Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks

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

Marcell Szakály
marcell.szakaly@cs.ox.ac.uk
University of Oxford
Oxford, United Kingdom

Joshua Smailes
joshua.smailes@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

Satellite communications are increasingly crucial for telecommunications, navigation, and Earth observation. However, many widely used satellites do not cryptographically secure the downlink, opening the door for radio spoofing attacks. Recent developments in software-defined radio hardware have enabled attacks on wireless systems including GNSS, which can be effectively spoofed using only cheap hardware available off the shelf. However, these conclusions do not generalize well to other satellite systems such as high data rate backhauls or satellite-to-customer connections, where the spoofing requirements are currently unknown.

In this paper, we present a systematic review of spoofing attacks against satellite downlink communications systems. We establish a threat model linking attack feasibility and impact to required budget through real-world experiments and channel simulations. Our results show that nearly all evaluated satellite systems were overshadowable at a distance of 1km in the worst case, for a budget of ~2000 USD or less.

We evaluate how the key challenges of antenna directionality, legitimate satellite signal presence, modulation schemes, and receiver saturation can be overcome in practice through antenna sidelobe targeting, overshadowing, and automatic gain control takeover. We also show that, surprisingly, protocols designed to be more robust against channel noise are significantly less robust against an overshadowing attacker. We conclude with a discussion of physical-layer countermeasures specifically applicable to satellite systems which can not be cryptographically upgraded.

1 MOTIVATION

Spoofing attacks against wireless channels – where the public nature of the channel allows an adversary to transmit a fictitious signal to impersonate a legitimate party – have been extensively studied, and the risks they pose are well established. These attacks have been significantly aided by recent developments in software-defined radio (SDR) hardware, which can capture signals for analysis, and transmit arbitrary waveforms at very low cost. This presents a particular threat to insecure wireless systems which do not yet use cryptographic authenticity to protect communication integrity.

Whilst satellite communications are becoming increasingly vital in areas such as telecommunications, global navigation, and Earth observation, many existing satellite operators do not cryptographically secure the downlink. Security features were historically considered unnecessary in both cost and complexity, owing to the high equipment budget required to attack these systems. However, even certain recent satellite deployments fail to encrypt the downlink, with governments only recently beginning to recommend encryption on satellite communications [1]. This is a particular issue because, unlike in a terrestrial context, satellites cannot be retroactively upgraded or cheaply replaced.

Recent work has shown that SDR-equipped attackers can mount a credible threat against not just terrestrial wireless systems such as mobile internet [2, 3] and avionics [4], but also GNSS satellite systems [5]. In particular, it has has been shown that nearly any device using civilian GPS can be spoofed using only a cheap SDR and open source software [6, 7].

Concerns have also been raised about the security of Earth observation and telecommunications satellite data links, but remain largely theoretical. For instance, it has been recently shown that a spoofing attacker can arbitrarily manipulate forest fires detected from NASA's real time satellite image service, to disrupt crisis analysis. Furthermore, the software processing this data has not been designed to be secure against arbitrary, unstructured input data, leading to denial of service vulnerabilities [8]. It was also demonstrated in 2020 that confidential maritime communications are regularly transmitted by DVB-S satellite broadband in the clear, raising concerns about TCP session hijacking [9, 10].

Spoofing attacks affect not only unauthenticated satellite communications; there is an increasing proliferation of satellites with either leaked keys, or which employ cryptography that is no longer considered secure. For example, two Korean satellites have had their master keys leaked through key mismanagement [11, 12] and one of them uses weak single DES [11].

Despite these concerns, no current academic work has considered the feasibility of performing spoofing attacks on real world satellite downlink systems other than GNSS. Results from these attacks, which target cheap omnidirectional antennas in end-user devices designed to distinguish satellites on a shared channel, do not apply to other systems such as dedicated space-to-ground data links. Rather, attacking these systems requires overshadowing a legitimate signal using a protocol not designed for multiple access, at a frequency not readily accessible with off-the-shelf hardware, and received by a large and highly directional antenna, potentially within a security perimeter. The wide variety of receiver systems have previously made presenting a detailed threat model difficult,

as the attacker's constraints are "strongly tied with the goals and security requirements of the target mission" [13].

In this paper, we seek to establish such a threat model, linking attack feasibility and impact to the required budget for a modern adversary. This threat model is derived from a systematic analysis of each component in the satellite communications stack, including both real-world experiments and simulation.

In Section 2 we draw together work in wireless spoofing attacks with specific attacks on satellite systems, identifying current knowledge gaps in these areas. In Section 3 we provide key background information required to understand our attack description and analysis. In Section 4 we set out the goals of an attacker seeking to disrupt satellite ground systems. In Section 5 we provide an overview of the requirements of downlink satellite signal spoofing in the general case, drawing attention to the key factors affecting the required attacker received power. In Section 6 we derive through real world experiments and simulation how satellite received power, antenna characteristics, and modulation and coding properties affect the required power budget of the attacker. In Section 7 we relate the analysis in the previous section to real-world satellite systems and attacker hardware, presenting an analysis of the threat presented by overshadowing attacks. Finally, in Section 8, we discuss the applicability of new and existing countermeasures in defending against this form of attack, especially for systems which can not be cryptographically upgraded.

2 RELATED WORK

Spoofing attacks against wireless systems have been well explored in academic literature in a wide range of areas, such as avionics [14], wireless telephony [2, 15], and short-range communication such as Zigbee [16]. Many of these systems use the wireless channel as a shared medium between multiple devices, with attackers spoofing when no other device is transmitting, reducing the overall power required. Unlike these attacks, satellite spoofing attacks in the general case require *signal overshadowing*, in which the attacker's signal must surpass the legitimate signal on the channel.

The majority of existing work in satellite signal spoofing focuses on GNSS systems such as GPS – these are particularly vulnerable to spoofing due to their unencrypted nature, and are received at a very low power by omnidirectional antennas [5, 17]. GPS spoofing has been demonstrated at a low budget, using only a cheap SDR and open source software [6, 7], and even encrypted GPS has been shown to be vulnerable to replay attacks [18]. However, these attacks target systems with omnidirectional antennas designed to pick up very weak signals at a low data rate, so the results do not generalize to all space systems – many of these use highly directional antennas and high data rate protocols, impacting requirements for a successful spoofing attack.

There are also a number of well-documented attacks on satellite uplinks – most notably, the *Captain Midnight broadcast signal intrusion*, in which a pirate satellite television signal successfully overshadowed a legitimate broadcast [19]. Attacks have also been executed on US government satellites *Landsat-7* and *Terra*, hijacking the telecommand to gain control of the satellite [20]. This demonstrates the vulnerability of satellite systems (and their attractiveness as a target) but does not provide a frame of reference for the power and hardware requirements to carry out similar attacks on ground systems.

There are some known attacks on terrestrial systems which more closely match the satellite spoofing scenario, particularly in cellular networks. The *AdaptOver* attack system demonstrates the use of overshadowing on LTE to achieve arbitrary message injection, persistent denial of service, and leaking sensitive information for the LTE and 5G-NSA protocols [3]. Additionally, the *SigOver* and *SigUnder* attacks demonstrate overshadowing attacks on LTE with a significantly reduced power budget [2, 21]. This is achieved by synchronizing with the carrier signal and taking advantage of error correcting codes present in the protocol, and by exploiting knowledge of the underlying data to flip individual bits in the signal rather than overshadowing the entire message. We build upon this work in Section 5, assessing these techniques in a zero-knowledge context (i.e. the message is not known and cannot be exploited to flip individual bits), with the added difficulty of overshadowing signals on a highly directional dish.

It is clear from the existing work that spoofing attacks on satellite ground systems are a concern, and we can see that they are certainly possible due to the similarities to other wireless systems. However, the focus on GNSS systems in satellite research has created a gap in knowledge – the majority of space systems are sufficiently different from GNSS that the attacks do not generalize. The extent to which these systems are vulnerable, and the power and hardware requirements for attacks, is currently unclear.

3 BACKGROUND

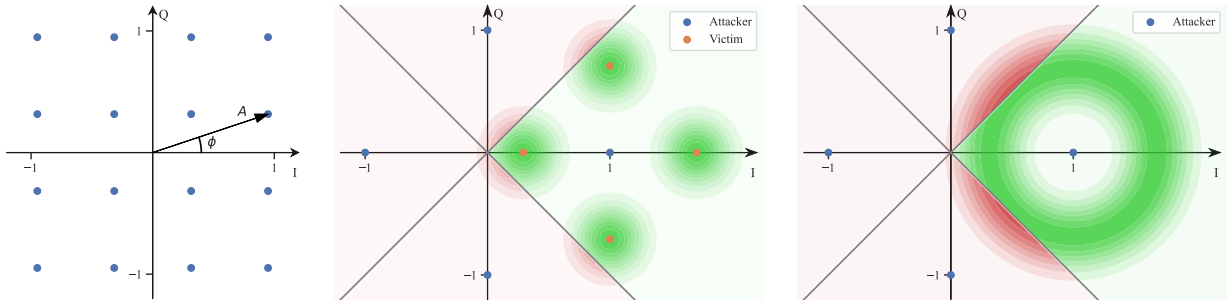
When sending information over radio, the data must first be modulated onto a carrier wave. This can be achieved in a number of ways; most commonly Phase Shift Keying (PSK) is used to encode symbols (i.e. bits, or sequences of bits) by varying the phase relative to the carrier signal. The amplitude can also be varied in Quadrature Amplitude Modulation (QAM), which achieves a greater symbol density for higher data rates.

For easier analysis, these signals can be decomposed into In-phase (I) and Quadrature (Q) components, that are in phase with the carrier and 90° out of phase respectively. This decomposition can be easily done in hardware, and is the basis of operation for all SDRs.

IQ constellation diagrams are commonly used to visualize digitally modulated signals, since carrier information is removed but the symbols remain as distinct points on the diagram. The symbol's angle represents its phase difference to the carrier, and distance from the center represents amplitude of the signal. An example of an IQ diagram for the 16-QAM constellation is shown in Figure 1a.

When multiple RF signals on the same carrier are superimposed (added), their IQ representations are also added. If the signals have the same frequency but are not synchronized in phase, the IQ representation of one signal will be rotated. Gaussian noise shows up as additive Gaussian noise on both the I and Q components. An example of this can be seen in Figure 1b, in which an attacker adds a constant offset to a QPSK modulated signal.

If a signal has not been properly phase matched, or if there is a frequency offset, then the phase is unknown. This causes the constellation to appear as a ring instead of distinct points. This can



(a) 16-QAM constellation (b) Phase-aligned victim (c) Non-phase aligned victim

Figure 1: Left: IQ diagram of the 16-QAM constellation, showing the amplitude and angle. Center: The more powerful attacker QPSK constellation offsets the phase aligned victim constellation. Right: The more powerful attacker QPSK constellation offsets the non-phase aligned victim. Shading shows the effect of Gaussian noise, with the region decoded as the attacker's symbol in green.

be seen in Figure 1c, in which the same constant offset is added to a QPSK signal that is not phase aligned.

4 THREAT MODEL

The goal of the adversary is to cause disruption to downlink processing systems by emitting counterfeit signals in the vicinity of the receiver. The adversary must achieve this by overshadowing the pre-existing victim satellite signal. The adversary seeks to transmit close to the minimum viable power level, to remain stealthy and avoid saturating the receiver.

We assume that the attacker has no prior knowledge of the victim message, and so must overshadow by transmitting an entire message, rather than through preempting and flipping individual bits. We also assume that the attacker has access to suitable equipment to transmit a signal at the correct frequency at sufficiently high power. This includes an off-the-shelf Software Defined Radio (SDR), which can typically cover all frequencies up to 6 GHz [22], alongside suitable upconverting and amplifying hardware as necessary. Furthermore, the attacker is able to maintain a presence either in the vicinity of the receiver, or has a suitably directional antenna to conduct the attack from a long distance.

Crucially, since the receiving satellite dish is highly directional and the attacker is likely ground-based, we do not assume that the attacker can emit signals within the beam of the receiver.

A more detailed discussion of the budget and constraints of the attacker is presented in Section 7.

5 ATTACK DESCRIPTION

Achieving a wireless spoofing attack fundamentally requires that the attacker's signal is transmitted at sufficiently high power to be decoded at the receiver. The properties required to achieve overshadowing at the satellite downlink are outlined in Figure 2.

Specifically, the attack proceeds as follows: the victim satellite signal is received at the victim antenna at power P_v, and the attacker at power P_a. The relative power of each signal as it reaches the demodulator and decoder depends upon the antenna and receiver characteristics. The attacker's received power is attenuated relative

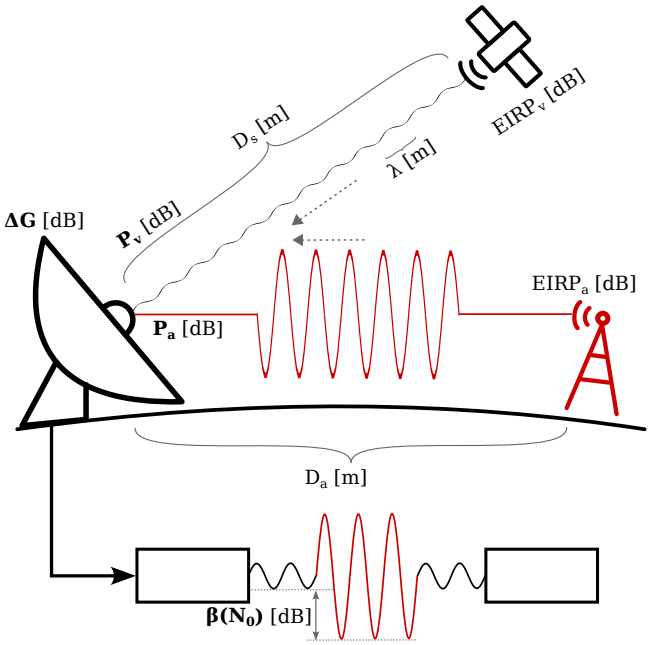


Figure 2: An illustration of the overshadowing attack described in this paper. The attacker is indicated in red. The variables relevant to the attacker in calculating transmit gain are labeled. Key parameters are in bold, and are derived from the non-bold parameters as described in Section 5.

to the victim by ΔG, the *out of beam loss*, due to the antenna. For example, highly directional dishes are designed to amplify signals within a specific beam, and attenuate signals outside of it.

Additionally, the electronics in the receiver add noise to the signal, N_0, affecting the overall signal-to-noise ratio.

The *overshadow factor*, $\beta(N_0)$, is the required relative power of the attacker to the victim signal, as received at the demodulator, to achieve attack success. Specifically, this factor expresses E_a/E_v,

the ratio of attacker energy per bit to victim energy per bit, at a given E_v/N_0, the energy per victim bit to noise power spectral density. This value depends upon the signal-to-noise level of the system; intuitively, attackers have to achieve a higher gain in noisier systems.

The attack is successful if the attacker's signal as attenuated by the out-of-beam loss is greater than the victim signal added to the overshadow factor. Specifically:

$$P_a > P_v + \beta(N_0) + \Delta G$$

We go on to explore each of these parameters, P_v, ΔG, and $\beta(N_0)$ in Section 6. Through real world experiments and simulation we determine the required attacker power, P_a, for a representative sample of real world satellite systems.

6 ATTACKER POWER BUDGET ESTIMATION

In this section, we derive through real world experiments and simulations how the feasibility of the attack varies with respect to the key parameters outlined in Section 5. We relate these factors to a representative selection of satellites, subdivided into GNSS, telecommunication (both to customer and ground station via backhaul), Earth observation, and CubeSat. The key parameters of these satellites are summarized in Table 3.

We first consider *modulation and coding*, deriving a lower bound for $\beta(N_0)$ under commonly-used modulation schemes through closed-form mathematical analysis. We validate this analysis using Monte Carlo simulation, and provide an upper bound in the maximal noise case. Our results quantify how modulation schemes differ in robustness to overshadowing. Furthermore, we show that overshadowing adversaries can abuse error correcting codes to decrease the required transmission gain.

We then consider *antenna gain*, where we demonstrate the large effect of antenna directionality on attack success through deriving ΔG from real-world experiments. We draw attention to the ease of overshadowing omnidirectional antennas and the relative difficulty of directional dishes, which ultimately require more specialized attacker transmitter hardware. Our experiments show that attackers against static dishes can realistically mitigate out-of-beam attenuation through targeting sidelobes, but that this presents difficulty against tracking dishes.

We finally demonstrate how the attacker can use OSINT to estimate an upper bound on the *satellite received power*, P_v. We derive this bound for a representative sample of satellites, including those at GEO and LEO orbits, across different frequencies, and downlinking at different data rates. Our findings show that most satellite systems are received at the same power, even across vastly different classes.

All real world experiments on antenna transmission capabilities were conducted in amateur radio bands, by licensed amateur radio operators. The experiments complied with the conditions of the amateur license, including the band plan and station identification requirements, and used the minimum possible power at all times.

6.1 Modulation and Coding

To understand the impact of different modulation schemes on the attacker's success, we seek to determine $\beta(N_0)$ for the most common satellite modulations, phase shift keying (PSK) and quadrature amplitude modulation (QAM). Intuitively, we expect that higher density constellation structures (those with more symbols in the IQ plot) are more resilient to overshadowing; the attacker's symbol needs to be resilient to any victim symbol, so the attacker's constellation must be larger.

We formalize this by defining a new metric called constellation density ρ, and use it to analyze the two extreme limits of sparse and dense constellations.

The ρ is given by the ratio of two distances on an IQ plot: the largest distance between the origin and a constellation point d_R, and the smallest distance between two constellation points d_C: $\rho = d_R/d_C$. BPSK is the ideal sparse constellation, with symbols located at $(1, 0)$ and $(-1, 0)$, giving a density of $1/2$. QAM-256 is an example of a dense constellation, consisting of a 16x16 grid of symbol points centered on the origin, giving a density of $7.5\sqrt{2}$.

If no noise is present, and the attacker is not phase aligned, the attacker can achieve perfect overshadowing if and only if the constellation is larger than the victim constellation (v) by a factor of 2ρ. To prove this, consider the closest two points of the attacker constellation (a). The distance between them is given by:

$$d_{C,a} \geq 2\rho d_{C,v} = 2\frac{d_{R,v}}{d_{C,v}} d_{C,v} = 2d_{R,v}$$

Since the IQ diagrams are made in voltage space, the power of the attacker must be $4\rho^2$ times larger than the victim to achieve perfect attacker symbol decoding, in the noiseless scenario. This is because each victim symbol can offset the attacker's symbol by no more than $d_{R,v}$, which is less than half of the distance between the closest two attacker points.

As noise increases, so the power of the attacker must increase to compensate. Therefore, we derive the following lower bound:

$$\beta(N_0) \geq 4\rho^2$$

6.1.1 Monte Carlo simulation. To understand how the required attacker-to-victim ratio (E_a/E_v) varies across these systems with respect to constellation structure and receiver noise (represented in overall signal-to-noise ratio, E_b/N_0), we build a fine-grained Monte Carlo simulation.

The simulation is set up as follows: the attacker and victim both generate a random message, which is encoded into the chosen modulation scheme. We derive $\beta(N_0)$ by varying E_a/E_v and E_v/N_0 across different constellation types. At the end, the resulting symbols are demodulated to form a bit stream, which is compared with the attacker's bit stream to give a bit error rate. We consider both the case of a phase aligned vs a maximally non phase aligned attacker by randomly offsetting the phase of the victim's symbols. During the simulation we assume that the receiver is locked onto the attacker's synchronization header, and hence is expecting symbols in the attacker's constellation.

We pay particular attention to the limiting cases of receiver noise: the zero noise case where $E_v/N_0 = \infty$, and the maximum noise for which the victim can be decoded, where $E_v/N_0 = \ln(2)$ (derived from the Shannon limit) [23]. The results of this analysis

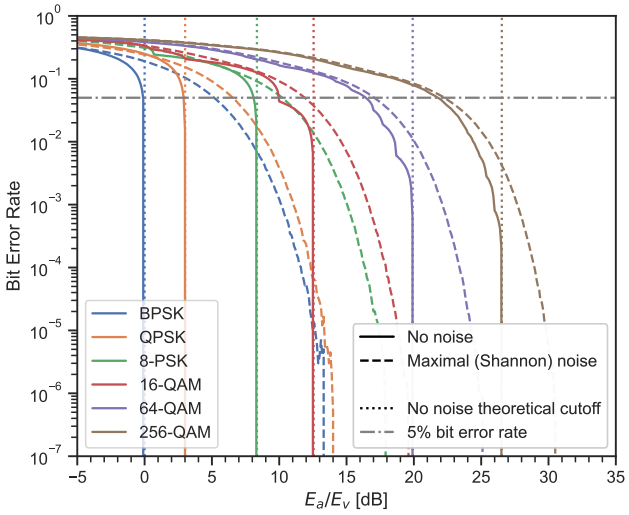


Figure 3: Attacker bit error rate against received attacker-to-victim ratio, in the minimum and maximum receiver noise cases. More complex modulation schemes require significantly increased gain, especially in the noisy setting. The dotted line represents the coding-correctable bit error rate of 5%. This assumes a worst-case, non phase-aligned attacker.

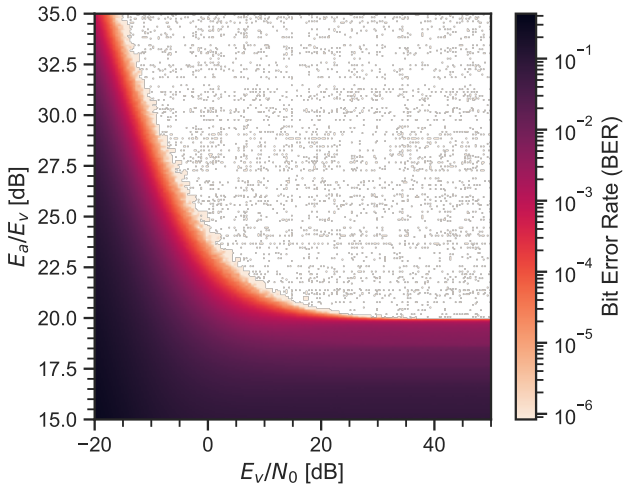


Figure 4: Heatmap of 64-QAM overshadowing attack success, against both the attacker-to-victim and overall signal-to-noise ratios. Successful region is lightly colored. This assumes a worst-case, non phase-aligned attacker.

at these limiting cases can be seen in Figure 3, as compared to the mathematically derived lower bound. We also consider this across varying noise levels for a given protocol in Figure 4.

6.1.2 Effect of modulation. As seen in Figure 3, for all the noise free lines there is a sharp cutoff at a certain E_a/E_v where the attacker's bit error rate suddenly drops to zero. This value agrees with the mathematical bound. For example, for BPSK it is at $4(1/2)^2 = 1$ or 0 dB, and for 256QAM it is at $4(7.5\sqrt{2})^2 = 450$ or 26.53 dB.

As the noise increases to the maximum bound, so the received symbol can end up even further from the original attacker symbol. The attacker has to counter this by increasing their received gain, thereby increasing the constellation size. Figure 3 shows that for the noisy channels, the bit error rate also goes to zero as the attacker overpowers the victim, however this happens at a much higher value compared to the noise free case. In theory, the infinitely long tail of the Gaussian noise distribution means that the error rate never truly drops to zero, but the likelihood is negligible and so is not represented in the numerical simulation.

The relationship between E_a/E_v and bit error rate across varying E_v/N_0 values is explored in Figure 4. The plot shows that for a victim who is stronger than the noise, the attacker's case reduces to the noise free one, with a sharp transition. In the limit when the victim power is less than that of noise, the plot shows a diagonal tendency corresponding to lines of constant attacker-noise ratio. This illustrates the extreme case of an attacker on a noisy channel, with no victim present.

The attacker can calculate the precise E_v/N_0 for a given receiver by considering that most of the noise N_0 is from the thermal noise of the electronics, which can be derived from the temperature T (assumed to be 300 K) and Boltzmann constant k_B.

$$\begin{aligned} N_0 &= 10\log_{10}(T) + 10\log_{10}(k_B) \\ &= 24.77 - 228.60 \\ &= -203.83\ \text{dB W/Hz} \end{aligned}$$

E_v/N_0 then depends upon the satellite's bit rate and received power as follows:

$$E_v/N_0 = P_v - 10\log_{10}(R) - N_0$$

We provide a table summarizing the values of $\beta(N_0)$, with E_b/N_0 at the limiting values, in Table 1.

6.1.3 Realizing the coding potential. To increase the protocol's resilience to noise, satellite protocols often contain error correcting codes to reduce the effective bit error rate. However, in an overshadowing scenario, these codes serve to correct bit errors in the attacker's received signal. This reduces the $\beta(N_0)$, since the attacker can afford to achieve a higher bit error rate.

As a case study, we take the Reed-Solomon error correcting code as used in Terra/Aqua X-band transmissions, which can correct up to a 5% bit error rate, marked as a horizontal dashed line [24]. The maximum coding potential the attacker can realize for a given modulation scheme is the difference between the E_a/E_v at the 5% and 0% bit error rates.

As can be seen, constellations approach the cutoff point more gradually as constellation density ρ increases, and as E_b/N_0 increases. Comparing modulations, the coding potential of BPSK is negligible, but the attacker can realize a gain of up to ~8 dB in the 256-QAM limiting case.

6.2 Antenna gain

We next consider the impact of the receiver antenna gain pattern on the attack by determining ΔG, the out-of-beam loss. This is the

Table 1: Base overshadow factor $\beta(N_0)$ [dB] needed to achieve BER = 10^{-6}, broken down by modulation scheme and receiver noise level. Results derived from Monte Carlo simulations shown on Figure 3, assuming unaligned phase between attacker and victim symbols.

	BPSK	QPSK	8-PSK	16-QAM	64-QAM	256-QAM
No noise	-0.1	3.0	8.3	12.5	19.9	26.5
Maximal noise	13.0	13.6	18.3	19.3	25.6	30.8

Table 2: Table of attacker antenna attenuation from out of beam transmission, varying antenna types and environments. Missing values from the large dish are due to restricted access from roof geometry. Min relative gain represents the approximate minimum gain an attacker can expect within an angle of 60°of the main beam. Starlink phased array antenna simulated using single slit diffraction, $\Delta G = 10\log_{10}\left(\frac{\sin^2(\frac{\pi a \sin\theta}{\lambda})}{(\frac{\pi a \sin\theta}{\lambda})^2}\right)$

Antenna type	Approx. main lobe size [degrees]	Sidelobe relative loss [dB]	Largest realistic relative loss [dB]
Large dish, rooftop	–	14.1	30 (estimated)
Mesh dish, rooftop	40	0.9	30 (estimated)
VHF Yagi, field	120	28.9	36.0
VHF Yagi, rooftop	120	5.5	30.2
UHF Yagi, field	90	16.7	26.2
UHF Yagi, rooftop	90	9.9	54.8
Starlink dish, simulated	10.31	13.25	31.15
Omnidirectional, theoretical	0	0	0

ratio of how attenuated the attacker's signal is relative to the victim, and depends on the choice of ground station antenna, the attacker's angle relative to the dish, and the effects of multipath propagation.

Most satellite systems fall into two key categories depending on the choice of ground station antenna. Some systems are intended for reception by low cost user terminals (Iridium) or even handheld devices (GPS), and are in non-geostationary orbits. These systems require small, omnidirectional antennas. However, systems intended for reception by a large ground station (Aqua, Terra) or systems in geostationary orbits (Satellite TV) can minimize the transmission power of the satellite, and instead choose to require a highly directional, high gain antenna, such as a satellite dish.[1]

A directional antenna will have a high gain in one direction, but will necessarily have a smaller gain in other directions, often well below that of an isotropic antenna. It is likely not feasible for an attacker to get into the directional beam, since they would need to place an antenna in the sky, potentially above a secure facility. Instead, the attacker must choose an accessible spot on the ground – this will be out of beam of the satellite dish, and experience a much lower gain. We call this the out of beam loss, defined as $\Delta G = G_{\text{Victim}} - G_{\text{Attacker}}$. In Section 6.1, we show that the received power of the attacker must be higher than the received power of the victim signal by a certain amount, depending on the modulation. However, since the antenna gain for the victim system is much higher than the antenna gain for the attacker's direction, the attacker signal strength at the dish must be higher than the victim signal by both the overshadow factor E_a/E_v and out of beam loss ΔG.

The attacker intends to transmit at the minimal possible power, so they can take measures to optimize the attack. The attacker can choose a position on the ground where the antenna has the highest possible gain, and hence the lowest possible out of beam loss. By knowing the value of out of beam loss they will experience, they can calculate the minimal amount of power needed to overcome both this loss, and the modulation. The attacker is aided by the existence of side lobes, which are directions away from the main lobe (beam) of the antenna, where the gain is higher than in generic other directions, while still being smaller than the main beam. Generally, for higher gain antennas, the main lobe is thinner, but side lobes also become thinner and increasingly frequent. If the attacker is able to determine the radiation pattern of an antenna, they can select an advantageous side lobe and know the exact out of beam loss they will be experiencing, thus allowing them to use the lowest possible power.

The extent to which an attacker can determine the radiation pattern depends on their budget. A well equipped attacker can get access to an identical copy of the dish, in a comparable environment, and perform measurements. In the case of shared ground stations, the attacker may also be able to rent time on the same dish as used by the victim, and perform measurements. If these are not feasible, the attacker can conduct detailed site surveillance, measuring the properties of the dish, and its surroundings, in order to construct an RF simulation. These methods will allow the attacker to accurately consider both the radiation pattern of the dish, and the effect of multi-path propagation of the out of beam signals due

[1]Despite its appearance, the Starlink user terminal is a highly directional antenna, using phased array technology.

(a) Large fixed Meteosat dish on rooftop. (b) X-band mesh dish on rooftop. (c) Directional Yagi antenna in open field.

Figure 5: A selection of the tested antennas in varying environments.

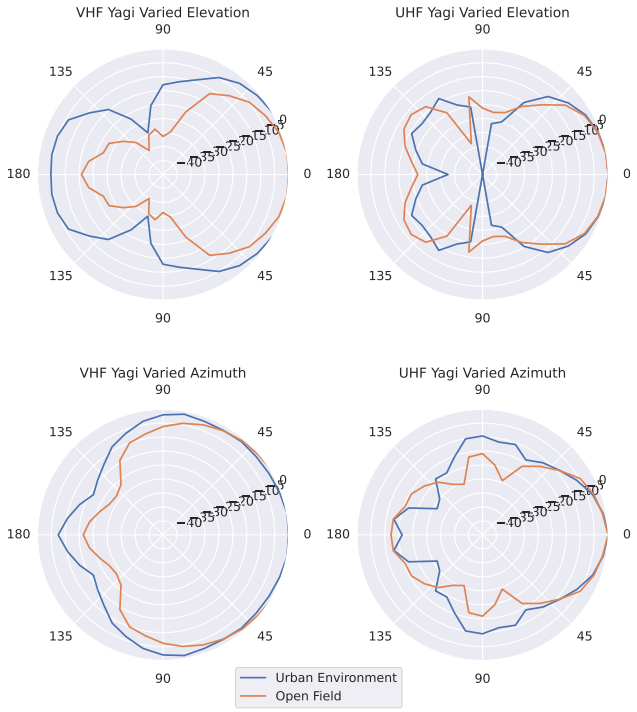


Figure 6: The received power of an out-of-beam attacking signal relative to an in-beam victim signal, across different antenna types and environments. The VHF antenna is a 3 element Yagi, and the UHF has 7 elements.

to the environment surrounding the dish. If these are not an option, the attacker can try identifying the manufacturer of the dish and obtaining a data sheet, or measure its key geometric properties and look up the theoretical radiation pattern. Theoretical patterns are well known and available for a variety of dishes, such as parabolas, yagis and monopoles.

Figure 6 shows measurements of the radiation pattern of multiple antennas, in an open field and an urban environment as depicted in Figure 5. Due to the presence of nearby walls in the urban environment, significant multi-pathing occurs, increasing the gain. A summary of these experiments against various realistic antennas can be found in Table 2.

The attacker faces further difficulties if the satellite is non geostationary, and hence the dish is rotating to track it. A rotating dish will mean that it is not possible for a stationary attacker to remain in an optimal spot, and they must choose whether to overshadow only a small portion of the transmission when the dish presents an appropriate side lobe, or increase power to attack the dish during the entire overpass.

6.3 Satellite received power

The received victim power P_v affects the attacker's required power P_a, since the attacker's signal must overcome both out of beam attenuation ΔG and the overshadow factor $\beta(N_0)$. Although P_v varies based on the specific satellite system being targeted and factors such as the weather, the attacker can determine an upper bound through OSINT. This is calculated by applying free space path loss to the satellite's EIRP (effective isotropic radiated power), over the distance of the satellite's altitude, as follows:

$$P_v = EIRP_v - 20\log_{10}(d) - 20\log_{10}(f) - 92.45$$

Where $EIRP_v$ is the victim EIRP, d is the distance in kilometers, and f is the frequency in GHz.

We estimate the P_v value for each of the satellites as an additional column in Table 3. Interestingly, the P_v is similar between most

satellites, tending to range between −150 dB W and −130 dB W, even between CubeSats and high data rate backhauls. We conclude that this is a conscious design decision: each satellite is designed to use the minimum power budget, and so high data rates are achieved primarily through more directional receivers rather than increased satellite power.

7 EVALUATION

In Section 6 we demonstrated how the overshadow factor $\beta(N_0)$, out-of-beam loss ΔG, and victim satellite received power P_v can be derived for a given satellite. Here we relate this analysis to real-world satellites against a fully budgeted overshadowing attacker, analyzing the threat that overshadowing attackers present to existing satellites.

We begin by calculating P_a, the attacker received power required to overshadow a given system, for the satellites in Table 3. We discuss the transmitter hardware available to buy or build at different frequency bands and power levels, analyzing the budget and skill level required to obtain. Using the techniques established in Section 6.3, we calculate the received power these can achieve across varying distances. We conclude our analysis by relating the attacker received power achievable through the budgeted transmitter hardware to the satellite systems, establishing that nearly all analyzed satellites are overshadowable at a range of 1km at a budget of $2000 or less.

7.1 Calculating required attacker receiver power

As discussed in Section 6, the attack succeeds for any $P_a > P_{a,min}$, where:

$$P_{a,min} = P_v + \beta(N_0) + \Delta G$$

We calculate these values for a set of realistic satellites in Table 4.

7.2 Attacker hardware

Although cheap SDR hardware and amplifiers are available, and have been successfully used to attack other wireless systems below 6GHz, a significant number of satellites downlink at frequencies higher than this [22, 48]. The hardware required to overshadow higher frequency bands therefore also requires an upconverter and dedicated amplifier.

Although the component costs of high frequency upconverters and amplifiers are low (circa $200 each), assembling a custom upconverter and amplifier setup requires a skilled attacker capable of RF engineering. This is not completely infeasible, as demonstrated by the amateur radio community; dedicated members often create upconverters for the 10 GHz [49] and 24 GHz [50] amateur bands, at prices available to hobbyists.

However, less skilled attackers will need to instead buy plug-and-play hardware for upconverting. Whilst the internal components are the same, there are few legitimate reasons for transmitting in these frequency bands aside from amateur radio and laboratory testing. As a result, ready-to-use hardware is significantly more expensive than the component costs alone. Although the cost of new hardware of this form is $9,000 or more, these costs can be reduced to $100 – $2000 by instead buying surplus lab equipment.

Table 5 shows, for multiple frequencies used in real world satellite, the cost of purchasing a new COTS up-converter, the estimated cost of buying used components on the second hand market, and the cost of creating it from a mixer IC and auxiliary components.

7.3 Vulnerable satellite analysis

The equipment budgeted in Table 5 transmits at a given power level, $EIRP_v$. Using the path loss formulae established in Section 6.3, we calculate the received power these can achieve across varying distances. In Figure 7 we compare these values to the received power level required to overshadow each satellite, as calculated in Section 7.1. We plot both the minimum and maximum bounds of $P_{a,min}$ for each system; ΔG is either maximum attenuation within 60° of the main lobe or instead the sidelobe, and $\beta(N_0)$ is either under zero or maximum receiver noise.

Our results show that all satellites are vulnerable to overshadowing over very short distances of 100m, and all but the Ku band are overshadowable in the worst case over distances of 1 km.

Satellites in the L band are trivially overshadowable; these use omnidirectional antennas and are subject to the least path loss. Therefore, the weakest equipment is capable of overshadowing the strongest signal with 40 dB to spare. Attackers can achieve overshadowing at a distance of over 8 km using only an SDR and very cheap amplifier. The X band satellites are overshadowable with a headroom of 20 dB in the worst case at 8 km using the strongest equipment. Starlink in the Ku band demonstrates the large effect of modulation; BPSK is guaranteed overshadowable within 1 km, but 64-QAM only at very close range. The Ka band is similar, being overshadowable from 8 km in the best case, but within 1 km in the worst case.

8 COUNTERMEASURES

The simplest solution to counter overshadowing attacks is cryptographic authentication on both the up and downlink. However, upgrading existing satellite hardware in place is infeasible. In new designs, operators may choose to omit cryptography, because in case of an error (e.g., a corrupted or lost key, or even a single bit flip) it can make the received data unusable, and thus potentially render the satellite inoperable. Cryptosystems also need to be regularly replaced, as the mathematical insight and computational power needed to break them becomes increasingly available; due to the long lifetime of satellites, it is likely that their cryptography will become obsolete and require replacement. In multiple previous cases, satellite keys have been leaked [11, 12], so an effective scheme must contain a key update protocol. In the event of a leak, this same key update system could also easily be used to hold the satellite for ransom, if the attacker is able to change keys.

For the downlink, it may be possible to implement protection on the ground station instead. Additional signal processing and sanity checking measures can be applied to determine if a signal is coming from the legitimate satellite, or a nearby attacker. A few potential measures are listed below.

8.1 Signal strength analysis

Satellite operators perform detailed calculations on the expected power levels when designing the satellite, in order to ensure that

Table 3: Table of satellites with their maximum estimated received power on Earth, attenuated according to free space path loss. Cited numbers represent a mixture of measured results and best estimations. Cryptographically protected systems are marked with a dagger†. Results are best estimates only based on publicly available information.

Satellite Class	Satellite	Receiver Type	Max bitrate [Mbps]	Modulation	Frequency [GHz]	EIRP [dBW]	Altitude [km]	Path loss [dB]	P_v – Received power [dBW]
GNSS (Navigation)	GPS L1	Omnidirectional	0.000050 [25]	BPSK	1.575 [26]	27.1	21,000 [26]	182.8	-155.8
	Galileo E1	Omnidirectional	0.000125 [25]	MBOC	1.575 [25]	37 [27]	23,000 [28]	182.7	-145.7
Telecommunication (Customer)	Iridium-NEXT	Omnidirectional/OpenPort terminal	1.5 [29]	QPSK	1.621 [30]	9.5	780	154.5	-145 [30]
	Inmarsat 3	Fixed small dish	10 [31]	BPSK/FSK	1.518 – 1.559 [32]	49 [33]	35,000 [34]	187.1	-138.1
	Alphasat	Fixed small dish	300 [35]	BPSK/FSK	19.7 [32]	70 [33]	35,000 [34]	187.1	-117.1
	Starlink†	Phased array antenna	250 [36]	BPSK up to 64QAM [37]	10.7 – 12.7 [38]	36.71 [39]	550	168.6	-131.9
	OneWeb†	Phased array antenna	-	16APSK [39]	11.7 [40]	34.6 [39]	1200 [40]	175.4	-140.8
Telecommunication (Backhaul)†	Starlink	Large tracking dish	21360 [41]	256-APSK (uplink) [39]	17.800 – 19.300 [39]	39.44 [39]	550	172.6	-133.2
	OneWeb	Large tracking dish	9970 [41]	256-APSK (uplink) [39]	17.8–20.2 [39]	38 [39]	1200	179.6	-141.6
	Telesat	Large tracking dish	36680 [41]	64-APSK (uplink) [39]	17.8–20.2 [39]	30.6–39 [39]	1000–1248 [39]	179.0	-144.2
	Iridium	Large tracking dish	-	–	19.1 – 19.6 [30]	30 [42]	780	176.0	-146.0
Earth Observation	Terra/Aqua (Direct Broadcast)	Large tracking dish	13.125 [43]	QPSK	8.1 [43]	15.81 [43]	710	167.6	-151.8
	Planet Labs Dove†	Large tracking dish	120 [44]	QPSK – 32-APSK [44]	8.15 [45]	8.2 [46]	500 [46]	164.7	-156.5
CubeSat	FUNcube	Tracking dish	0.0012 [47]	BPSK	0.145935	-4	600	131.3	-135.3

Table 4: The minimum attacker power required at the receiver ($P_{a,min}$), to successfully overshadow a representative sample of satellite systems. P_v derived from Section 6.3, Table 3. $\beta(N_0)$ derived from Section 6.1, Table 1. ΔG derived from Section 6.2, Table 2. $P_{a,min} = P_v + \beta(N_0) + \Delta G$

Satellite Class	Satellite	P_v [dBW]	$\beta(N_0)$ [dB]	ΔG [dB]	Required P_a [dBW]
GNSS (Navigation)	GPS L1	-155.8	3.0 – 13.60	0	-152.8 – -142.2
Telecommunication (Customer)	Iridium-NEXT	-145	3.0 – 13.60	0	-142 – -131.4
	Inmarsat 3	-138.1	-0.1 – 13.00	8.7 – 30	-129.5 – -95.1
	Alphasat	-117.1	-0.1 – 13.00	8.7 – 30	-108.5 – 74.1
	Starlink (64-QAM)	-131.9	19.90 – 25.60	13.25 – 31.15	-98.75 – -75.15
	Starlink (BPSK)	-131.9	-0.1 – 13.00	13.25 – 31.15	-118.75 – -87.75
Earth Observation	Terra/Aqua (Direct Broadcast)	-151.8	3.0 – 13.60	14.1 – 30	-134.7 – -108.2
	Planet Labs Dove (QPSK)	-156.5	3.0 – 13.60	14.1 – 30	-139.4 – -112.9
CubeSat	FUNcube	-135.3	-0.1 – 13.00	14.1 – 30	-121.1 – -92.3

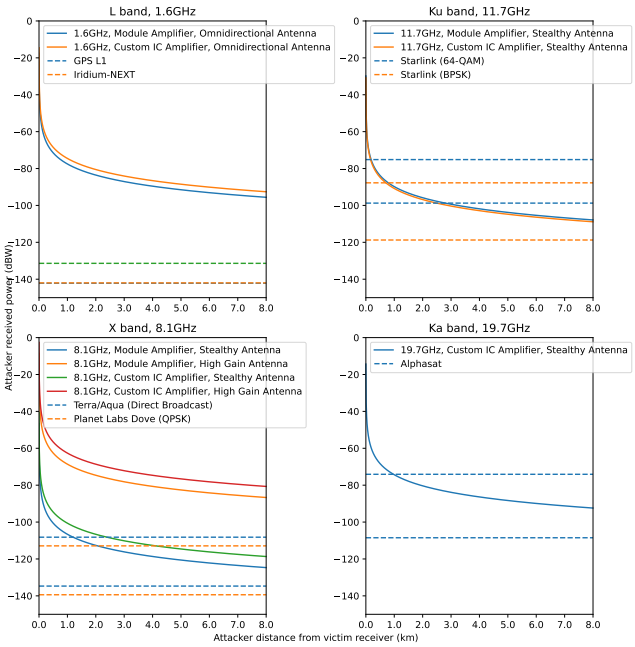


Figure 7: Attacker received power achieved as distance from the receiver varies, using the equipment budgeted in Table 5. Dashed lines represent $P_{a,min}$ at upper (max attenuation within 60°of the main lobe, max receiver noise) and lower bound (sidelobe, no receiver noise).

only the minimum power needed for reliable transmission is used on board the satellite. Since a successful attack depends upon achieving a received power of at least $\beta(N_0)$ over the victim, jumps in received power of this or greater can be compared to the known reasonable values. Applying an amplitude based protection means that the attacker can only transmit when the satellite received power is well below the maximum that the ground station expects at the given time, for example when just over the horizon or in adverse weather conditions.

8.2 Multi-receiver data comparison

Many satellite operators, particularly large organizations, will have multiple ground stations. This is done in order to increase their coverage, and hence the fraction of time when they can communicate with satellites. This allows two methods to detect forged signals: if the satellite downlinks the same data to multiple ground stations separately, or if the satellite transmits the data in view of multiple ground stations, then the stations can compare the received data, and ensure that they are identical. In the case of NASA's EOS fleet, such a system could be achieved by working alongside organizations currently operating their own EOS ground stations to compare data in an automated fashion, providing a significant boost to security at a fairly minor engineering cost. There are a large number of organizations capable of receiving downlinked EOS signals (168 at the time of writing [51]) spanning the entire globe, so it should be possible to compare signals received by a number of these ground stations to provide improved security for everyone involved. An attacker can overcome this by setting up near all the ground stations, however this greatly increases their logistics complexity and cost.

8.3 Multi-receiver timing analysis

Ground station operators who can rely on multiple dishes simultaneously receiving the same downlink can perform Time Difference

Table 5: Table of budget estimates for multiple satellite systems, in different frequencies. The attacker can choose between pricey COTS hardware, and connectorized amplifiers, or designing a custom system using RF Integrated Circuits (ICs) at a lower cost. *: ETL Systems BUCX5-860-7212, BUCK1-107-7208, BUCK1-117-7209, BUCKX-192-7210 †: Qorvo QPA2237, QPA2598, TGA2752-SM, QPA2598, TGA4548 ‡: Mini Circuits ZHL-5W-2GX+, ZHL-10W-2G+, ZVE-3W-183+ §: Any GPS patch antenna, Chelton FPA21-16L/1258, RF HAMDESIGN dish feed, RF HAMDESIGN 1m mesh dish, Fairview Microwave FM9854B/NF-20, Excel Wireless ZDAA03U018D-V34

Target		Upconverter			Amplifier		Antenna	
Freq [GHz]	Systems	New COTS	Used COTS	Custom hardware	Module	RF IC +$100 PCB	Stealthy	High gain
1.6, L band	GNSS, Iridium		Not needed		$1086, 7dBW‡ $1604, 10dBW‡	$134, 10dBW†	~$20, 0dBi§	21dBi§
8.1, X band	Aqua/Terra, Planet Labs	$9000, -10dBW*		~$100 [49]	$1638, 4dBW‡	$80, 3dBW† $144, 10dBW†	$106, 0dBi§	$106 + $325, 38dBi§
11.7, X/Ku band	Starlink, OneWeb	$9000, -3dBW*		~$100 [49]	$1638, 4dBW‡	$80, 3dBm†	$106, 0dBi§ $1700, 20dBi§	$106 + $325, 38dBi§
19.7, Ka band	Inmarsat, Alphasat	$19300, -5dBW*	$500-2000			$200, 10dBW†	$750, 34dBi§	

of Arrival (TDOA) analysis – measuring the small (approximately 1 µs to 10 ms) differences between the arrival of the signal to determine the direction of the source, and ensure it is consistent with the direction of the satellite. This has previously been demonstrated to be a viable method of authenticating satellites [52]. To attack such a system, the attacker must set up next next to all base stations, compute the expected time differences, and emit the attacking signals at exactly the right time. Due to the buffered nature of many SDR software pipelines, this poses additional technical difficulties.

8.4 Dummy receiver

The attacker's signal must overcome the large gain of the satellite dish, and hence will be significantly louder at the position of the dish than the legitimate signal. A second, omnidirectional antenna can be placed next to the dish, and connected to a monitoring receiver. The legitimate signal will be too weak to be picked up by the omnidirectional antenna with 0 gain, but it will be able to pick up and detect the attacker signals easily. This is akin to countermeasures employed to defend sensor systems against intentional analog interference attacks through the use of secondary sensors that detect only the out-of-band attack signal but not the legitimate measurement [53]. This countermeasure is not possible for systems using omnidirectional antennas, such as Iridium or GPS, but is feasible for any system using high gain directional basestations.

8.5 Physical-layer analysis

The radio signal itself can also be inspected to detect or prevent spoofing attacks. When a victim signal is overshadowed by an attacker, a number of factors will be affected, including the amplitude, SNR, phase, and doppler shift of the signal. These can be measured to provide real-time alerts of spoofing attacks. Existing research demonstrates the feasibility of this technique in aviation – Miralles et al. show that spoofing and jamming attacks can be consistently detected by measuring both the level of the Automatic Gain Control (AGC) on the receiver, and the carrier-to-noise power density (C/N_0) [54]. Manesh et al. also demonstrate success in detecting GPS spoofing attacks by using neural networks on features extracted from the signal [55].

It is also possible to identify the transmitter itself by looking at impairments on the signal created by small differences in the transmitter hardware. Such *fingerprinting* techniques provide a method of authenticating the transmitter, potentially preventing spoofing attacks. There is a large body of research in this area, focusing on terrestrial networks [56]. Fingerprinting satellite systems is more difficult due to increased atmospheric noise and multipath distortion, but recent work is showing promise even in these more difficult conditions [57, 58].

9 CONCLUSION

We have demonstrated that signal overshadowing attacks against real world satellite systems are feasible over long distances against nearly all tested satellite systems, for a budget of ~2000 USD or less. This represents a significant shift to the traditional threat model of attacks on satellite systems, enabled by increasing availability of software-defined radios and suitable upconverting and amplifying hardware.

Through simulations and real-world experiments, we analyze the contribution of modulation characteristics, victim signal power, and out-of-beam attenuation to attack success. In particular, we identify that despite their increased resilience to random noise, sparser constellations with more error correcting potential are actually more vulnerable to overshadowing attacks. We also note that attackers whose signals would otherwise be highly attenuated by transmitting out-of-beam can take advantage of sidelobes to achieve increased gain.

These results draw attention to yet another danger of satellite downlinks remaining largely unauthenticated, underlining the importance of new space systems implementing cryptography. Since upgrading existing satellites is infeasible, we have also discussed the extent to which overshadowing attacks can be mitigated without the use of cryptography, instead relying on physical-layer and timing analysis, or the use of dummy receivers.

With the cost of executing overshadowing attacks only set to decrease, satellite operators must move quickly to implement suitable countermeasures.

REFERENCES

[1] Cybersecurity & Infrastructure Security Agency. 2022. Strengthening Cybersecurity of SATCOM Network Providers and Customers. Retrieved Feb. 18, 2023 from https://www.cisa.gov/uscert/ncas/alerts/aa22-076a.

[2] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. 2019. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE. In *28th USENIX Security Symposium (USENIX Security 19)*, 55–72.

[3] Simon Erni, Martin Kotuliak, Patrick Leu, Marc Roeschlin, and Srdjan Capkun. 2022. AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks. In *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, 743–755.

[4] Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir. 2019. Wireless Attacks on Aircraft Instrument Landing Systems. *28th USENIX Security Symposium (USENIX Security 19)*, 357–372.

[5] 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.

[6] OSQZSS. 2018. GPS-SDR-SIM. Retrieved Nov. 29, 2022 from https://github.com/osqzss/gps-sdr-sim.

[7] Eric Horton and Prakash Ranganathan. 2018. Development of a GPS Spoofing Apparatus to Attack a DJI Matrice 100 Quadcopter. *The Journal of Global Positioning Systems*, 16, 1, 1–11.

[8] Anonymous Authors. 2023. Firefly: Spoofing Earth Observation Satellite Data through Radio Overshadowing. In *NDSS Workshop on Security of Space and Satellite Systems (SpaceSec)*. Accepted but not yet published.

[9] James Pavur, Daniel Moser, Vincent Lenders, and Ivan Martinovic. 2019. Secrets in the Sky: On Privacy and Infrastructure Security in DVB-S Satellite Broadband. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 277–284.

[10] James Pavur, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2020. A Tale of Sea and Sky: On the Security of Maritime VSAT Communications. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1384–1400.

[11] sam210723. 2018. COMS-1 LRIT Key Decryption. Retrieved May 9, 2022 from https://vksdr.com/lrit-key-dec.

[12] sam210723. 2020. Receiving Images from Geostationary Weather Satellite GEO-KOMPSAT-2A. Retrieved May 9, 2022 from https://vksdr.com/xrit-rx.

[13] Mark Manulis, Chris P Bridges, Richard Harrison, Venkkatesh Sekar, and Andy Davis. 2021. Cyber Security in New Space. *International Journal of Information Security*, 20, 3, 287–311.

[14] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2015. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. *IEEE Communications Surveys Tutorials*, 17, 2, 1066–1087. DOI: 10.1109/COMST.2014.2365951.

[15] Zhenhua Li et al. 2017. FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. In *NDSS*.

[16] Dimitrios-Georgios Akestoridis, Madhumitha Harishankar, Michael Weber, and Patrick Tague. 2020. Zigator: Analyzing the Security of Zigbee-Enabled Smart Homes. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 77–88.

[17] Zhijun Wu, Yun Zhang, Yiming Yang, Cheng Liang, and Rusen Liu. 2020. Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. *IEEE Access*, 8, 165444–165496. DOI: 10.1109/ACCESS.2020.3022294.

[18] Maryam Motallebighomi, Harshad Sathaye, Mridula Singh, and Aanjhan Ranganathan. 2022. Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals. (2022). DOI: 10.48550/ARXIV.2204.11641.

[19] Richard Zoglin. 1986. Video: Captain Midnight's Sneak Attack - A daring video intruder airs the beefs of dish owners. Time Magazine. (May 1986). Retrieved Sept. 1, 2023 from https://content.time.com/time/subscriber/article/0,33009,961333,00.html.

[20] 2011. 2011 Report to Congress of the U.S.-China Economic and Security Review Commission. U.S.-China Economic and Security Review Commission. Retrieved May 30, 2022 from https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf.

[21] 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*, 250–260.

[22] Great Scott Gadgets. 2014. HackRF One. Retrieved Feb. 15, 2023 from https://greatscottgadgets.com/hackrf/one/.

[23] Claude E Shannon. 1949. Communication in the Presence of Noise. *Proceedings of the IRE*, 37, 1, 10–21.

[24] NASA GSFC. 2002. *EOS PM-1 SPACECRAFT TO EOS GROUND SYSTEM INTERFACE CONTROL DOCUMENT*. NASA GSFC. (Mar. 2002). Retrieved May 13, 2022 from https://directreadout.sci.gsfc.nasa.gov/links/rsd_eosdb/PDF/ICD_Space_Ground_Aqua.pdf.

[25] Jérôme Leclère, René Landry Jr, and Cyril Botteron. 2018. Comparison of L1 and L5 Bands GNSS Signals Acquisition. *Sensors*, 18, 9, 2779.

[26] Joe Mehaffey, Jack Yeazel, Sam Penrod, and Allory Deiss. 2015. How much power do the GPS satellites output on the 1575MHz L1 frequency? gpsinformation.net. Retrieved Jan. 19, 2023 from http://gpsinformation.net/main/gpspower.htm.

[27] Peter Steigenberger, Steffen Thoelert, and Oliver Montenbruck. 2018. GNSS satellite transmit power and its impact on orbit determination. *Journal of Geodesy*, 92, 6, 609–624.

[28] European Space Agency. [n. d.] Galileo Satellites. Retrieved Jan. 19, 2023 from https://www.esa.int/Applications/Navigation/Galileo/Galileo_satellites.

[29] Spaceflight 101. [n. d.] Iridium-NEXT. Retrieved Feb. 17, 2023 from https://spaceflight101.com/spacecraft/iridium-next/.

[30] ViaLite Communications. 2021. Considering RF over Fibre links for the Iridium Satellite Network. Retrieved Jan. 19, 2023 from https://www.vialite.com/resources/white-papers/considering-rf-over-fiber-links-for-the-iridium-satellite-network/.

[31] Inmarsat. 2016. Inmarsat delivers record-breaking data rate to support small-aperture aero capability for global C4ISR. Retrieved Feb. 17, 2023 from https://www.inmarsat.com/en/news/latest-news/government/2016/inmarsat-delivers-record-breaking-data-rate-support-small-aperture-aero-capability-global-c4isr.html.

[32] Inmarsat. 2015. Strategic review of satellite and space science use of spectrum. Retrieved Jan. 19, 2023 from https://www.ofcom.org.uk/__data/assets/pdf_file/0030/49674/inmarsat.pdf.

[33] Jack Deasy. 2011. Inmarsat Update: architectures, technologies, users. (July 2011). Retrieved Jan. 19, 2023 from https://faculty.nps.edu/cdprince/mwc/docs/MWC_CONF/2011_-7_19-20_Conf/Deasy_Inmarsat_Intro_and_Program_Update.pdf.

[34] Inmarsat. [n. d.] Satellites. Retrieved Jan. 19, 2023 from https://www.inmarsat.com/en/about/technology/satellites.html.

[35] European Space Agency. 2008. Alphasat TDP#1: Broadband Data Relay. Retrieved Feb. 17, 2023 from https://artes.esa.int/projects/alphasat-tdp1-broadband-data-relay.

[36] Starlink. 2023. Starlink Specifications. Retrieved Feb. 17, 2023 from https://www.starlink.com/legal/documents/DOC-1002-69942-69.

[37] SpaceX. 2018. SpaceX Non-Geostationary Satellite System. FCC. (Nov. 2018). Retrieved Jan. 19, 2023 from https://fcc.report/IBFS/SAT-MOD-20181108-00083/1569860.pdf.

[38] 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*.

[39] Inigo Del Portillo, Bruce G Cameron, and Edward F Crawley. 2019. A technical comparison of three low earth orbit satellite constellation systems to provide global broadband. *Acta astronautica*, 159, 123–135.

[40] OneWeb. 2020. OneWeb Non-Geostationary Satellite System (LEO). FCC. Retrieved Jan. 19, 2023 from https://fcc.report/IBFS/SAT-MPL-20200526-00062/2379706.pdf.

[41] Patrick Gannon. 2019. LEO Update – The Big Three: Which is Best? Businesscom Networks. (Feb. 17, 2019). Retrieved Feb. 17, 2023 from https://www.bcsatellite.net/blog/leo-update-the-big-three-which-is-best/.

[42] Snehasis Dey, D Mohapatra, and SDRP Archana. 2014. An Approach to Calculate the Performance and Link Budget of LEO Satellite (Iridium) for Communication Operated at Frequency Range (1650-1550) MHz. *Int. J. Latest Trends Eng. Technol*, 4, 4, 96–103.

[43] NASA Goddard Space Flight Center. 1998. (Preliminary) Direct Access System User's Guide for the EOS-AM Spacecraft (ICD-107). Retrieved Jan. 19, 2023 from https://corpora.tika.apache.org/base/docs/govdocs1/391/391506.pdf.

[44] Spaceflight 101. 2016. 12 Doves – Flock 2p. Retrieved Feb. 17, 2023 from https://spaceflight101.com/pslv-c34/planet-labs-doves/.

[45] Kiruthika Devaraj, Ryan Kingsbury, Matt Ligon, Joseph Breu, Vivek Vittaldev, Bryan Klofas, Patrick Yeon, and Kyle Colton. 2017. Dove High Speed Downlink System.

[46] Kiruthika Devaraj, Matt Ligon, Eric Blossom, Joseph Breu, Bryan Klofas, Kyle Colton, and Ryan Kingsbury. 2019. Planet High Speed Radio: Crossing Gbps from a 3U Cubesat.

[47] AMSAT-UK. 2013. The AMSAT-UK FUNcube Handbook. (Nov. 2013). Retrieved Feb. 13, 2023 from https://funcubetest2.files.wordpress.com/2010/11/funcube-handbook-en_v13.pdf.

[48] European Space Agency. [n. d.] Satellite frequency bands. Retrieved Nov. 22, 2022 from https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellite_frequency_bands.

[49] Paul Wade, W1GHZ. 2016. Simple and Cheap Transverter for 10 GHz. Retrieved Feb. 17, 2023 from http://www.w1ghz.org/MBT/Simple_and_Cheap_Transverter_for_10_GHz.pdf.

[50] UK Microwave Group. 2021. 24 GHz Equipment. Retrieved Feb. 15, 2023 from https://wiki.microwavers.org.uk/24_GHz#24_GHz_Equipment.

[51] NASA. 2022. X-Band Direct Readout Sites Worldwide. Retrieved May 10, 2022 from https://directreadout.sci.gsfc.nasa.gov/?id=dspContent%5C&cid=78.

[52] 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.

[53] 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)*, 233–248. DOI: 10.1109/SP40000.2020.00026.

[54] Damian Miralles, Aurelie Bornot, Paul Rouquette, Nathan Levigne, Dennis M Akos, Yu-Hsuan Chen, Sherman Lo, and Todd Walter. 2020. An Assessment of GPS Spoofing Detection Via Radio Power and Signal Quality Monitoring for Aviation Safety Operations. *IEEE Intelligent Transportation Systems Magazine*, 12, 3, 136–146.

[55] Mohsen Riahi Manesh, Jonathan Kenney, Wen Chen Hu, Vijaya Kumar Devabhaktuni, and Naima Kaabouch. 2019. Detection of GPS Spoofing Attacks on Unmanned Aerial Systems. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 1–6. ISBN: 1-5386-5553-5.

[56] Naeimeh Soltanieh, Yaser Norouzi, Yang Yang, and Nemai Chandra Karmakar. 2020. A Review of Radio Frequency Fingerprinting Techniques. *IEEE Journal of Radio Frequency Identification*, 4, 3, 222–233.

[57] Gabriele Oligeri, Simone Raponi, Savio Sciancalepore, and Roberto Di Pietro. 2020. PAST-AI: Physical-layer Authentication of Satellite Transmitters via Deep Learning. *arXiv preprint arXiv:2010.05470*.

[58] Mahsa Foruhandeh, Abdullah Z Mohammed, Gregor Kildow, Paul Berges, and Ryan Gerdes. 2020. Spotr: GPS Spoofing Detection via Device Fingerprinting. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 242–253.