Firefly: Spoofing Earth Observation Satellite Data through Radio Overshadowing

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

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

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

Richard Baker
University of Oxford
richard.baker@cs.ox.ac.uk

Martin Strohmeier
armasuisse S+T
martin.strohmeier@armasuisse.ch

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

***Abstract*—Data from Earth Observation satellites has become crucial in private enterprises, research applications, and in coordinating national responses to events such as forest fires. These purposes are supported by data derived from a variety of satellites, some of which do not secure the wireless downlink channel effectively. This opens the door for modern adversaries to conduct spoofing attacks by overshadowing the signal with commercially available radio equipment.**

In this paper, we assess the vulnerability of current Earth Observation systems to spoofing attacks conducted at the physical layer. The effect of these attacks is amplified since the data is received at dedicated ground stations and distributed to hundreds of downstream systems, which are themselves not designed with security in mind. Specifically, we take NASA's live forest fire detection system as a case study, and demonstrate that the attacker can achieve arbitrary manipulation of fires in the derived dataset to trigger false emergency responses or mislead crisis analysis. We also assess the attack surface presented by ground station software which implicitly trusts data from the RF port. Against the NASA system we uncover several new vulnerabilities that can be exploited to stealthily deny service.

We conclude with a discussion of physical-layer countermeasures to detect and defend against spoofing, which can be implemented in existing deployments at the ground station.

Fig. 1: An overshadowing signal from the attacker manipulates the infrared channels of satellite imagery to create fictitious fires in the resulting dataset.

I. Motivation

Earth Observation (EO) satellite derived data has become a key part of critical infrastructure in use cases such as forest fire detection and analysis of activities in conflict areas. Although certain commercial satellites are being launched which cryptographically authenticate the downlink [5], even some of the latest EO satellites do not provide an authenticated downlink, such as JPSS-2 which was launched in 2022 [34], [38]. We furthermore inherit a legacy of satellite systems built when robust cryptography was uncommon due to less powerful onboard avionics. Since these satellites cannot be retrospectively upgraded, we therefore expect that critical EO data will continue to be transported in an unauthenticated wireless channel for the foreseeable future.

This opens the door for spoofing attacks, where an attacker can transmit a maliciously crafted radio signal to affect the data received at the decoder. The ground station software itself can be targeted in this manner by the insertion of malicious data. However unlike other satellite systems, EO satellite data is unique in its distribution model; in general, dedicated ground stations receive and process the raw satellite data, which is distributed over the internet to vast numbers of users. This amplifies the impact of an EO system attack across the downstream systems, which increasingly include satellite data startups, research activities, and government programs [4], [20], [29].

The dedicated groundstation model also increases the effectiveness of anti-spoofing countermeasures, which can be applied centrally and can therefore afford to be more computationally intensive.

Recent decades have seen a significant rise in the off-the-shelf availability of software-defined radio (SDR) hardware, capable of emitting arbitrary signals at a wide bandwidth.

Workshop on Security of Space and Satellite Systems (SpaceSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-89-4
https://dx.doi.org/10.14722/spacesec.2023.231879
www.ndss-symposium.org

This lowers the barrier to entry for spoofing attacks significantly [25]. In other satellite contexts such as GNSS, SDR attacks are known to result in attackers exercising control over the calculated location, as well as affecting downstream systems which rely upon the timing and position data [58], [16], [46], [40]. Spoofing attacks have also been shown against the uplink, through both telecommand hijacking and broadcast intrusion [62], [68]. Spoofing satellite internet has also been outlined as a potential issue [44]. However, no current work explores the effect, on either the ground station or the downstream users, of spoofing attacks against Earth Observation satellites.

In this work we therefore analyze the security threat posed by spoofing attackers against the Payload Data Downlink (PDD) of EO satellites, considering both the ground station and downstream users. We achieve this through an end-to-end case study of NASA's near real time forest fire API, *FIRMS*, which is a critical downstream system of the unauthenticated satellites *Terra* and *Aqua*.

We demonstrate firstly that attackers can target the sensor readings in the infrared band to affect the received datasets, and therefore the computed positions of forest fires as seen in Figure 1; this attack technique applies directly to other EO systems, which use similar data link level protocols. We also demonstrate that, since the ground station software was not designed with arbitrary input data in mind, attackers can exploit the software and cause system-wide crashes to achieve stealthy denial of service. Although specific to FIRMS, these issues are symptomatic of the larger issue: ground stations implicitly trust data from the RF port. This work therefore draws attention to considerations in secure ground station design.

We finally discuss how these issues can be mitigated by upgrading the ground station with backward-compatible, non-cryptographic countermeasures to detect spoofing and protect users of the derived data.

II. Background

It is well known that wireless systems communicating in the clear are vulnerable to spoofing by signal overshadowing. The sufficiency of cheaply-available software-defined radio hardware in reproducing accurate signals for spoofing purposes has been demonstrated in many domains, such as in mobile internet [67], [9], GNSS spoofing [58], and avionics [53].

Whilst government regulations, academic work, and recent reports by organizations such as GOES have drawn attention to space data link security more generally, these focus on securing the telecommand or internal bus rather than the Payload Data Downlink (PDD) [11], [64], [45]. To the best of our knowledge only one academic paper considers satellite systems spoofing outside of GNSS, and this only in a theoretical scenario of internet hijacking [44]. As a result, there are open questions on the effects of successful spoofing attacks against EO satellites, both at the ground station and downstream systems which depend on the data.

A. Earth Observation data link security

Over time, attitudes to securing the physical layer have changed, especially in wireless systems, where it is well accepted that cryptography should be used to verify authenticity of origin. Unlike in terrestrial systems, where insecure devices and protocols can be easily phased out, EO satellites often produce useful data for decades after their launch, and can not be easily replaced or upgraded. Also, unlike "bent pipe" satellites which simply relay a signal, the security of the overall system can not simply be upgraded at the ground segment.

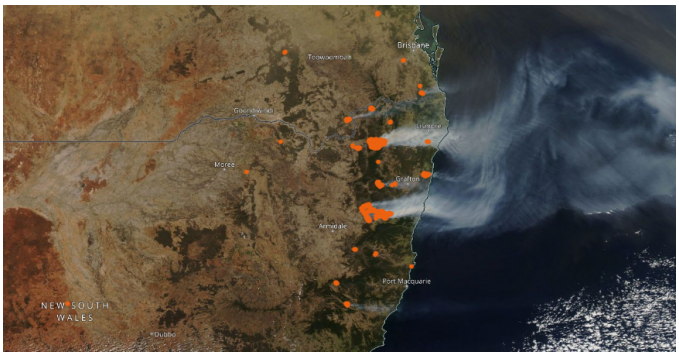


Fig. 2: The 2019 Australia bushfires as seen from Aqua's MODIS instrument, annotated with the *Fires and Thermal Anomalies* dataset on NASA's worldview.

Notably, in addition to inheriting a legacy of insecure satellite systems, even recently launched Earth Observation satellites do not always implement cryptography when downlinking data. This is due to a number of engineering constraints, including the power budget and cost of high-speed cryptographic devices, which must be reliable in the harsh environments of space.

We provide in Table I a sample of known unauthenticated or decryptable EO satellites, which are therefore vulnerable to signal overshadowing. These include unencrypted government satellites such as those in NASA's Earth Observing program and NOAA's GOES fleet, alongside the Chinese FengYun weather satellite series.

Additionally, there are certain authenticated PDDs that were secure at launch, but are now considered insecure. For example, the Korean satellite COMS-1 uses single DES encryption [49], which has led to customer keys being successfully extracted from satellite data. GEO-KOMPSAT-2A additionally had its keys leaked on the Korea Meteorological Administration website, which to this day remain publicly available [50].

B. Satellite derived data sets and use cases

Attacks against EO systems are motivated by their effect on both the ground station, but also the satellite-derived datasets (SDDs) which are distributed to end users. A growing market for specific purpose SDDs has emerged, including for forest fire monitoring [29], dust storm detection [52], flood tracking [4], and analysis of activities in conflict areas [20].

Many organisations, including satellite data startups, depend upon this data to provide geospatial data intelligence services, and are therefore at risk from spoofing through signal overshadowing. An example system is FIRMS, NASA's near real-time forest fire API, as seen in Figure 2. We provide

in Table II a number of satellite intelligence datasets which depend upon this unauthenticated downlinked data.

III. Related Work

Spoofing attacks against many different wireless systems have been well explored in the academic literature, including in areas such as avionics [56], wireless telephony [67], [24], and short-range communication such as Zigbee [1]. The threat of SDR-equipped adversaries against specific systems such as LTE and instrument landing systems has also been investigated [67], [53], [9].

Recent satellite systems security work has raised concerns about the security of the data link, with a surprising number of satellites communicating unencrypted [21], [44], [43]. For example, it was demonstrated in 2020 that confidential maritime VSAT satellite communications can be received and decoded by SDR-equipped attackers from a great distance away (covering a total area of tens of millions of square kilometers), thanks to the satellites' wide beam width and unencrypted payload [44]. This work also specifies the requirements of TCP session hijacking, which take advantage of the lack of cryptographic authenticity, using a high-speed wired connection to have the attacker's signal arrive before the legitimate response.

However, to the best of our knowledge, no current work evaluates Earth Observation satellite systems against signal overshadowing attacks; the most closely related spoofing work is instead in GNSS, satellite uplinks, and aircraft protocols.

A. GNSS spoofing

GNSS is particularly vulnerable to overshadowing, due to being unencrypted and received at very low power [58], [66]. Interestingly, it has also been shown that even encrypted GNSS messages can be spoofed through replay attacks, since the calculated position depends on the arrival time of the message [28]. This work is motivated by the high impact of attacks and the ubiquity of potentially vulnerable receivers.

In comparison, Earth observation satellite receivers are less widespread, and the impact of attacking such systems is less clear. As a result, these systems have received no attention from the security community. Despite this, Earth observation satellite systems are becoming increasingly promising targets; the data is used widely, and attacks against EO uplinks have been seen in practice [62].

Similarly to Earth observation satellites, GNSS spoofing attacks rely upon transmitting fictitious GNSS signals with a sufficiently high signal gain. Several papers have provided a comprehensive review of the methods and requirements of achieving this, including calculating the correct signal to send, and getting receivers to lock on to the attacker's signal [66], [58]. It was since shown that advances in software-defined radio (SDR) hardware has lowered the barrier to entry for GNSS spoofing; nearly any device using civilian GNSS can be spoofed using only a cheap SDR and open source software [42], [15].

Earth observation satellite communications share many similar physical characteristics with the GNSS wireless channel, and therefore face similar risks. However, creating fictitious data is significantly more difficult due to the increased complexity of EO protocols over GNSS. Frequency-dependent channel characteristics, different receiver power levels, and antenna directionality all additionally increase attack complexity at the physical layer.

Many GNSS anti-spoofing countermeasures have been proposed, which were classified in a 2012 paper by Jafarnia-Jahromi et al. in [17]. These broadly rely either upon GNSS-specific factors such as measuring clock consistency [3] or correlating with other satellite signals, cryptographic authentication, or signal processing methods such as measuring signal quality or spatially correlating the received signals. However, countermeasures based on signal processing methods are considered impractical in most contexts, since GNSS is often implemented in cheap embedded hardware.

In comparison, EO signals are received at dedicated ground stations, which have the capability to run expensive signals analysis. In this setting, existing anti-spoofing countermeasures that were considered impractical in GNSS deployments become possible. We explore these existing countermeasures, and their application to EO anti spoofing, in Section VII.

B. Satellite uplinks

Previous overshadowing attacks against the satellite uplink have been demonstrated in satellite television. One particularly famous incident was the *Captain Midnight broadcast signal intrusion*, where an operations engineer abused satellite transmitting equipment to overshadow a legitimate broadcast. This raised concerns that other satellite communications could be compromised through similar means [68].

These attacks have been successfully countered by increasing the terrestrial transmitter power, requiring that the attacker build or hijack a high power uplink station, of which there were only about 200 in the USA at the time [7]. Whilst EO satellites cannot simply be made to transmit at higher power, attackers targeting ground stations must be in the vicinity, making them significantly more traceable. This aspect is considered in Section VII.

C. Aircraft protocols

The security community has also explored spoofing in an avionics context, where unencrypted protocols such as ADS-B are used to communicate state between aircraft and air traffic control. Spoofing attacks have long been understood as a threat to these systems, with attackers able to create fictitious aircraft, mask existing ones, or hijack the communications link to a specific aircraft [65], [55], [13]. These are possible because the wireless channel is unauthenticated, due to the sunk cost of maintaining compatibility with existing hardware and legal barriers. This lack of authentication, alongside the shared nature of the channel, leads to plausible deniability of message spoofing [56].

In contrast, EO systems are not shared channels, instead being point-to-point data links. This increases the effectiveness of countermeasures based on fingerprinting, since the exact properties of the legitimate transmitter are known. We discuss this further in Section VII.

TABLE I: List of unauthenticated or decryptable Earth observation satellites, including some examples of the data users. The cited sources verify either the lack of encryption or how to decrypt the data.

Satellite	Launch Date	Usage	Provider	Encrypted
Terra, Aqua	1999, 2002	Fire detection and management, water flow monitoring	NASA	Unencrypted CADU [33]
NOAA-20/21 (JPSS-1/2)	2017–2022	Weather monitoring	NOAA	Unencrypted [34]
Landsat-7,8,9	1999–2021	Agriculture, geology, surveillance	NASA/US Geological Survey	Implied unencrypted [10]
FengYun-1,2,3,4 series	2002–2021	Meteorological monitoring in China	Chinese government	Unencrypted [12]
GOES-14,15,16,17	2009–2018	Weather forecasting, severe storm tracking, meteorology research	NOAA	Unencrypted LRIT/HRIT [48]
GK-2A	2018	Meteorological monitoring in Asia-Oceana	Korean Meteorological Association	Decryptable data link, leaked keys [48], [50]
Meteosat-8,9,10,11	2002–2015	Meteorology	EUMETSAT	Unencrypted DVB-S2 (also in GPM network) [57]
Meteor-M No. 1,2	2009,2014	Meteorological monitoring in Russia	Roscosmos/Roshydromet	Unencrypted LRPT [12]
Metop-A,B	2006,2012	Infrared sensing	ESA	Unencrypted [12]
Suomi-NPP	2011	Climate and ozone monitoring, weather	NOAA	Unencrypted [34]
NOAA-15,18,19	1998–2009	Weather monitoring	NOAA	Unencrypted APT [8]
Oceansat-2	2009	Ocean monitoring	Indian Space Research Organisation	Unencrypted [26]
CloudSat	2006	Cloud, climate, global warming	NASA	Unencrypted – SatDump support [2]
MTSAT-1R,2	2005,2006	Weather, aviation control	Japan Meteorological Agency	Unencrypted [57]
Aura	2004	Air quality, climate	NASA	Unencrypted, shown in picture being decoded [26]

TABLE II: Information on a number of organizations and satellite derived datasets which depend on satellite data transmitted via insecure wireless link.

		Satellites		
Organization	Usage	Provider	Nature	Data Access
NASA FIRMS [29]	Fire detection and management	Terra, Aqua, Suomi NPP	Self-operated	Open access
Google Maps [27]	Mapping and navigation services	Landsat-7,8	Commercial	Commercial
Cloud to Street [4]	Flood tracking (disasters and insurance)	NASA (Terra/Aqua)	Open access	Commercial
NCX Basemap [39]	Timber and carbon value monitoring in the USA	Landsat-8	Open access	Commercial
Upstream Tech HydroForecast [60]	Water flow and weather intelligence	NASA (Terra/Aqua)	Open access	Commercial
Ursa Space [61]	Oil and gas intelligence	SAR satellites (seemingly from Terra, Aqua, Landsat)	Commercial	Commercial
Descartes Labs [22]	Geospatial data intelligence	Terra, Aqua, GOES-16,17, Landsat	Commercial	Commercial

IV. Threat Model

The goal of the adversary is to manipulate the data received at a satellite receiver by emitting a sufficiently high power signal in its vicinity. The objective is to either affect the data received by the ground station, causing malicious data to be distributed downstream, or instead to target the ground station processing software itself by transmitting malformed packets.

The attacker has access to an off-the-shelf software-defined radio, which can produce signals within the 0–6 GHz range. This frequency range is below most PDD systems, which operate in the X-band (8–12 GHz) and above, requiring the attacker obtain an additional upconverter and high frequency power amplifier. Due to the low demand for radio equipment in these bands, this off-the-shelf hardware is expensive. However, the amateur radio community has produced guides on assembling suitable upconverters for ~100 USD and amplifiers at very low prices [63], [19].

We also assume the attacker is able to maintain a presence in the vicinity of the receiver, or has a suitably directional antenna, in order to transmit signals of a sufficient strength that they will be picked up by the receiver. Again the amateur radio community has shown that an attacker can cheaply acquire very large dishes without raising regulative eyebrows (up to 4.5m diameter from *https://www.rfhamdesign.com*). We consider further empirical analysis of a specific transmitter setup out of scope for this work.

The attacker additionally has either limited or complete knowledge of the communications protocol, which may be derived from public documentation or reverse engineering the signals. We go on to model how these constraints affect the required budget in real-world systems.

Affecting the satellite-derived datasets:

- Spoofing resulting in false data to mislead people – for example, to disrupt automated systems for forest fire and other anomaly detection;
- Masking important data to deny people information – for instance, to hide approaching natural disasters.

Exploiting or disrupting downlink processing stages:

- Achieving denial of service – for example, causing processing pipeline stages to crash or output malformed data;
- Executing arbitrary code – for instance, exploiting boundaries between processing applications that have access to the shell.

V. Case study: NASA's forest fire API

In this section we explore the underlying architecture and security of *Fire Information and Resource Management System* (FIRMS), NASA's near real time forest fire API and a downstream system of the satellites *Terra* and *Aqua* [30]. These satellites are part of NASA's Earth Observing System fleet, and communicate using an unauthenticated Payload Data Downlink (PDD). We explore how overshadowing attacks on the physical layer opens this system to the misclassification of forest fires, as well as software exploits at the ground station.

A. Mission architecture

FIRMs provides a worldwide map of active forest fires, each with precise coordinates and a confidence value. A near real-time fire notification service is provided which is used for

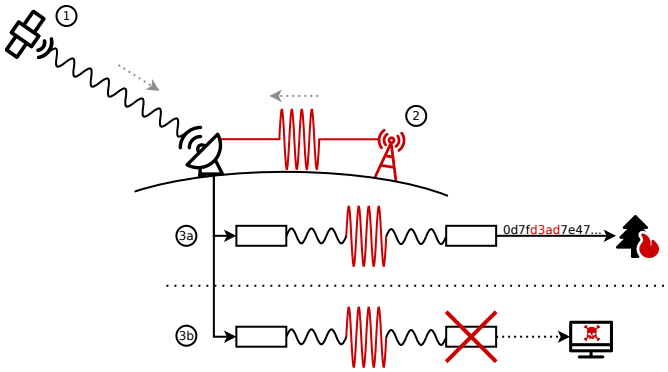


Fig. 3: An illustration of the attacks described in this paper. The attacker is indicated in red. 1) The satellite broadcasts a signal; 2) A ground-based attacker injects a crafted signal, overshadowing the legitimate signal and resulting in one of two scenarios; 3a) The victim receiver decodes the attacker-controlled data, poisoning derived datasets; 3b) The injected signal exploits vulnerabilities in the protocol decoders, resulting in denial of service or arbitrary code execution.

TABLE III: Summary of the open source toolkit for manipulating MODIS data, built for this paper. *https://github.com/ssloxford/firefly*

Library	Tool	Definition
`libgiis`[3]	`modismaskfires`	Processes SPP packet streams to manipulate fire data channels.
`libspp`[4]	`sppinfo`	Displays the header contents of a SPP packet stream from stdin.
	`sppfilter`	Filter SPP packets that match any given selector from stdin to stdout.
	`spppack`	Pack bytes from stdin into a SPP packet stream on stdout.
	`sppunpack`	Unpack a SPP packet stream from stdin to stdout.
`libcadu`[5]	`caduinfo`	Displays the header contents of a CADU stream from stdin.
	`cadupack`	Pack bytes from stdin into a CADU stream on stdout.
	`caduunpack`	Unpack a CADU stream from stdin to stdout.
	`caduhead`	Output the first part of a CADU stream from stdin, in whole CADUs, up to a given index.
	`cadutail`	Output the last part of a CADU stream from stdin, in whole CADUs, from a given index.
	`cadurandomise`	Applies the randomisation polynomial to a CADU stream on stdin.

emergency response, disaster planning, and crisis analysis, and is sent to users in more than 160 countries [32].

The *Terra* and *Aqua* satellites partially provide this data, being in polar sun-synchronous orbits to allow the entire Earth to be imaged each day. The satellites are equipped with sensors such as MODIS[1] which provides calibrated light readings, including in the infrared spectrum. These readings are used to determine hotspots on the Earth's surface, which indicate the presence of a fire.

The data is then downlinked by one of two mechanisms – either as a continuous stream known as *direct broadcast*, or via a data dump through TDRSS, NASA's relay satellites. The data link is unencrypted to enable the scientific community to set up custom receiver stations; MODIS data is thus widely available both from the central NASA archives[2] and from any of the 168 alternative receiver stations [31]. As a result, the MODIS instruments produce some of the most widely used open access satellite sensor data.

B. Protocol description

It is typically assumed, in cases such as software testing, that creating the input data for a given processing step is easy. These assumptions do not hold in radio systems; creating a sufficiently authentic signal requires imitating not just the complex protocol, but also the coding and modulation schemes. Unfortunately, software to reencode these formats is, in general, not available.

Terra and Aqua specifically downlink data in the custom *Channel Access Data Unit* (CADU) data frame. This structure is a physical channel coding block including a synchronisation header, bit randomisation scheme, and Viterbi encoding. Inside is the *Code Virtual Channel Data Unit* which provides a checksum, and the *Virtual Channel Protocol Data Unit* which provides a multiplexing header and data zone. This full structure is detailed in the relevant technical documents [33].

The MODIS sensor readings are contained within the data zone as CCSDS SPP (Space Packet Protocol) packets, packed in the GIIS format [6]. We provide a simplified illustration of the frame headers and structure of the data zone in Figure 4.

We have contributed tools to decode and reencode the *CADU*, *SPP*, and *GIIS* formats, as well as a tool to manipulate fire positions specifically. These are described in Table III.

C. Generating fictitious data

In this scenario, the attacker's objective is to generate fictitious MODIS data which decodes correctly but results in false sensor readings in a particular area. In particular, by manipulating the infrared channels of existing MODIS packets, they hope to either cause fictitious forest fires in the resulting SDD, or to mask existing ones. However, achieving this in practice is non-trivial, requiring that the attacker-produced data is sufficiently realistic to pass validation.

1) Overcoming geolocation checks: In order to affect fires in a certain area, the attacker must consider both the infrared and visible light sensor readings. This is because the precise position of each sensor reading is determined by correlating the visible spectrum image with a terrain map of the Earth's surface, through software known as *MODISL1DB_SPA*[6]. As a result, the easiest approach for the attacker is to modify legitimate MODIS data, derived from historical archives. Alternatively, the attacker can process the data in real-time if the attacker also has receiving hardware.

[1]Moderate Resolution Imaging Spectroradiometer
[2]https://ladsweb.modaps.eosdis.nasa.gov/

[3]https://github.com/ssloxford/libgiis
[4]https://github.com/ssloxford/libspp
[5]https://github.com/ssloxford/libcadu
[6]The MODIS Level 1 Database Science Processing Algorithm

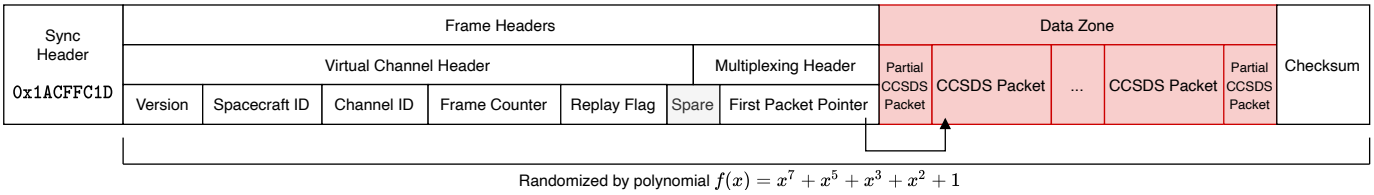


Fig. 4: Layout of data within a Channel Access Data Unit (CADU). The section marked in red can contain arbitrary attacker-specified data.

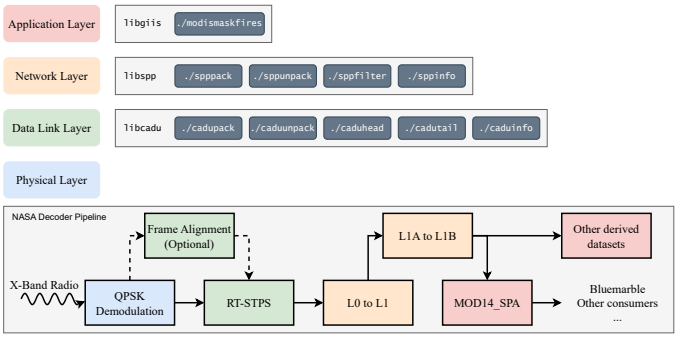


Fig. 5: Illustration of the steps involved in processing MODIS image data and derived datasets, as well as the packet structure and layer within the network stack.

2) Selecting historical data: Attackers need to select historical data from the NASA archives in the form of raw MODIS SPP packets, which is known as *Level 0* data. The attacker can target specific pixels in the image, since the sequence of packets encodes a scan over the image in a predictable pattern. The number of the scan line is indicated in the secondary header, with the *frame data count* increasing linearly throughout the scan.

3) Regenerating raw packets: Additionally, the lowest level data in the archives is MODIS SPP packets, but the attacker must transmit CADU frames. As a result, the attacker must reprocess the modified data into CADUs before transmission.

4) Overcoming forest fire sanity checks: To insert new forest fires into the data, the attacker must create hotspots at the desired locations by increasing the infrared sensor readings at the desired location. In order to be counted as forest fires, the resulting data must pass a series of checks carried out by the fire detection algorithm, *MOD14_SPA*. This includes making sure that the fire appears as a hotspot relative to its surrounding area, distinguishing smoke from cloud cover if present, and ensuring that the fire is not in water [35]. The attacker must position the fire carefully, which involves modifying the packet sequence in multiple locations at several different scan lines.

These checks make generating forest fire data more challenging; the attacker may wish to manually verify the data, or reprocess it through MOD14_SPA before transmission. As a result, generating forest fires is significantly harder to perform in real-time as opposed to on historical archives. This is unlike masking out forest fires, which can be performed trivially by smoothing out peaks in the infrared readings.

VI. Evaluation

To evaluate the effectiveness of overshadowing attacks on FIRMS, we set up a lab environment running the same decoding software pipeline as used at the NASA processing center. The code is available under the NASA open source licence, and is available with an academic account from the Direct Readout Laboratory[3]. The software pipeline takes as input the raw bytes demodulated from the radio signal, and produces a geolocated SDD of forest fires and their probabilities.

Since the existing implementations of the CADU protocol only handle decoding, we also implemented an open source library and set of command line tools to reencode the data. A summary of the tools can be found in Table III. We used these tools to reprocess archived data from NASA's archives, which we then input into the processing pipeline.

We considered three different case studies of the attack; inserting fictitious forest fires into archived data, masking existing forest fires in real time, and exploiting the decoding pipeline stages.

A. Experiment setup

The data is processed into satellite-derived datasets, which is initially decoded by RT-STPS and then processed by NASA's *International Planetary Observation Processing Package*, a software distribution for processing Earth Observing System data. The software in IPOPP contains all the necessary protocol decoding stages for satellites including Terra and Aqua, alongside their instruments including MODIS. Satellite-derived dataset generation algorithms are also distributed in IPOPP, including MOD14_SPA for detecting fires, and MOD-ISL1DB_SPA for extracting and geolocating raw MODIS data into a *Heirarchical Data Format* (HDF) [36].

However, the IPOPP framework is extremely large, measuring 35GB of source file as a compressed archive. To reduce the complexity of reproducing the results, we created a Docker pipeline containing only the relevant processing stages, alongside a simple shell script to replace the IPOPP GUI[4]. The entire pipeline can therefore be easily run on arbitrary input data, under any host operating system. A diagram of the pipeline is found at Figure 5. Sample output of running the processing pipeline can be found in the Appendix.

B. Case Study: Inserting fictitious forest fires

As a case study, we downloaded Level 0 data containing MODIS SPP packets from the NASA archives. These are raw

[3]https://directreadout.sci.gsfc.nasa.gov/
[4]https://github.com/ssloxford/firefly

CCSDS SPP packets, in files with extension `.PDS`, and can be manipulated using the SPP tools described in Table III.

In particular, we considered sensor data of the California basin in 2015 during active forest fires. The timestamp and coordinates were found through the NASA Worldview web interface, and the raw data located from the archives.

Using the tool `modismaskfires`, we are able to process the file to affect the 4 and 11 micrometer wavelength channels, which correspond to the infrared spectrum, at the desired location [6]. By randomising infrared sensor data at certain locations, fires can be inserted at specific rows or uniformly across the map. The difference between Figure 6a and Figures 1 and 6b show the results of the FIRMS software stack within IPOPP decoding the resulting signal. The commands to generate the packet sequence are shown in Appendix A.

C. Case Study: Masking existing forest fires

The attacker can also seek to mislead the fire detection algorithm through masking existing forest fires. Unlike the case of creating fictitious fires, the attacker does not need to perform geolocation of the image, greatly simplifying the operation of processing the packets. As a result, it becomes significantly easier to perform the attack in real time.

Again, the tool `modismaskfires` is capable of masking out the infrared channels at the desired location. This is achieved by setting all of the infrared channels to a roughly uniform value. This causes MOD14_SPA to detect the infrared peaks, and the resulting dataset contains no marked fires. The results can be seen in Figure 6c.

D. Case Study: Inserting malformed data

The attacker can take advantage of vulnerabilities in processing stages that do not correctly validate input data by inserting malformed data. We proceed to demonstrate how an attacker can exploit MODIS SPP packet decoding in the *L0 to L1* stage as shown in Figure 5. This results in a crash of the software pipeline, causing data loss.

The *L0 to L1* processing stage extracts MODIS data from SPP packets into a hierarchical data format using two *OceanColor Science Software* (OCSSW) [37] command-line programs, specifically `l0const_write_modis` and `l0fix_modis`. Since valid MODIS packets are always either of length 642 or 276, these lengths have been hardcoded into the programs; a crash occurs if any packet of a different length is received. A non-zero exit code from one of these programs results in a crash of the entire processing pipeline, which loses the state of the packet sequence currently being processed. By repeatedly sending bad packets, the attacker can continue to deny service. The results of this attack on the processing pipeline can be seen in Appendix B.

Software vulnerabilities such as this open the door for further attacks; `l0fix_modis` can also be made to read past the end of its allocated buffer, and its output passed directly into the shell. Furthermore, the processing algorithms in IPOPP framework contains many pre-built bundled dependencies. This includes duplicate libraries and those with active CVEs. For example, at the time of writing, MODISL1DB_SPA comes bundled with HDF5 v1.12.0, which has 11 active CVEs.

These concerns draw attention not only to potential further vulnerabilities such as code execution, but also to the fundamental issue: ground stations are designed to implicitly trust data from the RF port.

VII. Countermeasures

The ultimate countermeasure against spoofing attacks is cryptographic authentication. However, with even new satellites being launched without authenticated downlinks, spoofing through overshadowing is due to remain an effective attack against many satellite deployments in the long term.

A further countermeasure is physical defence; attackers must be transmitting at high power in the vicinity of the ground station, increasing the traceability of the signal. However, the effectiveness of this defence relies upon further countermeasures to initially detect the spoofing attack.

Therefore we consider non-cryptographic countermeasures which only require upgrading the ground station.

A. Multi-receiver data comparison

When the same satellite data is received at multiple ground stations, the received data can be compared at multiple locations. This increases the cost for the attacker, who must attack each ground station individually, and would only require minimal engineering for satellites such as *Terra* and *Aqua*, which already have many volunteer-run ground stations [31].

A similar approach has been implemented in TCCON, a network of several satellites whose measurements are compared at different locations for calibration purposes [59].

B. Timing analysis

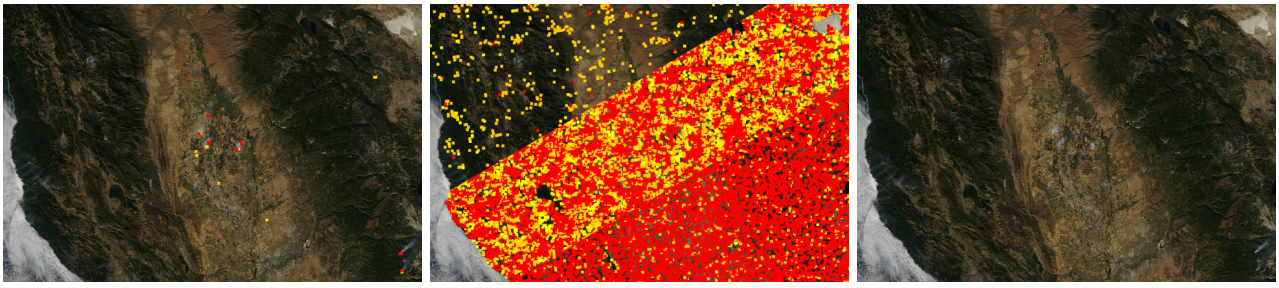
It is well known that signal timing analysis is a practical and effective mechanism to triangulate the source of a transmission [54], [14], [47]. Recent work has shown the effectiveness of this approach in satellite systems; for example, the triangulated transmitter position can be compared to the predictable orbit of a satellite to determine its authenticity [18].

Although a sufficiently sophisticated attacker can compute the expected timing differences and offset their transmission times accordingly, more accurate timing measurements drive the attacker cost up significantly. Therefore, this countermeasure is particularly effective where demodulation and decoding are performed in hardware, where the precise delay introduced from each component can be calculated.

C. Physical layer fingerprinting

In wireless systems overshadowing, the victim signal constructively interferes with the attacking signal. This introduces unique features into the received signal which can be analyzed to determine whether signal overshadowing has occurred.

Several recent papers have considered how RFI in satellites can be characterized, to distinguish overshadowing from environmental noise and accidental crosstalk. Lefcourt *et. al.* evaluated the effectiveness of a convolutional neural network to distinguish GNSS attacks [23]. Other work has considered how differences between the attacker and victim satellite



(a) Original image with some fires.

(b) Fires randomly inserted uniformly across the map.

(c) MODIS image with legitimate fires masked out.

Fig. 6: An overview of the possible ways an attacker can manipulate the output of the forest fire detection algorithm by overshadowing the downlinked data. In each image, forest fires detected by the algorithm are highlighted in yellow, orange, and red in increasing order of intensity.

transmission hardware, as well as Doppler shifting and orbital atmospheric effects can affect the received signal. Through fingerprinting, a model can be trained to identify the unique way in which the transmitting radio hardware impairs the received signal [51], [41].

Overcoming this countermeasure requires the attacker to transmit with a highly accurately timed arbitrary signal generator, significantly increasing the cost. It is most suitable at dedicated ground stations with sufficient computational power.

VIII. Discussion

We have demonstrated that signal overshadowing against satellite downlink processing systems can have a significant effect, both against the ground station as well as on downstream systems which rely upon the data.

This clearly showcases the risks that downstream satellite-derived dataset users are exposed to, stemming from previously uninvestigated insecure downlinks. We have aimed to bring awareness to these risks by mapping vulnerable satellites such as those in Table I, to the downstream systems which rely upon their data, such as in Table II. This requires a twofold reponse: ground station operators must implement countermeasures to defend against these sorts of attacks, and clearly mention that the derived data cannot be fully secured against spoofing. Furthermore, the users must build services that are resilient to poor data, potentially correlating sensor readings from multiple sources.

Furthermore, we have shown that attacks against the ground station software are possible, causing denial of service in real world NASA systems. Although specific vulnerabilities will differ for each system, similar conclusions have been made in a GNSS software security review, where multiple manufacturers were vulnerable to reporting erroneous data by making similar oversights [40]. This draws attention to a vital consideration in ground station design: that data from the RF port cannot be implicitly trusted.

There is scope for future work validating our overshadowing simulations against real-world receiver dishes, which could demonstrate the attack in practice. A comprehensive review is also required of satellite systems vulnerable to this type of attack outside of Earth observation, considering the possible effects on downstream systems which depend on their data.

IX. Conclusion

We have demonstrated that spoofing attacks against satellite Payload Data Downlinks can have a significant effect both on the groundstation and on services that depend upon the derived data. These attacks are enabled by a systemic lack of cryptographic authentication on the wireless channel of both legacy satellites and recent deployments. Although further work is required to analyze the effects of the physical channel, our initial analysis has shown that software-defined radio, and an amateur radio upconverter and amplifier are sufficient to attack high frequency downlinks with a budget under 1000 USD.

We have shown through an end-to-end analysis that major users of unauthenticated satellite data, such as NASA's near real time forest fire API, are vulnerable to spoofing attacks.

Due to the centralized data distribution model of Earth Observing systems data, attackers can cause misclassification, such as the detection of non-existant forest fires, across vast numbers of users by attacking a single ground station. Furthermore, we have demonstrated attacks against NASA's ground station software, which can be exploited through the transmission of malformed protocol data. These draw attention to the wider issue of ground stations implicitly trusting data received through the RF port.

We have furthermore discussed how the risk of these attacks can be mitigated through non-cryptographic countermeasures. Operators of ground stations and satellite data services should move quickly to understand the impact of spoofing on their service, cross-verifying unauthenticated data, and deploying appropriate defences.

Acknowledgement

We are grateful for the support from armasuisse S+T. We would further like to thank Joshua Smailes whose continuous input throughout helped shape this paper, and Jonathan Tanner for his assistance in writing the packet encoding software.

REFERENCES

[1] D.-G. Akestoridis, M. Harishankar, M. Weber, and P. Tague, "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*, 2020, pp. 77–88.

[2] Altillimity. SatDump Pipelines. [Online]. Available: https://github.com/altillimity/SatDump/tree/master/pipelines/

[3] M. T. Arafin, D. Anand, and G. Qu, "A Low-Cost GPS Spoofing Detector Design for Internet of Things (IoT) Applications," in *Proceedings of the on Great Lakes Symposium on VLSI 2017*, 2017, pp. 161–166.

[4] Cloud to Street. (2022) Cloud to Street. [Online]. Available: https://www.cloudtostreet.ai/

[5] K. Colton and B. Klofas, "Supporting the Flock: Building a Ground Station Network for Autonomy and Reliability," *Small Satellite Conference*, 2016.

[6] H. A. Company, "MODIS Command, Telemetry, Science and Engineering Description," NASA, Tech. Rep., 1997, pg. 177, 183–189. [Online]. Available: https://directreadout.sci.gsfc.nasa.gov/documents/satellite_gen/MODIS_UG.pdf

[7] Discover. (1986, 07) A signal event: on the track of Capt. Midnight - Home Box Office's transmission interrupted. [Online]. Available: https://web.archive.org/web/20050329140604/http://www.findarticles.com/p/articles/mi_m1511/is_v7/ai_4293600

[8] D. Eliuseev. (2021, 01) Decoding NOAA Satellite Images Using 50 Lines of Code. [Online]. Available: https://medium.com/swlh/decoding-noaa-satellite-images-using-50-lines-of-code-3c5d1d0a08da

[9] S. Erni, P. Leu, M. Kotuliak, M. Röschlin, and S. Čapkun, "AdaptOver: Adaptive Overshadowing of LTE signals," *arXiv preprint arXiv:2106.05039*, 2021.

[10] European Space Agency. (2022, 03) Landsat-8/LDCM. European Space Agency. [Online]. Available: https://www.eoportal.org/satellite-missions/landsat-8-ldcm

[11] GOES Commercial Remote Sensing Regulatory Affairs Office. (2022, 08) Guidance for Licensees - Cybersecurity measures. [Online]. Available: https://www.nesdis.noaa.gov/s3/2022-08/960.9%20(a)-1%20Guidance_%20Cybersecurity%20Measures.pdf

[12] "GEO Quarterly Newsletter Issue 61," Group for Earth Observation, 03 2019. [Online]. Available: http://www.geo-web.org.uk/quarterly/geoq61.pdf

[13] B. Haines. (2013) DEF CON 20 - RenderMan - Hacker + Airplanes = No Good Can Come Of This. DEF CON 20. [Online]. Available: https://www.youtube.com/watch?v=mY2uiLfXmaI

[14] J. G. Herrero, J. B. Portas, F. J. Rodriguez, and J. C. Corredera, "ASDE and multilateration mode-S data fusion for location and identification on airport surface," in *Proceedings of the 1999 IEEE Radar Conference. Radar into the Next Millennium (Cat. No. 99CH36249)*. IEEE, 1999, pp. 315–320.

[15] E. Horton and P. Ranganathan, "Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter," *The Journal of Global Positioning Systems*, vol. 16, no. 1, pp. 1–11, 2018.

[16] R. T. Ioannides, T. Pany, and G. Gibbons, "Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1174–1194, 2016.

[17] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," *International Journal of Navigation and Observation*, vol. 2012, 2012.

[18] E. Jedermann, M. Strohmeier, M. Schäfer, J. Schmitt, and V. Lenders, "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*, 2021, pp. 175–180.

[19] H. Kellock, OH2GAQ. A 10GHz Power Amplifier from Surplus components. [Online]. Available: https://www.qsl.net/oh2gaq/files/10ghz_poweramp.pdf

[20] A. Kochnev. (2018, 05) Exploring the separatist-controlled areas of Ukraine from outer space. [Online]. Available: https://www.researchgate.net/publication/328462360_Exploring_the_separatist-controlled_areas_of_Ukraine_from_outer_space

[21] A. Kurzrok, M. D. Ramos, and F. Mechentel, "Evaluating the Risk Posed by Propulsive Small Satellites with Unencrypted Communications Channels to High-Value Orbital Regimes ," *Small Satellite Conference*, 2018.

[22] D. Labs. (2023) Premium data for advanced geospatial analysis. [Online]. Available: https://descarteslabs.com/datasources/

[23] S. Lefcourt, N. Gordon, H. Wong, and G. Falco, "Space Cognitive Communications: Characterizing Radiofrequency Interference to Improve Digital Space Domain Awareness," in *2022 International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2022, pp. 1–7.

[24] Z. Li, W. Wang, C. Wilson, J. Chen, C. Qian, T. Jung, L. Zhang, K. Liu, X. Li, and Y. Liu, "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild," in *NDSS*, 2017.

[25] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber Security in New Space," *International Journal of Information Security*, vol. 20, no. 3, pp. 287–311, 2021.

[26] M. Margaras. SATELLITE FUN SOFTWARE. [Online]. Available: https://sv1cal.com/satellite-fun-software/

[27] R. Meyer. (2016, 06) Google's Satellite Map Gets a 700-Trillion-Pixel Makeover. The Atlantic. [Online]. Available: https://www.theatlantic.com/technology/archive/2016/06/google-maps-gets-a-satellite-makeover-mosaic-700-trillion/488939

[28] M. Motallebighomi, H. Sathaye, M. Singh, and A. Ranganathan, "Cryptography Is Not Enough: Relay Attacks on Authenticated GNSS Signals," 2022. [Online]. Available: https://arxiv.org/abs/2204.11641

[29] NASA. (2022) Fire Information for Resource Management System (FIRMS). [Online]. Available: https://earthdata.nasa.gov/earth-observation-data/near-real-time/firms

[30] NASA. (2022) FIRMS Frequently Asked Questions. [Online]. Available: https://www.earthdata.nasa.gov/faq/firms-faq

[31] NASA. (2022) X-Band Direct Readout Sites Worldwide. [Online]. Available: https://directreadout.sci.gsfc.nasa.gov/?id=dspContent&cid=78

[32] NASA EarthData. (2021, 10) NASA, Forest Service Partnership Expands Active Fire Mapping Capabilities. NASA EarthData. [Online]. Available: https://earthdata.nasa.gov/learn/articles/usfs-firms-us-canada

[33] *EOS PM-1 SPACECRAFT TO EOS GROUND SYSTEM INTERFACE CONTROL DOCUMENT*, NASA GSFC, 03 2002. [Online]. Available: https://directreadout.sci.gsfc.nasa.gov/links/rsd_eosdb/PDF/ICD_Space_Ground_Aqua.pdf

[34] *Joint Polar Satellite System (JPSS) Common Data Format Control Book – External (CDFCB-X) Volume VII – Part 1 JPSS Downlink Data Formats*, NASA GSFC, 01 2012. [Online]. Available: https://directreadout.sci.gsfc.nasa.gov/links/rsd_eosdb/PDF/474-00001-07-01_JPSS-CDFCB-X-Vol-VII-Part-1_0122-_20120126.pdf

[35] *MOD14 Science Processing Algorithm (MOD14_SPA) User's Guide*, NASA GSFC Direct Readout Laboratory, 01 2017.

[36] *MODIS Level-1 Science Processing Algorithm (MODISL1DB_SPA) User's Guide*, NASA GSFC Direct Readout Laboratory, 07 2021.

[37] Ocean Data Science Software Repositories. NASA. [Online]. Available: https://is.sci.gsfc.nasa.gov/ancillary/ephemeris/schedule/terra/downlink/

[38] NOAA's newest satellite heads toward orbit. National Oceanic and Atmospheric Administration. [Online]. Available: https://www.noaa.gov/news-release/noaas-newest-satellite-heads-toward-orbit

[39] NCX. (2022) What is NCX's Basemap? [Online]. Available: https://help.ncx.com/hc/en-us/articles/9757486481691-What-is-NCX-s-Basemap-

[40] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 450–461.

[41] G. Oligeri, S. Raponi, S. Sciancalepore, and R. Di Pietro, "PAST-AI: Physical-layer authentication of satellite transmitters via deep learning," *arXiv preprint arXiv:2010.05470*, 2020.

[42] osqzss. (2018) GPS-SDR-SIM. [Online]. Available: https://github.com/osqzss/gps-sdr-sim

[43] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "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*, 2019, pp. 277–284.

[44] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A Tale of Sea and Sky On the Security of Maritime VSAT Communications," in *2020 IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 1384–1400.

[45] C. I. Protection, "Commercial satellite security should be more fully addressed, US Government Accountability Office Report," GAO-02-781, August, Tech. Rep., 2002.

[46] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, 2016.

[47] L. Purton, H. Abbass, and S. Alam, "Identification of ADS-B system vulnerabilities and threats," in *Australian Transport Research Forum, Canberra*, 2010, pp. 1–16.

[48] RTL-SDR. (2019, 08) RTL-SDR.COM GOES 16/17 and GK-2A Weather Satellite Reception Comprehensive Tutorial. RTL-SDR. [Online]. Available: https://www.rtl-sdr.com/rtl-sdr-com-goes-16-17-and-gk-2a-weather-satellite-reception-comprehensive-tutorial/

[49] sam210723. (2018) COMS-1 LRIT key decryption. [Online]. Available: https://vksdr.com/lrit-key-dec

[50] sam210723. (2020) Receiving Images from Geostationary Weather Satellite GK-2A. [Online]. Available: https://vksdr.com/xrit-rx

[51] K. Sankhe, M. Belgiovine, F. Zhou, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, and K. Chowdhury, "No Radio Left Behind: Radio Fingerprinting Through Deep Learning of Physical-Layer Hardware Impairments," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 165–178, Mar. 2020.

[52] A. Sarikhani, M. Dehghani, A. Karimi-Jashni, and S. Saadat, "A New Approach for Dust Storm Detection Using MODIS Data," *Iranian Journal of Science and Technology, Transactions of Civil Engineering*, vol. 45, no. 2, pp. 963–969, 2021.

[53] H. Sathaye, D. Schepers, A. Ranganathan, and G. Noubir, "Wireless Attacks on Aircraft Instrument Landing Systems," *28th USENIX Security Symposium (USENIX Security 19)*, pp. 357–372, 2019.

[54] A. Savvides, H. Park, and M. B. Srivastava, "The Bits and Flops of the N-hop Multilateration Primitive For Node Localization Problems," in *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, 2002, pp. 112–121.

[55] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental Analysis of Attacks on Next Generation Air Traffic Communication," in *International Conference on Applied Cryptography and Network Security*. Springer, 2013, pp. 253–271.

[56] M. Strohmeier, V. Lenders, and I. Martinovic, "On the Security of the Automatic Dependent Surveillance-Broadcast Protocol," *IEEE Communications Surveys Tutorials*, vol. 17, no. 2, pp. 1066–1087, 2015.

[57] D. Taylor. Receiving Meteosat, GOES, Himawari, Metop, AVHRR and ATOVS data from the EUMETCast DVB-S2 Service. [Online]. Available: https://www.satsignal.eu/wxsat/atovs/index.html

[58] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful GPS spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*, 2011, pp. 75–86.

[59] G. Toon, J.-F. Blavier, R. Washenfelder, D. Wunch, G. Keppel-Aleks, P. Wennberg, B. Connor, V. Sherlock, D. Griffith, N. Deutscher *et al.*, "Total column carbon observing network (TCCON)," in *Hyperspectral Imaging and Sensing of the Environment*. Optica Publishing Group, 2009, p. JMA3.

[60] Upstream Tech. (2022) HydroForecast. [Online]. Available: https://www.upstream.tech/hydroforecast

[61] Ursa Space Systems. (2023) Ursa Space Systems – Satellite Intelligence Infrastructure. [Online]. Available: https://ursaspace.com

[62] (2011) 2011 REPORT TO CONGRESS of the U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. U.S.-China Economic and Security Review Commission. [Online]. Available: https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf

[63] P. Wade, W1GHZ. (2016) Simple and Cheap Transverter for 10 GHz. [Online]. Available: http://www.w1ghz.org/MBT/Simple_and_Cheap_Transverter_for_10_GHz.pdf

[64] J. M. Willis, R. F. Mills, L. O. Mailloux, and S. R. Graham, "Considerations for Secure and Resilient Satellite Architectures," in *2017 International Conference on Cyber Conflict (CyCon US)*. IEEE, 2017, pp. 16–22.

[65] A. Wood. (2006) After ADS-B launch, security concerns raised. [Online]. Available: https://www.ainonline.com/aviation-news/aviation-international-news/2006-09-14/after-ads-b-launch-security-concerns-raised

[66] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey," *IEEE Access*, vol. 8, pp. 165 444–165 496, 2020.

[67] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE ," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 55–72.

[68] R. Zoglin. (1986, 05) Video: Captain Midnight's Sneak Attack - A daring video intruder airs the beefs of dish owners. Time Magazine. [Online]. Available: https://content.time.com/time/subscriber/article/0,33009,961333,00.html

APPENDIX A
FIRE MANIPULATION PIPELINE

`modismaskfires` is used to affect the infrared channels in a packet sequence to add or remove forest fires. The `-r` flag selects only the infrared channels, `--mask-rows` which rows to mask, and `-R` a threshold for the new values.

```
cat MYD00F.A2015299.2110.20152992235.001.
    PDS | modismaskfires -r 21 -r 22 -R
    1000 --mask-rows 20
```

APPENDIX B
MALFORMED PACKET INJECTION

A packet of unexpected length is created and inserted into a valid packet sequence, causing the processing pipeline to crash and lose the image data.

```
$ printf %1337s | tr " " "f" | spppack --
    type-flag telecommand --sec-hdr-flag 1
     --app-id aqua_modis > bad_packet.PDS
$ cat bad_packet.PDS good_packet_sequence.
    PDS > ./data/MYD00F.A2015299
    .2110.20152992235.001.PDS
$ ./run_all.sh ./data/
DATA_PATH: /mnt/data/firefly/repo/
    decoder_pipeline/data
CONTAINER_RUNTIME: docker

### Processing new PDS: MYD00F.A2015299
    .2110.20152992235.001.PDS

### Running modisl1db l1a-geo initial
    processing
l0fix_modis: Unrecoverable error in
    l0fix_modis!
```