity has been shown for GNSS using multiple omnidirectional antennas [13]. Commercial TOoA solutions for other signals are available off-the-shelf [20]. Since colocating satellite ground stations is challenging, Jedermann et al., proposed orbit-based authentication in which geographically distributed receivers compare measured time differences against the expected satellite orbit [9]. However, the wide geographical separation opens the system to attacks by distributed and synchronized attackers [24, 14]. SideDish overcomes these challenges by co-locating an omnidirectional receiver with the ground station, making it challenging to attack the two antennas separately, and using TDoA to distinguish attackers intentionally targeting only the secondary receiver.

2.3 Auxiliary Sensors and EMI inspired Methods

The principle of introducing a secondary receiver for the detection and suppression of interference has long been considered in the field of radar and EMI. Prior works study external interference suppression such as coherent sidelobe cancellation by exploiting the

directional properties of interfering signals [5]. These approaches typically use a main antenna (or array) to capture the desired radar returns together with self- and external interference, and an auxiliary antenna to estimate only the external interference. Certain advanced ground stations for satellite systems use a secondary receiver for auto-tracking, but this is intended purely as a dish-pointing method rather than a countermeasure.

In 2020, Zhang et al. investigated a version of this countermeasure that requires few additional components, randomizing when the sensor is powered and measuring readings in the unpowered state [32]. Similarly, Tu et al. demonstrated how a second, identical dummy sensor can be used to detect EMI attacks [28]. In the GNSS context, Jansen et al. [8] examine the detection of GPS spoofing using multiple receivers positioned within 5 meters. For a full systemization, we refer the reader to [30]. Whilst similar in principle, these countermeasures rely on an identical co-located receiver, and do not distinguish the signal based on its angle-of-arrival. SideDish is similar in its use of a secondary sensor to detect the attack signal while remaining unaffected by the legitimate measurement.

3 Principles of Wireless Overshadowing

Against satellite data systems, spoofing attacks are conducted by wireless overshadowing in which the attacker's signal contends with the interference of a pre-existing signal. If the attacker's signal is of sufficiently high power, the receiver lock is captured and the attacker's data decoded. Against high data rate downlinks, which ubiquitously use highly directional antennas to maximize bandwidth, attackers operating out of the main beam must also contend with the resulting attenuation. Prior work has shown that a lower bound on the required attacker power to overshadow can be derived, and that these requirements are easily met through cheaply available radio hardware [22].

Suppose the victim satellite signal is incident to the antenna at power P_v, and the attacker at P_a, expressed in dB W. The power of the victim and attacker signals as they reach the primary and secondary demodulators are affected by $G(\theta, \phi)$, the gain pattern of the antenna. This is a function of the transmitter position relative to the dish expressed in spherical coordinates, with respect to polar angle θ and azimuthal angle ϕ. In-beam signals are amplified by $G(0, 0)$.

From the attacker's perspective, their signal as incident to the receiver front end contends with interference that consists of both the victim signal of power $P_v + G(0, 0)$, and the thermal noise of the receiver of power N_0. The interference power is therefore expressed $P_I = (P_v + G(0, 0)) \oplus N_0$, where $\oplus$ denotes addition in linear space.

The power to overshadow depends not only on the total interference power, but also on the proportion of victim power to noise power. The *overshadow factor*, $\gamma(P_v + G(0, 0) - N_0)$, describes this attacker-to-interference power ratio required to overshadow a given victim signal-to-noise power ratio, and takes into account the protocol construction and receiver behavior. This expresses the ratio $E_a - E_i = E_a - (E_v \oplus N_0)$, the attacker energy per bit to interfering energy per bit, where the total interference is the sum of the victim energy E_v and noise power spectral density N_0.

Overshadowing at position (θ, ϕ) succeeds if the attacker's signal power as attenuated by the out-of-beam loss is greater than the total interference by an amount greater than the overshadow factor:

$$P_a \geq P_{a,min}(\theta, \phi) = P_I + \gamma(P_v + G(0, 0) - N_0) - G(\theta, \phi) \quad (1)$$

4 Threat Model

In this paper, we consider a wireless adversary conducting spoofing attacks against satellite downlink communications. Where there is already an existing satellite signal on the channel, the attacker must achieve this by *overshadowing* the pre-existing signal, that is contending with the effects of the interference.

We assume that the attacker is equipped with suitable hardware to transmit a signal from a single location at the correct frequency and sufficiently high power. This consists of a Software Defined Radio (SDR), upconverter, amplifier, and antenna. We assume that the primary and secondary antennas are colocated sufficiently closely that beamforming attackers are incapable of targeting the primary or secondary antenna alone. However, the attacker can choose a position where the signal is highly attenuated by only one antenna.

SideDish is an angular-domain countermeasure, with the system considered more secure when attacker positions are more restricted [29]. This assumes maintaining presence in the signal path is more challenging than having ground station line-of-sight.

5 SideDish: Theory of Operation

SideDish is a retrofittable and cheap authentication system for protecting against out-of-beam overshadowing attacks at the downlink using an omnidirectional secondary antenna colocated with the primary antenna (e.g., a ground station). The fundamental principle is that the highly directional primary antenna amplifies the victim signal and attenuates out-of-beam attackers, whilst the secondary antenna treats both signals the same. Since the victim transmitter is much further away than the attacker transmitter, the secondary receiver senses the victim signal at much lower power than the attacker. If any out-of-beam attacker signal powerful enough to overshadow is also powerful enough to be sensed by the secondary receiver, then *secondary receiver sensing* upgrades authenticity. If less powerful signals can be detected, this also provides an early warning against attackers ramping up the power as part of an attack. This aspect of the Spoofing/Not Spoofing decision is shown in the columns of the decision process in Table 1.

As compared to a ground station without SideDish, attacking authentication – that is to have Spoofing classified as Not Spoofing – requires a higher capability attacker. Either the attacker must operate from an in-beam position with, e.g., a drone, or from two positions to simultaneously overshadow the primary receiver and jam the secondary receiver.

However, *secondary receiver sensing* alone could be easily targeted to deny authentication – that is to have Not Spoofing classified as Spoofing – if the attacker transmits an irrelevant signal that is decoded by the secondary receiver but does not disrupt decoding at the primary receiver. This attack is always possible owing to null points within the primary antenna gain pattern. A secondary approach is therefore needed to mitigate *denial of authentication* (DoA) attacks. Therefore we filter by *decoded signal comparison* between the primary and secondary receivers, and in particular on the contents and timestamps of the decoded frames. This aspect

Table 1: Decision Matrix for the SideDish. Spoofing is declared when the secondary receiver decodes data that is also comparable to the primary receiver data. Authentication is denied if the attacker causes the secondary receiver to fail decoding or decode incomparable data. Authentication is defeated only if the attacker causes the secondary receiver to incorrectly decode comparable data.

		Secondary Receiver Sensing	
		Decoded	**Not Decoded**
Decoded Signal Comparison	**Equal**	Spoofing	N/A
	Not Equal	Not Spoofing (warn)	Not Spoofing

of the Spoofing/Not Spoofing decision is shown in the rows of the decision process in Table 1.

Whereas a true overshadowing attack will cause the two receivers to decode the same data at the same time, an attacker transmitting non-overshadowing interference will not. Furthermore, *decoded signal comparison* does not open up the system to further DoA. Whilst an attacker could, from two positions, simultaneously overshadow both the primary and secondary receivers with different data, this requires a higher power budget than merely jamming the secondary receiver and achieves a worse effect in that the system will warn the operator.

In a real implementation, neither *secondary receiver sensing* nor *decoded signal comparison* perform perfectly, so the level of authenticity and associated DoA risk depend on a number of factors. First, *secondary receiver sensing* requires the gain pattern and protocol effects between the primary and secondary receivers to be sufficiently distinct that in-beam and out-of-beam overshadowing interference can be distinguished. Second, *decoded signal comparison* requires the clocks between the two receivers to be sufficiently synchronized that irrelevant out-of-beam interference can be identified and ignored. We now go on to define metrics by which these properties can be measured and evaluated.

5.1 Secondary Receiver Sensing

If the same carrier signal is incident at two receivers with different antenna gain patterns and with different amounts of receiver interference present, then the minimum required power to overshadow each receiver will differ. Interference that is out-of-beam from a primary, directional receiver and at sufficient power to overshadow can be detected if, from all out-of-beam positions, the power required to overshadow the secondary receiver is lower than the power required to overshadow the primary.

Equation 1 governs the lower bound for overshadowing a receiver, and can be specialized for any specific colocated receiver n, where $n = 1$ for the primary and $n = 2$ for the secondary:

$$P_a \geq P_{min,n}(\theta,\phi) = P_{I,n} + \gamma(P_v + G_n(0,0) - N_0) - G_n(\theta,\phi) \quad (2)$$

The incident satellite power P_v is equal for colocated receivers, and the decoder behavior $\gamma(...)$ and receiver noise N_0 is also equal where the receiver is of the same type.

For a given position (θ,ϕ), the attacker's *window of opportunity* as the margin where the attacker can spoof undetected by being received at the primary receiver without being detected at the secondary receiver:

$$\begin{aligned} W(\theta,\phi) &= P_{\min,2}(\theta,\phi) - P_{\min,1}(\theta,\phi) \\ &= [G_1(\theta,\phi) - G_2(\theta,\phi)] \\ &+ [((P_v + G_2(0,0)) \oplus N_0) - ((P_v + G_1(0,0)) \oplus N_0)] \\ &+ [\gamma(P_v + G_2(0,0) - N_0) - \gamma(P_v + G_1(0,0) - N_0)] \end{aligned} \quad (3)$$

Thus the window depends on 1) antenna design and positioning, specifically the in-beam and out-of-beam gains between the two antennas, and 2) protocol and receiver design. We explore these effects with respect to system design in Section 6.

5.2 Decoded Signal Comparison

As aforementioned, secondary receiver sensing alone leads to DoA attacks at any position where signals can be decoded at the secondary receiver, but do not affect decoding at the primary receiver. This window of opportunity for performing DoA attacks is expressed:

$$\begin{aligned} W_{DoA}(\theta,\phi) &= P_{max,1}(\theta,\phi) - P_{min,2}(\theta,\phi) \\ &= [G_2(\theta,\phi) - G_1(\theta,\phi)] + \left[P_{I,1} - P_{I,2}\right] \\ &+ [\overline{\gamma}(P_v + G_1(0,0) - N_0) - \gamma(P_v + G_2(0,0) - N_0)] \end{aligned} \quad (4)$$

where $P_{a,max}(\theta,\phi)$ is the maximum attacker power before decoding of the existing signal is affected, and $\overline{\gamma}$ is the *undershadow factor* that expresses the maximum relative attacker to total interference power before decoding is affected[1]. Successful attackers must operate at positions (θ,ϕ) such that $W_{DoA}(\theta,\phi) > 0$.

The addition of decoded signal comparison further constrains DoA attackers, which must ensure the data decoded by the secondary receiver compares equal with the primary receiver to be incorrectly classified as spoofing. In order to compare equal, the primary and secondary signals must contain the same data and be received within a time t set by the operator. Thus to deny authentication, that is causing the authentic satellite signal to classified as Spoofing according to the decision matrix in Table 1, the attacker must intercept and rebroadcast the satellite signal to be receiver at no greater latency than t to have the satellite signal appear to arrive from a single overshadowing source. To maximize replay protection, t must be set as low as possible, but not so low that the decision matrix causes overshadowing attacks to be classified as Not Spoofing with any realistic frequency.

By assuming a worst-case attacker that can intercept and retransmit with zero latency, the speed of light C places a bound on the maximum additional signal path distance the attacker can cause. The probability of spoofing misclassification given this zero latency attacker operating at additional signal path distance D is given by:

$$P(DoA) = 1 - \Phi\left(\frac{t - D/C}{\sigma}\right) \quad (5)$$

[1] If the pre-existing and overshadowing signal are using the same physical-layer attributes including modulation coding, $\gamma(\ldots) = -\overline{\gamma}(\ldots)$, so $W_{DoA} = -W - 2\cdot\gamma(\ldots)$.

Table 2: Example parameters relating to the satellite signal used in our tests.

Parameter	Value	Parameter	Value
Satellite Elevation	60°	Bandwidth	1.5 MHz
Protocol	DVB-S2	Frequency	10 GHz
Modulation	QPSK	Modulation and Coding	QPSK4/5
Forward Error Correction	1/4, 4/5, 9/10	RRC filter rolloff	0.2
Pilot Symbols	Off	Framing efficiency	0.9972

where Φ is the CDF of the standard normal distribution and σ is the standard deviation of the inter-receiver jitter.

6 System Implementation

As discussed in Section 5, the authenticity provided by SideDish depends on 1) *antenna design and positioning*, and 2) *protocol and receiver design*. Robustness against denial of authentication additionally depends on 3) *inter-receiver timestamp jitter*. To understand the implication of the system design on its security, we consider each of these aspects in turn.

6.1 Antenna Design and Positioning

We first consider the security of the system under idealized antenna models, where the primary antenna is an ideal parabolic reflector, and the secondary receiver an ideal isotropic (omnidirectional) antenna. Here we consider only the plane of the spherical coordinate system slicing through the main beam.

Whereas the secondary receiver has equal gain in all directions, the gain pattern of the primary receiver thus expressed by:

$$G(\theta) = \left(\frac{\pi d}{\lambda}\right)^2 e_a \cdot \frac{2\lambda}{\pi d} \frac{J_1[(\pi d/\lambda)\sin\theta]}{\sin\theta} \tag{6}$$

where d is the antenna diameter and λ the wavelength, both in m, e_a the aperture efficiency, and J_1 the first-order Bessel function. In this case we set $d = 1$ m, and $\lambda = C/10$ GHz which is our chosen X-band downlink wavelength from Table 2. We also consider the secondary antenna gain as amplified by an ideal low-noise amplifier, which can increase the gain without increasing receiver noise.

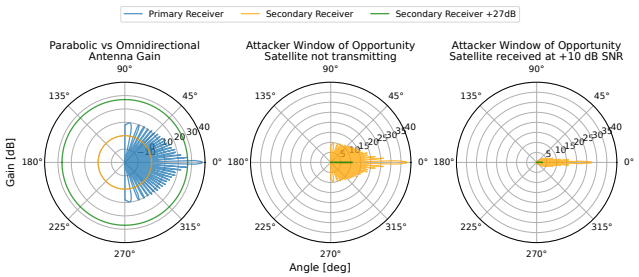
The effectiveness of carrier classification is expressed in terms of the proportion of out-of-beam space where the window of opportunity is positive:

$$\eta = \frac{1}{4\pi} \int_\theta \mathbb{I}\left(W(\theta,\phi) > 0\right) d\theta \tag{7}$$

where $\mathbb{I}(\cdot)$ is the indicator function which equals 1 when the condition $W(\theta,\phi) > 0$ is satisfied and 0 otherwise, and 4π is the total surface area of the unit sphere.

The gain patterns of the primary antenna, and secondary antenna with +0 dB and +27 dB of gain are plotted in Figure 2, left subplot. We note the high number of sidelobes which result from the high frequency interference pattern. Whereas the unamplified secondary antenna provides little coverage of the sidelobes, complete coverage is possible when the gain is boosted.

This effect is seen in Figure 2b, which plots the attacker's window of opportunity when the satellite is not transmitting. From Equation 3, since both the interference powers and overshadow factors are equal between both receivers, the window is given purely



(a) **(b)** **(c)**

Figure 2: (a) Gain plot of theoretic parabolic antenna compared to ideal omnidirectional receiver. (b) Window of opportunity when satellite is not transmitting; SideDish provides smaller benefit ($\eta = 26\,\%$ unamplified, $\eta = 1.1\,\%$ amplified). (c) Window of opportunity when satellite is received at 10 dB SNR at the primary; protocol decoding effects make both amplified and unamplified receivers twice as effective ($\eta = 11\,\%$ unamplified, $\eta = 0.56\,\%$ amplified). Note the change in scale between plots (a) and (b).

by the subtraction of the primary and secondary gain patterns, $W(\theta,\phi) = G_1(\theta,\phi) - G_2(\theta,\phi)$. Interestingly, even the unamplified secondary receiver provides some coverage, with spoofing only possible from $\eta = 26\,\%$ of all angles. However, the amplified secondary receiver provides significantly improved coverage, with only the main beam uncovered and $\eta = 1.1\,\%$.

We then consider the case where the satellite is transmitting such that the victim *Signal-to-Noise power ratio* (SNR) at the primary receiver is 10 dB. Further protocol effects are not considered here but left for Subsection 6.2, so we set the overshadow factor $\gamma(x) = 0$ dB for all x. The satellite signal, which disproportionately affects the primary receiver, acts to the countermeasure's advantage leading to a 2.36× improved sidelobe coverage of $\eta = 11\,\%$ for the unamplified secondary receiver. A similar performance improvement is seen in the amplified case, with $\eta = 0.56\,\%$.

6.2 Protocol and Receiver Design

We next consider the security of the system, extending the model from Section 6.1 to include the effect of protocol and receiver design. We are interested in the impact of the overshadow and undershadow factors on the attacker's window of opportunity for defeating authentication (Equation 3) and denying authentication (Equation 4).

As discussed in Section 3, the overshadow factor compares the attacker power required to overshadow as the total amount of interference remains constant, but the proportion of its constituent victim and noise components (the victim SNR) varies. This allows us to isolate the effect of the protocol and receiver on required overshadowing power and determine whether overshadowing is more difficult with a higher proportion of noise, or victim signal.

To evaluate this, we consider a number of modulation schemes commonly used in satellite communications: BPSK, QPSK, and 8-PSK. We set up a Monte Carlo simulation, modulating random data for both the attacker and victim signals and mixing them with additive Gaussian noise. We consider the worst case in which the

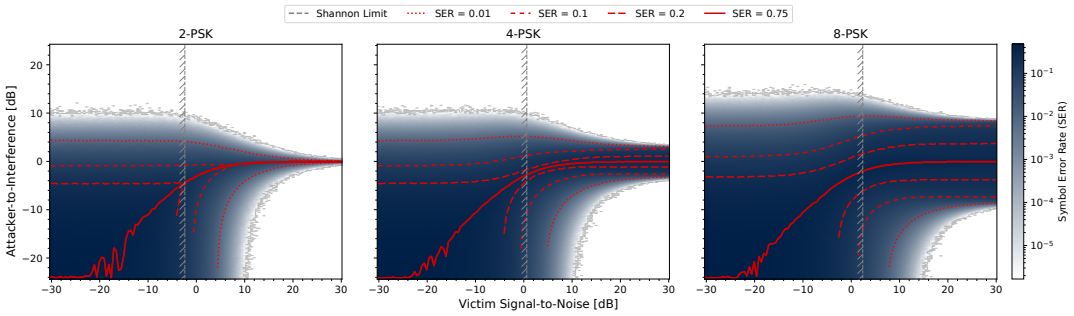


Figure 3: The overshadow factor $y = \gamma(x)$, expressing attacker-to-total interference power ratio (y axis) as victim signal-to-noise power varies (x axis). Three modulation schemes compared, hard demodulated without forward error correction. Overshadowed signal desynchronized with randomized phase. Attacker window of opportunity decreases when overshadowing signal requires higher power than overshadowing noise, as better performing FECs can cope with higher Symbol Error Rate (SER). Vertical line denotes the Shannon limit calculated in Appendix Equation 8.

overshadowed signal is entirely desynchronized to the overshadowing signal, leading to random phase rotations. The receiver attempts to decode attacker symbols when $P_a - P_v \geq 0$, and victim symbols otherwise. Bit error rate is determined by hard demodulation.

The results are plotted in Figure 3 with the lighter colored region corresponding to decoding success. The top region is where the attacker symbols are successfully demodulated, whereas the bottom right region is where the victim symbols are demodulated. As expected, at all victim SNRs an attacker with sufficient power will cause overshadowing. The overshadow factors are marked for different code rates, corresponding to different tolerable levels of the Symbol Error Rate (SER). It can be seen that the overshadow factor appears as an S-shaped curve, approaching an asymptote on each side as $P_v - N_0 \to -\infty$ on the left (interference is purely Gaussian noise), and $P_v - N_0 \to \infty$ on the right (interference is purely victim signal).

The attacker's window of opportunity is reduced when overshadowing victim-dominated interference requires more power than overshadowing noise-dominated interference, since the primary receiver is typically victim-dominated and the secondary receiver noise-dominated. We see that SideDish is disadvantaged for poorly performing codes which can only tolerate low SER, but this trend flips for codes which are better at correcting errors, thus requiring lower attacker power in noise-dominated interference.

The undershadow factors are also marked as the lower red curves, and are contours of the light region in the bottom right. This is the region within which the attacker can operate without affecting decoding; at the primary receiver, attackers attempting to deny authentication must operate within this region. The region does not extend into low $P_v - N_0$, since when the victim signal is too low relative to the noise it cannot be decoded. The Shannon limit, which is the theoretical limit of noise-free decoding, is marked as a vertical line – in an operational system, the SNR at the primary receiver would never drop below this limit by design [26, 31]. This is calculated according to Appendix Equation 8. Since the attacker's window of opportunity for denying authentication is reduced when the undershadow factor is decreased, SideDish benefits slightly when the primary receiver SNR is low.

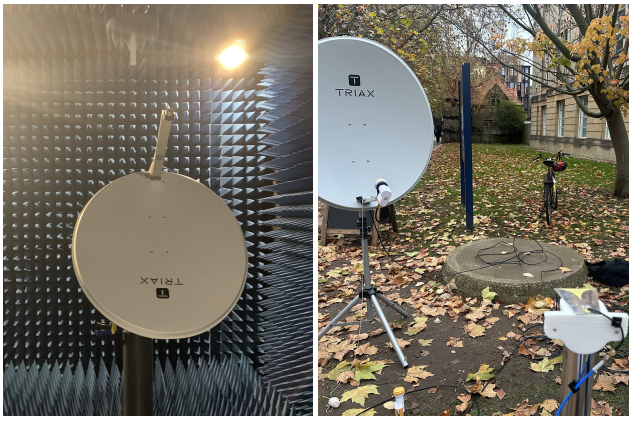
6.3 Inter-receiver Timestamp Jitter

We finally consider the security of the system against DoA attacks. From Table 1 we see that to deny authenticity, the attacker's signal must compare equal to the authentic satellite signal, causing the authentic signal to be rejected as spoofing. As discussed in Section 5.2, the primary and secondary receiver data compare equal if the decoded data is equal, and are received within time bound t.

The timestamp jitter, that is the timestamp error between a frame received at both the primary and secondary receiver, has variance σ^2 (from Equation 5) and can be decreased by minimizing differences in antenna position and subsequent RF path lengths, and signal processing jitter. Generally speaking, the earlier in the signal processing that frame timestamps are provided, and the more synchronized the receiver clocks, the lower the jitter. An implementer of SideDish should choose, based on the receiver architecture, the lowest jitter timestamps available to them.

A practical lower bound on timestamp jitter is given by considering that the primary and secondary receivers are both Software-Defined Radios (SDRs) with a shared clock, and can therefore provide sub-sample timestamp precision with variance equal to twice the jitter variance between any one SDR and the clock. A practical upper bound is instead given by considering a receiver which can only resolve timestamps to the nearest data symbol, which is a prerequisite of signal decoding.

Taking the USRP N210 SDR as an example, which has jitter with standard deviation $\sigma = 3.3\,\text{ns}$, a practical lower bound of timestamp standard deviation between two N210s with a shared clock is $\sqrt{2}\sigma = 4.67\,\text{ns}^2$ [7]. Using our chosen symbol rate of 1.5 MHz from Table 2 as an example, a generous but practical upper bound on standard deviation can be found by setting the confidence interval on symbols being sampled correctly to $\sigma = \sqrt{2}/1.5\times10^6 = 0.943\,\mu\text{s}$.



(a) Primary antenna under test in near-field range.

(b) SideDish targeted by attacker antenna in urban environment.

Figure 4: Various antennas set up in the test environment as described in Sections 7.1 and 7.3. The near field range consists of (a) an X-band waveguide mounted to a robotic arm with adjustable elevation ϕ, and the antenna under test mounted to a plate with adjustable azimuth θ. Decoded signal comparison evaluated in (b) an urban environment with the secondary antenna positioned underneath the primary antenna, at various attacker antenna angles.

7 Experiment Design

Thus far we have established, with respect to theoretic models, the effect of SideDish design decisions on both the level of authenticity provided and the robustness to DoA attacks. In this section we establish the experiment design and method to evaluate SideDish through three real-world hardware experiments: *antenna gain pattern measurement*, *software protocol decoding*, and *measuring inter-receiver timestamp jitter*.

We set up the receiver system as follows. For the primary antenna, we use the RF Hamdesign X-band horn feed mounted in a TRIAX 1 m offset dish as shown in Figure 4b. The main secondary antenna consists of two RF Hamdesign X-band horn feeds mounted in a forward or backward placement in the vicinity of the primary receiver. The combined placement is evaluated by combining these gain patterns in post-processing. The primary and secondary antennas are each connected to a USRP N210 SDR, which both share a common 10 MHz clock signal to minimize inter-receiver timestamp jitter. Both DVB-S2 receivers are implemented in software, using the `leandvb` [17] software package.

7.1 Antenna Gain Pattern Measurement

As established in Section 5.1, the relative gain patterns between the primary and secondary antennas are critical to the success of the countermeasure. For the primary antenna we are interested in the sidelobes and backlobes, which are the best candidates for the attacker to transmit with the least power. For the secondary antenna we are interested in its gain pattern shielding these lobes in two scenarios: ideal placement, where the gain pattern is not influenced by the presence of the primary antenna, and other placements where the gain pattern is influenced. We consider backward and forward placement where the secondary antenna covers the back and front of the dish respectively, and combined placement that uses two secondary antennas to cover both.

We establish the gain patterns of passive antennas through high-precision *near-field range* experiments in a $4 \times 4\,\text{m} \times 4\,\text{m}$ anechoic chamber. The tests are conducted at 10GHz, the same frequency chosen for our earlier simulations from Table 2. The test facility consists of an NSI-700S-120 near-field measurement system capable of scanning 270° and 360° in the azimuth and elevation axes respectively, and is shown in Figure 4a. The probe antenna is an open-ended waveguide assembly manufactured by NSI-MI. The data is finally processed using the NSI 2000 Pro software package to transform the near-field data to the final far-field gain pattern.

7.2 Software Protocol Decoding

In Section 6.2 we saw that the level of authenticity provided depends on the protocol decoding effects, with different selections of modulation and error correcting code advantaging or disadvantaging SideDish. We now go beyond considering hard demodulated symbols to overshadow the full DVB-S2 protocol structure.

We determine the overshadow and undershadow factor on a software decoder to understand the amount of power the attacker needs to overshadow the receiver with three different protocol variants. In each case, the frame error rate is measured at different levels of attacker power relative to the total interference. The interference consists of a mixture of additive white Gaussian noise and the victim signal in different proportions.

To evaluate this, we set up the GNURadio flowgraph in Appendix Figure 10. Victim and attacker MPEG-TS streams are each encoded with `leandvbtx`, and then mixed on a channel with additive white Gaussian noise. The resulting signal is normalized to 0 dB to prevent floating point errors at extreme cases. This is then decoded with `leandvb`, using the external `xdsopl-LDPC-pabr` decoder, which performs 25 decoding iterations.

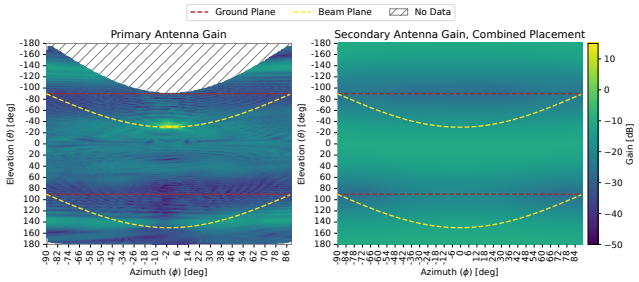
The packet recovery rate is recorded as the victim signal-to-noise ratio and attacker-to-total-interference ratios vary. The undershadow and overshadow factors are computed with respect to a 50 % error rate threshold. The specific choice of threshold is irrelevant due to the sharp digital cliff exhibited by error correction.

7.3 Measuring Inter-receiver Timestamp Jitter

As discussed in Section 6.3, increasing robustness of the receiver against DoA attacks requires decreasing inter-receiver timestamp jitter. We conduct a live spoofing attack with a primary and secondary receiver in a real world environment to establish this effect, and thus understand the level of replay protection provided. The parameters for these experiments are provided in Table 2. All experiments are conducted in compliance with amateur radio license restrictions, since we operate only in amateur bands with licensed signals, and target only our own receivers.

The transmitter chain consists of a USRP N210 SDR, a DEM 10368-144 transverter which upconverts to the X-band and amplifies up

[2]This standard deviation is the maximum of all tested configurations by De Dominicis et al [7], but we note that this paper measures jitter for a different protocol. We consider a complete evaluation of SDR timestamp jitter out of scope for this work.



(a) (b)

Figure 5: High-precision gain plots comparing 1 m primary directional antenna and secondary omnidirectional antenna in the spherical coordinate system. The path of ground-based and beam-plane transmitters are traced in dashed lines. Main beam is centered at elevation 60° ($\theta = -30°$), sidelobes between the ground plane lines, and backlobes either side of ground plane lines. Secondary antenna oriented vertically to cover the side and back lobes ($\theta = 0°, \pm 180°$)

to 3 W, a 30 dB attenuator, and a WA5VJB Vivaldi X-band antenna. The primary receiver is a Golden Media GM202 LNB mounted on the TRIAX 1m dish, pointed with the main beam at elevation 60° as shown in Figure 4b and Table 2. The secondary LNB receiver is positioned directly beneath the primary receiver LNB feed, pointing upward. Each LNB is connected to a USRP N210, which share a common clock via a MIMO cable.

The azimuth θ of the attacker is varied with respect to the fixed dish through a number of angles. At each position, the power of the attacker is varied until the signal is decoded at both the primary and secondary receivers. In total, we capture 8 recordings of 30 s each, simultaneously recording both the primary and secondary signals. In total our dataset consists of 13 110 frames which are decoded at both the primary and secondary receivers.

8 Evaluation

Using the experiment design discussed in Section 7, we now provide an end-to-end analysis of the performance of SideDish in a real world setting. In particular we evaluate its performance in *spoofing detection* and *mitigating denial of authentication.*

8.1 Spoofing Detection

As discussed in Sections 6.1 and 6.2, SideDish can detect spoofing attacks wherever, in order to overshadow the primary receiver, the attacker must necessarily overshadow the secondary receiver too. This depends on the *antenna design and positioning*, and *protocol and receiver design.*

8.1.1 Antenna Design and Positioning. The measured gain patterns for the primary and secondary antennas (photographed in Figure 4) are shown as flattened heatmaps in Figure 5. We trace the contour of ground-based transmitter positions in brown, and those in the plane intersecting the main beam in yellow. The region between the ground plane lines represents the hemisphere below the dish, and the region either side of the ground plane is the hemisphere above the dish. The main beam, sidelobes, and backlobes of the primary antenna can be clearly seen, as well as the front and back lobe of the secondary antenna.

We evaluate whether the antenna gain plot by itself is sufficient to detect spoofing by considering $P_v = -\infty$dB, where the satellite is not transmitting. This is seen in Figure 6a, with the attacker window of opportunity marked in red. By integrating over the plot as in Equation 7, we find that spoofing is only possible from $\eta = 4.73\,\%$ of the measured positions under combined placement.

However, in the real world the proximity of the secondary receiver to the primary dish affects its gain pattern. We measured the secondary antenna gain pattern as directly adjacent to the dish, shown in Appendix Figure 12a. The effect of dish backscattering is evident, as the pattern is more inconsistent and includes more null regions. The corresponding spoofing region therefore increases, and is shown in Appendix Figure 12b. We measure $\eta = 27.9\,\%$ for the Backward Placement, and $\eta = 6.45\,\%$ for the combined placement.

In scenarios where the satellite is transmitting, the attacker must overshadow the interfering signal. This requires a higher power budget, and therefore advantages SideDish. Protocol-specific effects aside, we see from Equation 3 that the window of attacker opportunity depends on relative levels of interference received at the secondary and primary receivers. This is heavily influenced by the in-beam gains: the primary antenna amplifies the signal by +14.61 dB, whereas the secondary antenna achieves only −14.56 dB.

8.1.2 Protocol and Receiver Design. In addition to the gain pattern, spoofing detection also depends on the effects of the protocol (cf. Equation 3). We now measure the extent to which deficiencies in gain pattern are compensated for by these protocol effects.

The results of the software decoder evaluation are plotted in Figure 8, which shows the attacker-to-interference ratio required to overshadow a number of protocol variants, as the victim satellite SNR varies. The image is split into multiple distinct regions. In the top half, we see the overshadow factor γ traced out as a red dashed line – in order to reliably overshadow, the attacker must exceed this power level. The lower right region is where decoding the original signal succeeds. Notably, we see that in all cases overshadowing requires more power at the primary receiver (where the satellite is received at higher power) than the secondary receiver (where, relatively speaking, the noise power is higher).

Combined with the gain pattern, this significantly advantages SideDish. Taking the victim satellite SNR to be 10 dB with DVB-S2 MODCOD QPSK4/5 as an example, the resulting overshadow windows for the different secondary antenna placements are shown in Figure 6b and Appendix Figure 12b. In all cases the spoofable region is significantly decreased: the Ideal Placement reduces from $\eta = 4.73\,\%$ to $0.16\,\%$, the Backward Placement from $\eta = 27.9\,\%$ to $1.1\,\%$, and the Combined Placement from $\eta = 6.45\,\%$ to $0.34\,\%$. Figure 7 plots how this proportion decreases as victim SNR increases for each placement, demonstrating conclusively that even satellite power only barely above the decodable Shannon limit nevertheless results in a significant increase in spoofing detection.

However, Figure 7 also shows that as satellite SNR increases, the undershadowable region increases – these are positions from which the adversary can potentially cause DoA. This is calculated using the undershadowing threshold $\bar{\gamma}$ traced in Figure 8 in the lower

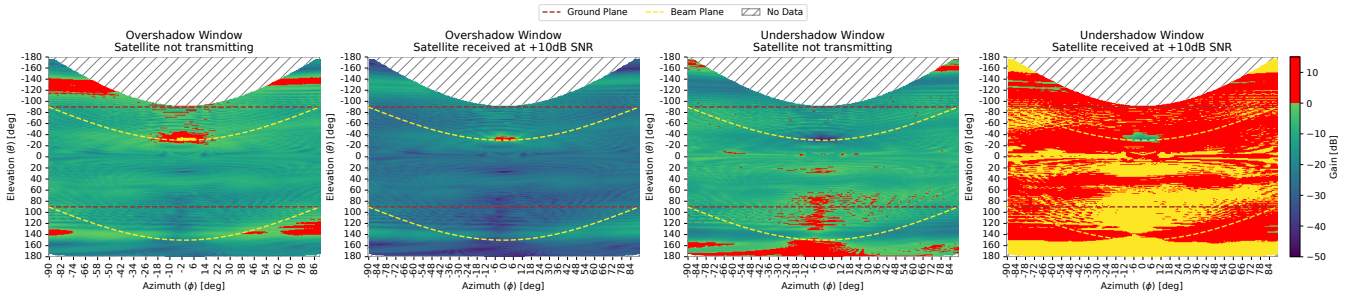


Figure 6: Heatmaps of overshadow and undershadow window of opportunity where red indicates attack success. a) When satellite not transmitting, the attacker can only spoof if present within the main beam or back lobes, or c) undershadow if present in particular antenna null zones. b) When satellite signal present (victim SNR = 10 dB), protocol effects are sufficient to allow very narrow localization, however d) undershadowing can occur anywhere outside the main beam. This underscores the importance of decoded signal comparison as discussed in Sections 5.1 and 6.3.

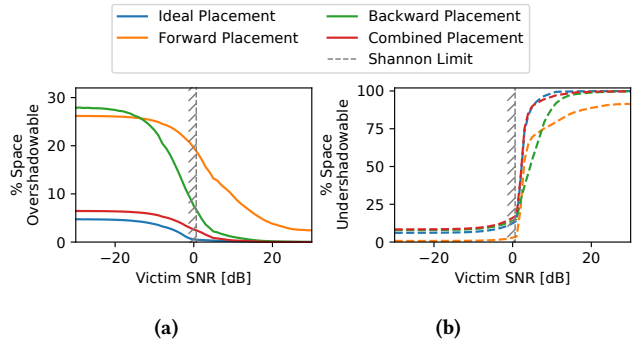


Figure 7: Proportion of positions (η) available to the attacker to overshadow (a) and undershadow (b) as victim SNR varies, for different secondary antenna placements and DVB-S2 MODCOD QPSK4/5. As the attacker compensates for higher satellite power, the available positions to overshadow the signal from decrease. We see that even poorly placed antennas still provide reasonable protection even when the satellite is not transmitting, reducing the possible attacker positions by over 70 %. Decoded signal comparison (Section 5.2) is required to mitigate DoA since the available undershadowing region increases with SNR, approaching 100 %.

right region. The effect on the undershadowable region is seen clearly by comparing Figure 6c (no satellite signal) with Figure 6d (with satellite signal). This underscores the importance of mitigating DoA by a mechanism which is independent of the undershadowable region size, such as decoded signal comparison.

8.2 Mitigating Denial of Authentication

As discussed in Section 6.3, overshadowing attacks are detected by comparing the data decoded at both the primary and secondary receivers according to Table 1. If the signals simultaneously contain the same data, the data is rejected as Spoofing. Therefore it is important to prevent an attacker from simply replaying the satellite data stream, causing it to appear as overshadowing and thus denying service at low power. We mitigate DoA by bounding the acceptable latency between frames received by the two receivers.

Using the experiment setup described in Section 7.3, we conducted live transmit-receive experiments in an outdoor urban environment. The resulting timestamp jitter distribution (the difference between the secondary and primary received times) is shown in Appendix Figure 11, which fits a Gaussian distribution model with mean $\mu = -0.018\,\mu s$ and standard deviation $\sigma = 0.042\,\mu s$. The negative bias in μ indicates that frames are received at the primary receiver later than the secondary receiver possibly due to a longer RF path. We note that our measured σ lies within the upper and lower bounds calculated in Section 6.3, and is significantly closer to the lower bound than the upper bound.

Using this known level of jitter, and assuming a perfect attacker that introduces no latency in intercepting and retransmitting, we can derive a bound on the additional signal path distance the attacker can cause without detection. This is plotted for the lower bound, upper bound, and measured value in Figure 9. We find that in order to have a 50 % chance of denying authentication, the attacker must be no further from the signal path than 48 m, and at 100 m the chance of denying authentication asymptotically approaches zero.

8.3 Discussion

From these results, we see that despite its simplicity, SideDish is a highly effective countermeasure in detecting satellite downlink overshadowing attacks. The system achieves highly effective overshadowing detection in all tested cases, spatially constraining the attacker in the worst case by at least 70 % (cf. Figure 7), and up to 99.84 % (as given by the Ideal Placement at satellite SNR of 10 dB).

Attacks to defeat authentication instead require a stronger attacker: either they must maintain presence in-beam, or else transmit from two locations to simultaneously overshadow both the primary and secondary receivers, and jam the secondary receiver. We note that in this case the system is no worse off than without SideDish.

We also see that through decoded signal comparison, DoA attacks are not feasible with realistic constraints. In particular, DoA

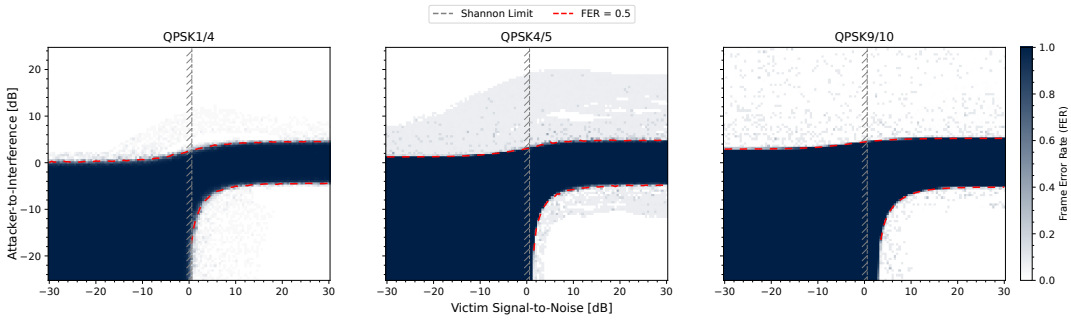


Figure 8: MPEG-TS packet recovery for varying victim SNR and attacker-to-total-interference ratio, for DVB-S2 MODCODS QPSK1/4, QPSK4/5 and QPSK9/10. Darker colours represent greater packet loss. Vertical hatched lines represent the Shannon limit for QPSK, below which error-free decoding cannot occur. Dashed red lines at the 50% recovery boundaries indicate the overshadow (upper) and undershadow (lower) factors.

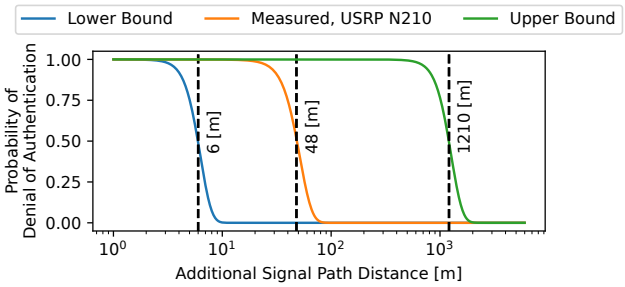


Figure 9: Worst-case chance that authentication can be denied as attacker distance from the beam path varies. The attacker introduces zero latency other than speed of light delays, and replays the authentic satellite signal within the undershadow window. Bounds calculated in Section 6.3.

requires the attacker to intercept the authentic signal and to retransmit with low latency to appear as spoofing. The required latency is sufficiently low that even an ideal attacker with no delay is constrained to operate within the vicinity of the signal path – at 100 m, even the ideal attacker has a negligible probability of success. Furthermore, the decision matrix in Table 1 has the potential to emit early warnings in the case when the secondary receiver decodes non-overshadowing signals: this may indicate an attacker ramping up power to eventually overshadow.

We note that since SideDish relies only upon differences in dish gain pattern, received power, and overshadow factor, it is applicable to any satellite downlink frequency. The results from Appendix Figure 12 show that significant angular-domain security is provided even when considering scattering effects from the primary antenna. The effect of different DVB-S2 protocol variants was considered in Section 8, but further work is required to assess the specific overshadow factors of other protocols. Since our evaluation is focused on the specific hardware described in Section 7, deployments with different gain patterns would also need to be validated separately.

9 Conclusion

In this paper we have presented SideDish, a low-cost countermeasure for protecting cryptographically unauthenticated satellite downlink signals. Through theoretic simulations and real-world experiments, we confirmed that placing a secondary antenna in the vicinity of the receiver is sufficient to detect spoofing interference, even when considering antenna scattering. This is possible because the effect of the existing satellite signal is to require a higher-power attacker. Our results show that this constrains the space that single-transmitter spoofers can operate from by 70 % in the worst case, and up to 99.84 % in the best case. We also confirmed that the countermeasure cannot be abused to deny authentication with realistic constraints, since even idealistic zero-delay attackers can only deny authentication if less than 100 m from the beam path.

The effectiveness of this cheap countermeasure represents a significant shift in the defense of satellite signals, since wireless spoofing attacks can be detected with high accuracy without the need for an expensive interference monitoring platform.

References

[1] Norman Adams, Judy Bitman, David Copeland, Dipak Srinivasan, and Antonio Garcia. 2013. RF Interference at Ground Stations Located in Populated Areas. In *2013 IEEE Aerospace Conference*, 1–8. doi:10.1109/AERO.2013.6496880.

[2] Robin Bisping, Johannes Willbold, Martin Strohmeier, and Vincent Lenders. 2024. Wireless Signal Injection Attacks on VSAT Satellite Modems. In *33rd USENIX Security Symposium (USENIX Security 24)*, 6075–6091.

[3] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen, and Gérard Lachapelle. 2012. GNSS Spoofing Detection in Handheld Receivers based on Signal Spatial Correlation. In *Proceedings of the 2012 IEEE/ION position, location and navigation symposium*. IEEE, 479–487.

[4] Luca Canzian, Stefano Ciccotosto, and Samuele Fantinato. 2017. GSTS: Ground-to-Space Threat Simulator — Project Executive Summary Report (SR v2.0). Technical report ESA-QAS-GSTS-ESR. GSTS SR v2.0 — Project Executive Summary Report. European Space Agency (ESA) / QAS, (Feb. 2017). https://nebula.esa.int/sites/default/files/neb%5C_tec%5C_studies/3050/public/96577.pdf.

[5] Hing C Chan and Eric K Hung. 1999. An Investigation in Interference Suppression for HF Surface Wave Radar. Tech. rep. DREO TR2000-028. Defence Research Establishement Ottawa.

[6] Andrej Danis. 2025. *Exploiting Smart TVs using the HbbTV Protocol*. Ph.D. Dissertation. Technische Universität Wien.

[7] Chiara Maria De Dominicis, Paolo Ferrari, Emiliano Sisinni, Alessandra Flammini, P Pivato, and D Macii. 2012. Timestamping Performance Analysis of IEEE 802.15. 4a Systems based on SDR Platforms. In *2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings*. IEEE, 2034–2039.

[8] Kai Jansen, Nils Ole Tippenhauer, and Christina Pöpper. 2016. Multi-Receiver GPS Spoofing Detection: Error Models and Realization. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 237–250.

[9] Eric Jedermann, Martin Strohmeier, Matthias Schäfer, Jens Schmitt, and Vincent Lenders. 2021. Orbit-based Authentication using TDOA Signatures in Satellite Networks. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 175–180.

[10] Minjae Kang, Sungbin Park, and Yeonjoon Lee. 2024. A Survey on Satellite Communication System Security. *Sensors*, 24, 9, 2897.

[11] Minjeong Kim, Daseon Hong, and Sungsu Park. 2020. A Study on the Amplitude Comparison Monopulse Algorithm. *Applied Sciences*, 10, 11, 3966.

[12] Edson Stevens Galagarza Martinez. 2018. *Recent Advances on Physical Layer Security for Wireless Communications*. Master's thesis. Northeastern University.

[13] Paul Y. Montgomery, Todd E. Humphreys, and Brent M. Ledvina. 2009. Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-antenna Receiver Defense Against a Portable Civil GPS Spoofer. Tech. rep. Novariant Inc, University of Texas at Austin, and Virginia Tech. https://repositories.lib.utexas.edu/server/api/core/bitstreams/0eb5f718-e142-4ff9-b233-b117547757fe/content.

[14] Daniel Moser, Patrick Leu, Vincent Lenders, Aanjhan Ranganathan, Fabio Ricciato, and Srdjan Capkun. 2016. Investigation of Multi-Device Location Spoofing Attacks on Air Traffic Control and Possible Countermeasures. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, 375–386.

[15] Nathaniel Mott. 2022. Report: NSA Investigates Viasat Hack That Coincided With Ukraine Invasion. *PCMag*, (Mar. 2022). https://www.pcmag.com/news/report-nsa-investigates-viasat-hack-that-coincided-with-ukraine-invasion.

[16] NL Times. 2024. Cyber Attack on TV channel BabyTV: Toddlers Suddenly Exposed to Russian Propaganda, (Apr. 2024). https://nltimes.nl/2024/04/06/cyber-attack-tv-channel-babytv-toddlers-suddenly-exposed-russian-propaganda.

[17] pabr. 2016. leandvb: A lightweight software DVB-S/S2 demodulator. Accessed: 2025-10-14. (Feb. 2016). https://www.pabr.org/radio/leandvb/leandvb.en.html.

[18] Mark L. Psiaki, Steven P. Powell, and Brady W. O'Hanlon. 2013. GNSS Spoofing Detection Using High-Frequency Antenna Motion and Carrier-Phase Data. In *Proceedings of the ION GNSS+ 2013*. Ithaca, N.Y. 14853-7501, U.S.A. https://gps.mae.cornell.edu/Paper_F5_8_ION_GNSS_2013b.pdf.

[19] Aanjhan Ranganathan, Hildur Ólafsdóttir, and Srdjan Capkun. 2016. SPREE: A Spoofing Resistant GPS Receiver. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, 348–360.

[20] Rohde & Schwarz. 2026. *R&S® UMS400 Universal Monitoring System: Outdoor Spectrum Monitoring and Radiolocation Solution*. (Version 05.00 ed.). Product brochure. R&S UMS400 Brochure, PDF. Rohde & Schwarz. Munich, Germany, (Apr. 2026). https://scdn.rohde-schwarz.com/ur/pws/dl%5C_downloads/pdm/cl%5C_brochures%5C_and%5C_datasheets/product%5C_brochure/3609%5C_8144%5C_12/UMS400%5C_bro%5C_en%5C_3609-8144-12%5C_v0500.pdf.

[21] Edd Salkield, Sebastian Köhler, Simon Birnbach, Richard Baker, Martin Strohmeier, and Ivan Martinovic. 2023. Firefly: Spoofing Earth Observation Satellite Data through Radio Overshadowing. In *NDSS Workshop on Security of Space and Satellite Systems (SpaceSec)*. doi:10.14722/spacesec.2023.231879.

[22] 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*, 341–352.

[23] Desmond Schmidt, Kenneth Radke, Seyit Camtepe, Ernest Foo, and Michał Ren. 2016. A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Computing Surveys (CSUR)*, 48, 4, 1–31.

[24] Oliver Senn, Giorgio Tresoldi, Daniel Moser, Vincent Lenders, and Martin Strohmeier. 2025. Universal Spoofing of Real-World Aircraft Multilateration. In *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 268–273.

[25] SKAI Data Services. 2025. Navigating the Future: Mitigating GPS Spoofing & Jamming Risks in Aviation. Tech. rep. https://gpswise.aero/white-paper.

[26] C. E. Shannon. 1949. Communication in the Presence of Noise. *Proceedings of the Institute of Radio Engineers*, 37, 10–21.

[27] 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*, 75–86.

[28] Yazhou Tu, Vijay Srinivas Tida, Zhongqi Pan, and Xiali Hei. 2021. Transduction Shield: A Low-Complexity Method to Detect and Correct the Effects of EMI Injection Attacks on Sensors. In *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 901–915.

[29] Nachiappan Valliappan, Angel Lozano, and Robert W Heath. 2013. Antenna Subset Modulation for Secure Millimeter-Wave Wireless Communication. *IEEE Transactions on communications*, 61, 8, 3231–3245.

[30] Chen Yan, Hocheol Shin, Connor Bolton, Wenyuan Xu, Yongdae Kim, and Kevin Fu. 2020. SoK: A Minimalist Approach to Formalizing Analog Sensor Security. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 233–248.

[31] Randy Yates. 2014. Derivation of the Shannon Spectral Efficiency Limit. *Digital Signal Labs*.

[32] Youqian Zhang and Kasper Rasmussen. 2020. Detection of Electromagnetic Interference Attacks on Sensor Systems. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 203–216.

Appendix

Calculating the Shannon Limit

The minimum required Eb/N0 (in dB) for a given bits-per-symbol, roll-off factor and framing efficiency is given by:

$$E_b/N_0^{\min}(\text{dB}) \;=\; 10\log_{10}(\ln 2) \;+\; 10\log_{10}\left(\frac{b\cdot\eta_f}{1+\alpha}\right) \qquad (8)$$

where b is the number of bits per symbol, $alpha$ is the roll-off factor, and eta_f is the framing efficiency.

Software Protocol Decoding Flowgraph

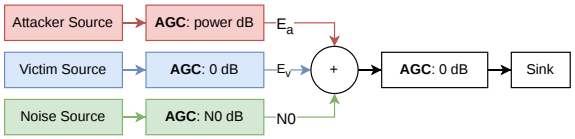


Figure 10: Schematic of DVB-S2 simulation pipeline used in GNURadio. Attacker, victim and noise signals are combined and normalized to 0 dB. The victim power is fixed at 0 dB, and the attacker and victim power are varied. The result is decoded and the TS packet count is recorded.

Inter-receiver Timestamp Jitter

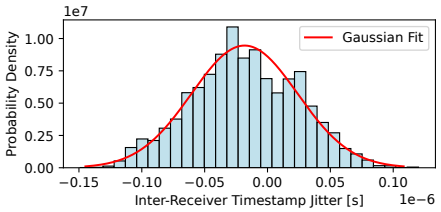


Figure 11: Distribution of the *inter-receiver timestamp jitter* from experimental data of 13 110 overshadowed frames. The mean < 0 indicating a longer RF path for the primary receiver. The $\sigma = 0.042\,\mu s$ is less than the calculated upper bound of $0.943\,\mu s$ in Section 6.3, indicating tight bounding of attacker distance.

Secondary Antenna Placement

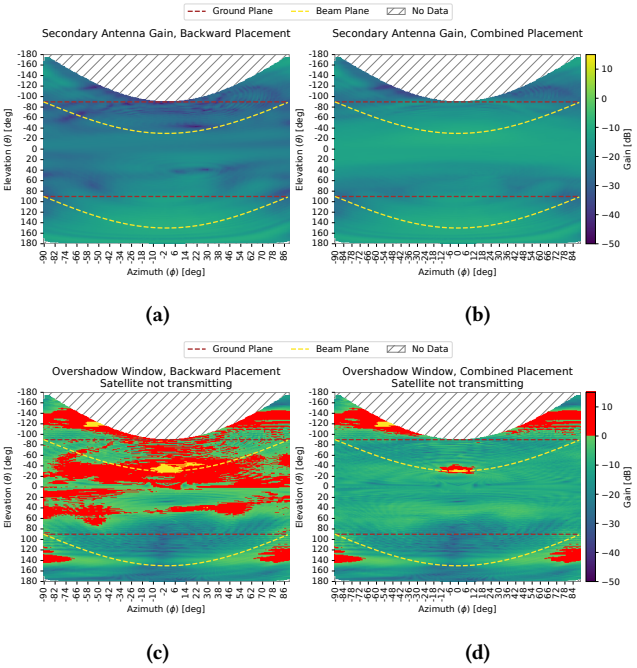


Figure 12: Heatmaps of the overshadow window of opportunity for SideDish, considering a secondary antenna that experiences backscattering from the primary antenna due to its proximity. *Top:* Gain patterns of the secondary receiver in backward (a) and combined (b) placement. The uneven pattern and null regions are evident compared to the ideal placement in Figure 5. *Bottom:* The overshadow window associated with the backward (c) and combined (d) placement. Whilst the backward placement covers the backlobes, it covers the sidelobes poorly. The combined placement pattern is significantly improved.

Acknowledgments

We would like to thank armasuisse Science and Technology for their support, and Satellite Applications Catapult for use of the Near Field Range for the antenna tests. We would also like to acknowledge the useful feedback from and discussions with ESA throughout the course of this work. 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 programme.