On the Security of Satellite-Based Air Traffic Control (ADS-C)

Tobias Lüscher
ETH Zürich
lutobias@student.ethz.ch

Martin Strohmeier
Cyber-Defence Campus
martin.strohmeier@armasuisse.ch

Vincent Lenders
Cyber-Defence Campus
vincent.lenders@armasuisse.ch

***Abstract*—Automatic Dependent Surveillance - Contract (ADS-C) is an satellite-based aviation datalink application used to monitor aircraft in remote regions. It is a crucial method for air traffic control to track aircraft where other protocols such as ADS-B lack connectivity. Even though it has been conceived more than 30 years ago, and other legacy communication protocols in aviation have shown to be vulnerable, ADS-C's security has not been investigated so far in the literature. We conduct a first investigation to close this gap. First, we compile a comprehensive overview of the history, impact, and technical details of ADS-C and its lower layers. Second, we build two software-defined radio receivers in order to analyze over 120'000 real-world ADS-C messages. We further illustrate ADS-C's lack of authentication by implementing an ADS-C transmitter, which is capable of generating and sending arbitrary ADS-C messages. Finally, we use the channel control offered through a software-defined ADS-C receiver and transmitter as a basis for an in-depth analysis of the protocol weaknesses of the ADS-C system. The found vulnerabilities range from passively tracking aircraft to actively altering the position of actual aircraft through attacks on the downlink and the uplink. We assess the difficulty and impact of these attacks and discuss potential countermeasures.**

I. Introduction

As air traffic continues to rise [10], *Air Traffic Control* (ATC) becomes increasingly critical and complex. Its main responsibility – preventing collisions between aircraft and maintaining an orderly flow of traffic [15] – is essential for the safety of aircraft and passengers. To achieve this mission, ATC relies on *Air Traffic Services* (ATS), which include surveillance technologies. Within continental airspaces, these technologies encompass radar systems and *Automatic Dependent Surveillance - Broadcast* (ADS-B). Notably, ADS-B relies on *Very High Frequency* (VHF) data links for communication, a mechanism operational only within the aircraft's and ground station's line of sight. Thus, there is no connectivity in more remote areas, such as oceanic airspaces. Traditionally, this challenge has been solved using voice communication over satellite links to exchange positional data between aircraft and ATC. However, as the available VHF frequencies become more congested, this is no longer a viable option [37].

More recently, with the emergence of *Future Air Navigation System* (FANS), two data link protocols have been used to solve this problem. The first protocol, *Controller Pilot Data Link Communications* (CPDLC), is used to exchange noncritical text-based messages between pilots and ATC. In doing so, voice channels are decongested and are thus available for more urgent correspondence. The second protocol, *Automatic Depended Surveillance - Contract* (ADS-C), enables the automatic transmission of aircraft's positional data to ATC. The main advantage of this protocol is its use of *satellite communication* (SATCOM) to extend connectivity to remote regions. Accordingly, aircraft's ADS-B signals are used primarily in continental airspace while ADS-C is seen mainly in oceanic airspace.

While security and privacy of ADS-B, CPDLC, and other aviation protocols have been studied extensively (see [32], [12] for some recent overviews), there is little research available on ADS-C and nothing with regards to its security. This lack of attention can be attributed to the higher difficulty associated with analyzing satellite signals compared to terrestrial ones. While the lack of existing literature addressing ADS-C security is thus explainable, it does raise some questions, particularly in light of the ongoing deployment of ADS-C-based surveillance technology to decrease aircraft separation in oceanic airspaces around the world [36].

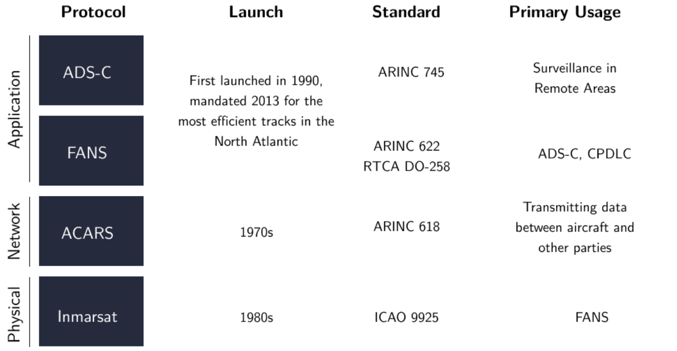
To fill this gap, this paper studies privacy and security aspects of ADS-C. We have built a receiver setup to analyze ADS-C messages and a spoofer to encode and transmit ADS-C messages. With these two primitives in mind, we create a threat model, assess vulnerabilities in the ADS-C protocol, and analyze their potential impact on air traffic control.

We offer the following contributions:

- We present a comprehensive overview of the ADS-C protocol, including relevant standards, message structure, encoding, and modulation.
- We demonstrate how a low-resource attacker can attack the ADS-C protocol by building an ADS-C receiver and transmitter.
- We conduct a security analysis of ADS-C, uncovering significant privacy and security issues in the protocol.

We provide background knowledge on satellite-based aviation protocols in (Section II) and our threat model in (Section III. Our experimental setup is described in (Section IV). We demonstrate a working transmitter in Section V, based on which we conduct our security analysis in Section VI). Lastly, we discuss the results of our approach (Section VII), provide the related work in Section VIII and conclude in Section IX.

Workshop on Security of Space and Satellite Systems (SpaceSec) 2024
1 March 2024, San Diego, CA, USA
ISBN 979-8-9894372-1-4
https://dx.doi.org/10.14722/spacesec.2024.23022
www.ndss-symposium.org



	Protocol	Launch	Standard	Primary Usage
Application	ADS-C	First launched in 1990, mandated 2013 for the most efficient tracks in the North Atlantic	ARINC 745	Surveillance in Remote Areas
	FANS		ARINC 622 RTCA DO-258	ADS-C, CPDLC
Network	ACARS	1970s	ARINC 618	Transmitting data between aircraft and other parties
Physical	Inmarsat	1980s	ICAO 9925	FANS

Fig. 1: ADS-C Protocol Overview.

II. Background

A. History and Usage

ADS-C is embedded into the Future Air Navigation Systems (FANS), envisioned by the *International Civil Aviation Organization* (ICAO) during the 1980s and presented in 1991. As is common in aviation, the rollout of new technology can take several decades, as such ADS-C and other FANS protocols have only started to see more widespread usage in the second half of the 2010s. ADS-C tackles the limitations of the prevalent (V)HF communication systems by using SATCOM as a data link layer and enabling surveillance even in remote areas. Second, ADS-C reduces the reliance on voice communication systems by automatically transmitting position updates to ground stations over digital data links.

ADS-C thus enables the substantial enhancement of separation standards – the minimum distance maintained between aircraft to avoid collisions. While the standard lateral separation was conventionally set at 50 nautical miles (nm), and longitudinal separation at 80 nm, aircraft equipped with FANS systems benefit from a significantly reduced separation standard of just 23 nm in both dimensions [36], while maintaining the same level of safety. This reduction in separation standards has led to a more efficient utilization of airspace and translated into substantial cost-savings for airlines. Initially introduced in Pacific airspace, FANS has progressively expanded its presence to encompass nearly all oceanic regions and certain continental areas. In the North Atlantic region, FANS implementation has even become a mandatory requirement [37].

B. Protocol Stack

We focus on the satellite-related layers and ADS-C (see Fig. 1 for an illustration of the stack). More information on the generic ACARS message structure and content can be found in [3], [5]. An overview is given in [38].

1) ADS-C: The term *Automatic* indicates that ADS-C operates without input from the flight crew. *Dependent* signifies that the system relies on external data, like GPS for position. *Surveillance* denotes that the protocol supplies essential monitoring data such as position, velocity, and waypoints. Lastly, *Contract* means that aircraft and ATSUs negotiate agreements to share data. While aircraft can establish concurrent contracts with multiple ATSUs, messages are exclusively exchanged between the aircraft and the ATSU with which a particular contract was established. This differs from ADS-B, where aircraft indiscriminately broadcast messages to everyone.

a) Contracts: All surveillance data from the aircraft is sent via contracts. To negotiate such a contract, the ATSU sends a contract request, containing information regarding the surveillance data the ATSU wants to receive, to an aircraft. The aircraft then responds to a contract with a positive acknowledgement and the appropriate report. In case of an error, the aircraft responds with a negative acknowledgement (if the message cannot be parsed), or a non-compliance notification (if the request contains data that is not available to the aircraft).

The type of contract then defines what information the aircraft will return to the ATSU:

- **Periodic contract**: With this contract type, an ATSU can request ADS-C reports at a specified reporting interval with following data: flight ID, predicted route, earth reference, meteorological data, airframe ID, air reference, and aircraft intent.
- **Event contract**: Whenever an event contract is established, the aircraft sends reports in the case a given event occurs. It can be requested in case of the following events: vertical range change, altitude range change, waypoint change, and lateral deviation.
- **Demand contract**: In the case of a demand contract, an aircraft only sends a single report. This can be useful, when a periodic report is not received in time.

Every ADS-C report comprises, at a minimum, a basic report detailing the aircraft's position, accompanied by a timestamp and a figure of merit. The figure of merit denotes the precision of the positional information within the report and the operational status of the *Traffic Alert and Collision Avoidance System* (TCAS). Advanced reports encompass extra data as stipulated in the ADS-C contract.

b) Modes of Operation: Contracts usually operate in *normal-mode*. Apart from *normal-mode*, ADS-C contracts can also operate in *emergency-mode*. The *emergency-mode* can be initiated by either the aircraft, which can send an emergency report, or the ATSU, which can transmit an emergency contract. Once the emergency mode is activated, aircraft send reports more frequently than in normal mode.

2) FANS: ADS-C uses FANS-1/A. It is used over the ACARS network and defined by the ARINC 622 [4] data communication standard.

To adhere to the ARINC 622 standard, FANS adds a header before the ADS-C message and appends a 16 bit CRC after the message (refer to Figure 2). The header fields encompass the message origin, an *Imbedded Message Identifier* (IMI), and the *Aircraft Registration Number* (AN). Given that ACARS operates as a character-oriented network while ADS-C is bit-oriented, a conversion is needed.

3) Classic Aero: Classic Aero is the lowest part of the protocol stack. It is a geo-stationary satellite system operated by Inmarsat and provides voice and data communication for aviation [14] since the late 1980s. Next to ADS-C over FANS it is also used for applications such as Oceanic Clearance and Digital Automatic Terminal Information Service [14].

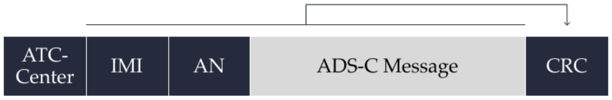


Fig. 2: FANS Message structure.

The Classic Aero system comprises an aircraft, called an *Aircraft Earth Station* (AES), that can receive and transmit data on the L-Band at around 1.6 GHz to a satellite. The satellite ground station, called a *Ground Earth Station (GES)*, can receive data from the satellite on the C-Band at 3.6 GHz, and transmit signals on 6.5 GHz. We define the *uplink* as the communication direction from GES to AES (via the satellite) and the *downlink* as the reverse.

a) Communication Channels: The communication between satellite, AES, and GES happens on four channel types. Three are data-oriented, sending so-called Signal Units (SU).

- **P Channel**: Used on the downlink for both signalling and user data. The transmission is continuous, thus there are empty packets sent when there is no user data. Multiple SUs are combined in a frame.
- **R Channel**: *Random access channel*, used on the downlink. SUs are sent individually in the form of short bursts.
- **T Channel**: *Time Division Multiple Access*, used on the downlink. An AES requests a slot to transmit data to a GES. This data is then divided into SUs and combined into one large frame, which is then transmitted in a burst.
- **C Channel**: The C channel is used in both directions to carry voice communication.

Many channels are grouped together on neighbouring frequency bands and used simultaneously by a single satellite.

b) Encoding and Modulation: Encoding in Aero depends on the channel type and data rate used to transmit messages. The specifics of this procedure are described below:

- **Channel Packets**: An SU is a structure defining header fields (such as an AES and GES identifier), user data, and a 16-bit CRC checksum.
- **Scrambler**: The user data, which is now in bite-sized pieces, next passes through a scrambler. The scrambler turns the signal units into a pseudorandom sequence of bits. This ensures easier timing recovery at the receiver and better distributes power spectral density.
- **Convolutional Encoder**: Aero uses a rate 1/2 convolutional encoder with constraint length 7. The rate parameter specifies that the encoder doubles the length of the bit sequence. The constraint length of 7 means that the encoding of one bit depends not only on the current bit but also on the six previous bits.
- **Interleaver**: After applying the error correction code, the bit sequence is interleaved, i.e. adjacent bits are evenly distributed into a new sequence of bits.
- **Modulation**: Finally, the interleaved bits are modulated and transmitted. Again, the modulation scheme depends on the data rate of the channel. For 600 and 1200 kbit/s, *Aviation Binary Phase Shift Keying* (A-BPSK) is used. For larger data rates, *Aviation Quadrature Phase Shift Keying* (A-QPSK) is applied.

As A-BPSK is an uncommon modulation scheme, we describe it in more detail in the Appendix.

III. Threat Model

We outline three distinct attackers: a passive attacker, an attacker with control over the downlink channel, and an attacker controlling the uplink channel. We exclude attackers controlling both uplink and downlink channels because we found that such attackers have no more impact than an attacker controlling only one of these channels.

- **Passive Attacker**: This attacker's actions are limited to the observation of signals. They have access to SDRs, open-source software and an interference-free environment in the ADS-C spectrum.
- **Active Downlink Attacker**: This attacker is equipped with a downlink transmitter and can overshadow legitimate signals on the ground [27]. They have knowledge of the satellite ground station's position through open sources and can get close enough and into line of sight.
- **Active Uplink Attacker**: This adversary is equipped with an uplink transmitter and sufficient transmission power. It is important to note that the attacker does not target aircraft directly. Rather it injects messages to the satellite, which then forwards the signals to the aircraft. To successfully execute uplink signal spoofing, this attacker has to know the target satellite's location. In contrast to the previous attacker, an adversary only controlling the uplink channel is not necessarily restricted to a location close to the satellite ground station.[1] However, they need large satellite dishes of several meters and significant power, putting this avenue outside of the realm of typical hobbyists.

Figure 3 illustrates the positional constraints and capabilities of the different attackers. It is worth emphasizing that while these attackers exhibit varying degrees of capabilities, all of them operate within the realm of plausibility for non-state actors, such as RF enthusiasts or hobbyists.

IV. Experimental Setup

A. Receiver

Unless the antenna is located close to a ground station or aircraft, it can only capture signals transmitted by a satellite. The first step is to identify the satellite, based on open-source information [18]. In a next step, we determine on which frequencies the chosen satellite is transmitting signals. A first reference can again be open sources [24] and [9], which indicate the approximate frequency bands. Identifying the exact frequencies to receive messages is a manual process.

[1] Unless the satellite is applying beamforming methods, which effectively constrict the location.

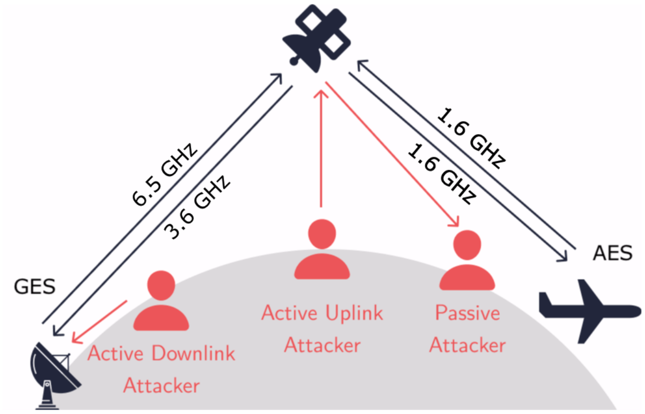


Fig. 3: System and attacker model.

Recalling that the uplink signal can be received on 1.6 GHz and the downlink signal on 3.6 GHz, a receiver requires two different setups to capture these signals. For both, we use *JAERO* [22] to demodulate and decode ADS-C signals. As JAERO can only decode one Aero channel at a time, *SDRReceiver* [16] splits digital signals into smaller frequency bands, and outputs them individually to JAERO.

1) Uplink Receiver Hardware: Receiving and decoding uplink ADS-C messages can be achieved with hardware components of around $200. We used a patch antenna with +3.5 dBi of gain at 1550 MHz, capable of receiving right hand circular polarized signals, a Nooelec SAWbird iO Low Noise Amplifier, pre-configured to a center frequency of 1.542 GHz [21], and an RTL2832U, all connected to a Raspberry Pi 4.

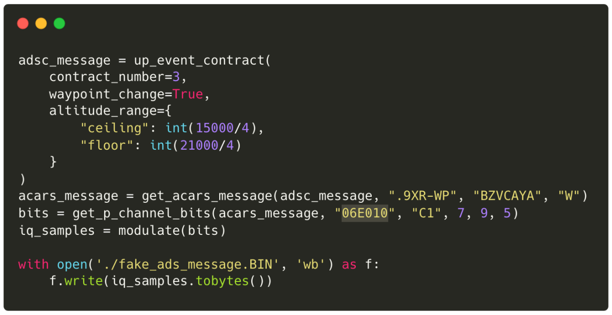
2) Downlink Receiver Hardware: As the downlink signal is much weaker than the uplink signal [13], a satellite dish is required. Additionally, the location of a downlink receiver is highly restricted because it suffers from interference with the stronger 5G signals in many jurisdictions (e.g. Europe). As we are targeting geostationary satellites, which exhibit an analemma pattern, our non-tracking dish can receive signals for about 10 hours a day.

We used the hardware at a cost of around $10'000: a stationary 2.4 meter C-Band antenna (CPI SAT Series 1252), a C-Band feed with circular polarization (FEED-VS-RP3CP300), a low-noise block downconverter (Norsat C-BAND PLL 3000), connected to an RTL-SDR RTL2832U and an Intel NUC.

B. Transmitter

Having built a receiver, we proceed to assemble an ADS-C transmitter capable of injecting messages in the uplink and downlink direction. In order to do this, we generate an ADS-C message, encode it, and then modulate it. The generation of ADS-C messages is significantly simplified by the lack of authentication in ADS-C. This process mirrors the protocol stack described in Section II and is built on a Python API.

Using the uplink and downlink receiver and publicly available documentation, we reverse-engineered the process to generate and encode ADS-C messages. This step was aided considerably by the fact that ADS-C, FANS and ACARS are well documented. However, implementing the Aero layer was more challenging. Especially the physical layer aspects of the Aero protocol – scrambling, encoding, interleaving, and modulating – were demanding, as the available documentation is rather brief and lacks necessary details. In this process, having the already working ADS-C decoding software JAERO available was crucial. Since JAERO is open-source, we modified it to deconstruct and reverse-engineer the above-mentioned physical layer aspects of Aero.



```
adsc_message = up_event_contract(
    contract_number=3,
    waypoint_change=True,
    altitude_range={
        "ceiling": int(15000/4),
        "floor": int(21000/4)
    }
)
acars_message = get_acars_message(adsc_message, ".9XR-WP", "BZVCAYA", "W")
bits = get_p_channel_bits(acars_message, "06E010", "C1", 7, 9, 5)
iq_samples = modulate(bits)

with open('./fake_ads_message.BIN', 'wb') as f:
    f.write(iq_samples.tobytes())
```

Fig. 4: Python snippet generating a waypoint and altitude range event contract. The fake message is generated to appear as it originates from the ATSU *BZVCAYA* and is destined for an aircraft with the ICAO ID *06E010*.

This API can be used to generate arbitrary ADS-C messages, as illustrated in Figure 4. The output is a file containing the modulated message in the form of IQ samples. Such a file can then be used by SDR software such as GnuRadio to transmit the messages on the desired frequency.

V. ADS-C Spoofing Proof of Concept

Due to regulatory reasons and the lack of an ADS-C capable flight computer, we do not test the ADS-C transmitter on operational equipment. Therefore, we tested the transmitter with the receiver described above. We rate a transmission as a success if JAERO is able do demodulate and decode the received signal.

A. Uplink Transmission

As not to interfere with actual ADS-C signals, we tested the uplink transmitter in an RF shield box. Within this box, we placed the uplink and downlink antennas. While the downlink antenna was connected to an RTL-SDR, the transmitter antenna was linked to an USRP B210 capable of transmitting radio signals. We connected both these SDRs to a laptop outside the box. This laptop runs both the ADS-C receiver and transmitter software. This setup is depicted in Figure 5. To simulate an actual ADS-C system as accurately as possible, the receiver was configured identically to the receiver used to eavesdrop on real ADS-C messages. Within this experiment, we were able to successfully transmit and receive fake ADS-C messages on the P-Channel with a data rate of 600 kbit/s. Note that the satellite converts the frequency on the uplink direction from 6.5 GHz to 1.6 GHz. Thus, the attack frequency would have to be scaled up accordingly when attacking the satellite.

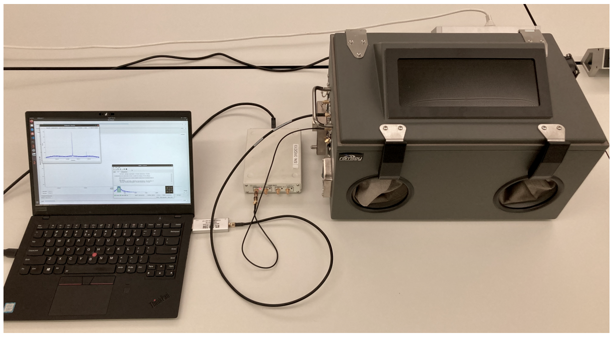


Fig. 5: Setup to test the uplink transmitter in an RF shield box. The laptop is connected to an USRP to transmit signals, and an RTL-SDR to receive them, inside the box.

B. Downlink Transmission

As the downlink receiver relies on a 2.4 meter antenna, we were unable to test the downlink transmitter in an RF shield box. However, we tested the transmitter with our downlink receiver setup. Due to regulatory constraints, we were required to test the transmitter on a lower frequency than the one used by ADS-C. This test resulted in a successful transmission of spoofed ADS-C messages using the T-Channel and a data rate of 1’200 kbit/s.

VI. Security Analysis

As there is no authentication in ADS-C, a number of passive and active attacks on the protocol are possible. We will discuss the vulnerabilities in ADS-C based on the three attacker models in the following.

A. Passive Attacker

Using the capabilities of a passive attacker, we recorded more than 60’000 uplink and 65’000 downlink messages over the span of a month. The recorded messages originate from 2’684 different aircraft operated by 114 different airlines, and 57 ATSUs.

1) Message Distribution: The overview in Table I depicts the number of messages recorded on a given frequency and bandwidth. Notably, there was an absence of R-Channel messages and downlink messages exhibiting data rates other than 10,500 kbit/s have not been acquired. We could not establish whether this was due to the satellite not utilizing them or because of an issue with the receiver setup. Even for uplink messages, 90% came from the broader channels.

2) Message Content:

a) Uplink Messages: As illustrated in Table II almost 80% of all uplink messages are contract requests. The remaining communication are either *Cancel Contract* messages (20.09%) or emergency contract requests (0.06%). We saw up to four ATSUs establishing contracts with an aircraft at the same time, leading the aircraft to transmit identical contract reports to the same ground station. The recorded uplink messages provide an attacker with the ICAO identifier of the aircraft, the contract number, and contract reporting intervals.

Frequency [Hz]	Channel	Bandwidth [kbit/s]	# Messages
3’623’623’000	T	10’500	45’557
1’546’005’000	P	10’500	30’664
1’546’020’000	P	10’500	22’829
3’623’930’000	T	10’500	21’597
1’545’118’000	P	600	4’549
1’545’128’000	P	600	4’205
1’545’123’000	P	1’200	643
1’545’163’000	P	600	13
1’545’158’000	P	600	8

TABLE I: Summary of recorded ADS-C messages over a month on different Aero channels.

Message Type	# Messages	Ratio
Contract Request	50’231	79.84%
Cancel All Contract	10’074	16.01%
Cancel Specific Contract	2’568	4.08%
Emergency Contract Request	38	0.06%

TABLE II: Types of recorded uplink messages.

b) Downlink Messages: In the downlink direction (Table III), more than 75% of all messages are contract reports. The rest of the messages are acknowledgements (23.31%), noncompliance notifications (0.13%), and emergency related messages (0.1%). The median of captured periodic reports is 5 and the median of event reports is 3 per observed flight. Most periodic reports are transmitted in a 16-minute interval. The captured messages are destined to 57 different ATSUs around the globe. All but 42 messages were exchanged over the satellite ground station in Fucino, Italy. The other messages were received by the secondary ground station in Burum, Netherlands. Table IV depicts the type of data contained in the reports.

Tracking Aircraft: Each ADS-C report includes the coordinates and altitude of the aircraft sending the message. Using these coordinates, we examined the coverage of Alphasat by plotting the position of each aircraft communicating with the satellite on a map using *libacars* [17]. The resulting aircraft positions, as well as the location of the ADS-C ground stations and involved ATSUs are depicted in Figure 6.

B. Active Downlink Attacker

As messages are almost exclusively received by only one ground station, an entity near this ground station can potentially influence all ADS-C communication received over this satellite/ground station combination .

1) Denial of Service: One way to attack ADS-C is to prevent communication between ATSUs and aircraft. As a consequence, ATC would not receive any ADS-C reports and lose the capability to surveil aircraft. ATC would have to resort to traditional voice communication over HF/VHF.

The simplest approach would be to jam the downlink signals. However, continuously jamming a satellite ground station would quickly raise suspicion. Therefore, we explore more efficient and stealthy DoS on the physical layer (Aero) and on the application layer (ADS-C).

Message Type	# Messages	Ratio
Contract Report	50’997	75.94%
Positive Contract Acknowledgement	15’611	23.25%
Negative Contract Acknowledgement	451	0.67%
Noncompliance Notification	90	0.13%
Emergency Report	4	0.01%
Cancel Emergency Mode	1	0.00%

TABLE III: Types of recorded downlink messages.

Report Group	# Reports	Ratio
Predicted Route	24’950	69.19%
Meteorological	17’604	48.81%
Flight Identification	13’615	37.76%
Earth Reference	12’816	35.54%
Air Reference	10’036	27.83%
Fixed Project Intent	227	0.63%
Intermediate Project Intent	137	0.38%
Airframe Identification	4	0.01%

TABLE IV: Report groups are included in periodic reports.

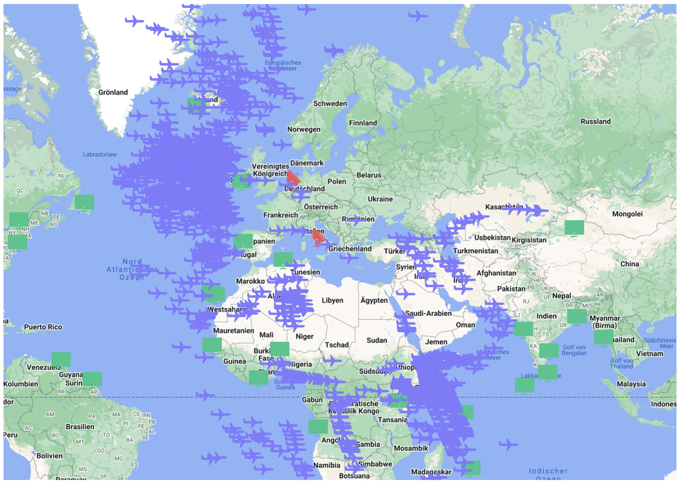


Fig. 6: Map showing aircraft’s (purple) position (extracted from ADS-C reports), ATSUs (green) communicating with aircraft, and satellite ground stations (red).

DoS via Aero Log-off: One vulnerable, unauthenticated target is the Aero log-off request. According to [13], an aircraft can send such requests at any given time. In response, the GES transmits a log-off acknowledgement and considers the aircraft as logged-off. To regain connectivity, the aircraft must re-initiate the connection.

DoS via ADS-C NACK: We recall that an ATSU initiates an ADS-C connection to an aircraft by sending a contract request. The aircraft then responds with a positive or negative acknowledgement. According to [2], upon receiving three negative acknowledgements from an aircraft, the GES will cancel all contracts and end the connection. Since an attacker can eavesdrop on uplink messages, they can send a negative acknowledgement to the GES whenever the GES requests a contract from a given aircraft.

2) Change Contract Content: Further active attacks are possible by changing the content of established contracts.

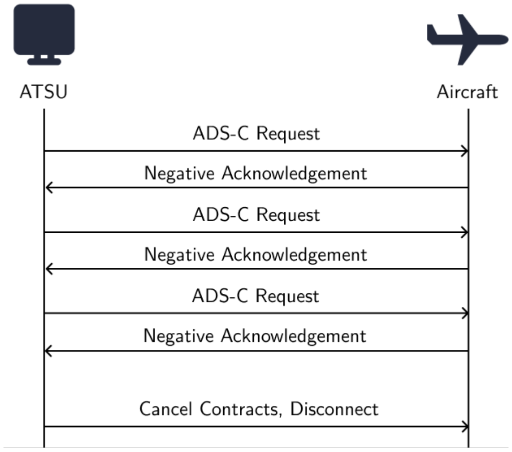


Fig. 7: Preventing communication between aircraft and ATSUs by sending three consecutive negative acknowledgements.

Fake Position: The first and most obvious attack is injecting malicious ADS-C reports with fake positional data. Since an attacker can obtain a list of active ADS-C contracts, they can generate a fake ADS-C report including the latitude, longitude, and altitude of their choosing. Since the reporting interval of the contract is sent in the contract request, an attacker can transmit the fake report a few seconds earlier than the actual report, and then jam the ground station for a short amount of time preventing the correct report from being received. Altering the position of only one aircraft has limited impact; however, it is rather easy to change the position of multiple aircraft simultaneously (see Figure 8). Similar to the *Virtual Trajectory Modification* on ADS-B described in [29], an attacker can even modify speed, heading, waypoints, and intent of the aircraft to make the deception more believable.

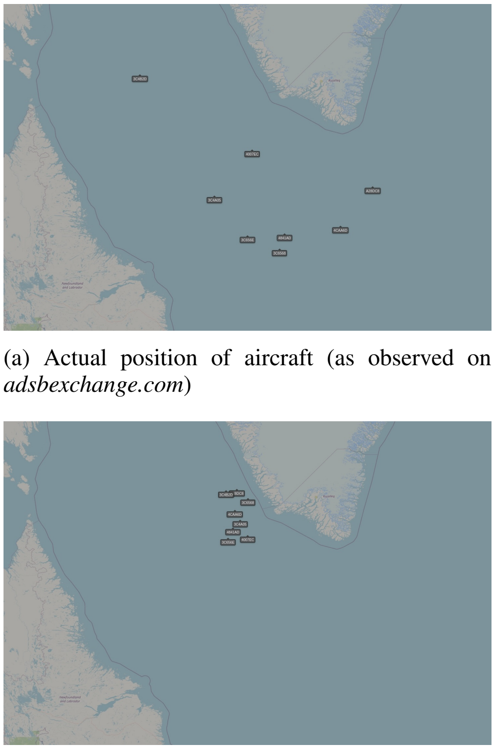
Emergency Mode Flooding: Pilots can initiate the ADS-C emergency mode. An attacker can imitate such an action by injecting an emergency periodic contract. The impact is greater if the attacker were to initiate emergency mode for not only one aircraft but tens or hundreds such as recently happened to Flightradar24 in a software-based attack [11].

Cancel Emergency Mode: When ADS-C is operating in emergency mode, the reporting interval is lowered from a few minutes to 64 seconds. The pilot can return to normal operating mode and restore the initial reporting interval by sending a cancel-emergency-mode message to the ATSU. Taking advantage of this, an attacker can transmit a single message to cancel the emergency mode of an aircraft, withholding potentially crucial information from ATC.

Ghost Aircraft: Other papers such as [29], [7] also consider ghost aircraft flooding attacks, where an attacker injects messages from non-existent aircraft to overload ATC. However, this attack is not possible with ADS-C because ATC always initiates contracts and messages from aircraft without a valid contract will simply be discarded.

C. Active Uplink Attacker

We now discuss possible attacks by an adversary controlling the uplink channel.



(a) Actual position of aircraft (as observed on *adsbexchange.com*)

(b) Fake position of aircraft after injecting malicious ADS-C reports into our setup.

Fig. 8: Aircraft positions before and after injecting fake ADS-C reports, plotted by *Virtual Radar Server*.

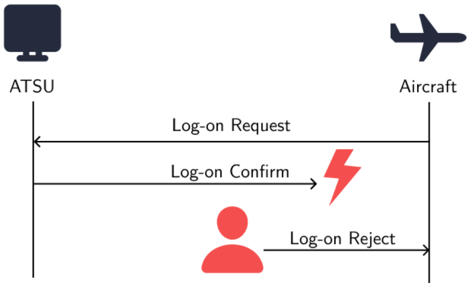
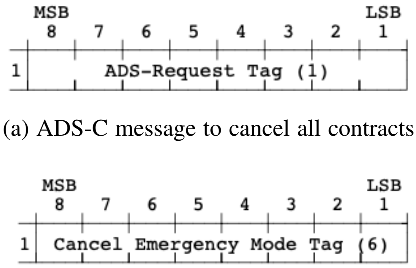


Fig. 9: Aero Handshake rejected by an active adversary.

1) Denial of Service: Several DoS attacks are possible:

DoS via Aero Log-On Reject: An efficient and stealthy DoS is found in the Aero log-on procedure, which is outlined in [13]. After an aircraft sends a log-on request, the ATSU responds with a log-on confirmation. Then, both parties exchange log-on acknowledgements. However, an attacker eavesdropping a log-on request can simply jam the log-on confirmation and inject a log-on reject message to the aircraft (see Figure 9). Having received a log-on reject message, the aircraft stops sending to the ATSU.

DoS via Aero Log Off: The downlink log-off attack can also be performed in the uplink direction by injecting a log-off message to a target aircraft.



(a) ADS-C message to cancel all contracts.

(b) ADS-C message to cancel emergency mode.

Fig. 10: ADS-C message to cancel contracts and cancel emergency mode [2].

Cancel Contracts: According to the ADS-C specification, an ATSU can cancel only one or all contracts with an aircraft at any point in time. Thus, an attacker can send such an ADS-C message (Figure 10a) to a victim aircraft, which would cause the aircraft to no longer send reports to the ATSU. Again, this attack results in ATC not having access to automatic surveillance information of the aircraft under attack and having to resort to voice communication.

2) Change Contract Content: On the uplink it is also feasible to manipulate ADS-C contracts.

Emergency Mode: It is possible to send an emergency periodic contract to the aircraft or cancel the emergency mode on the uplink (Figure 10b). As in the downlink direction, both these attacks have the potential to confuse pilots and ATC, and to deny crucial information in actual emergencies.

D. Difficulty and Impact of Attacks

We classify all attacks regarding their impact and difficulty in Table V. We use the following impact classification:

- **Low impact**: Reveals little information / likely does not cause any ATC disturbances.
- **Medium impact**: Reveals crucial aircraft information / creates some additional workload for pilot or controller, briefly affects situational awareness.
- **High impact**: Denies ADS-C communication, creates substantial additional workload, poses a risk of violating minimal separation.

To classify the difficulty of the attacks, the subsequent guidelines are applied:

- **Easy**: An attack is easy to perform if an adversary only has to eavesdrop on uplink messages or inject a single downlink messages to perform it.
- **Medium**: An attack is considered to be of medium difficulty if an attacker captures downlink messages and injects single, independent messages in the uplink or downlink direction to perform it.
- **Hard**: An attack is hard if an adversary executing it has to inject multiple uplink or downlink messages, which depend on each other in timing and content.

Vulnerability	Attacker	Impact	Difficulty
Uplink Eavesdropping	Passive	Low	Easy
Downlink Eavesdropping	Passive	Medium	Medium
Aero Log-off	Active Downlink	High	Easy
Three Negative Acks	Active Downlink	High	Hard
Fake Position	Active Downlink	High	Medium
Fake Trajectory	Active Downlink	High	Hard
Emergency Mode Flooding	Active Downlink	Medium	Medium
Cancel Emergency Mode	Active Downlink	Low	Easy
Aero Log-on Reject	Active Uplink	High	Hard
Aero Log-off	Active Uplink	High	Hard
Cancel Contracts	Active Uplink	Medium	Hard
Cancel Emergency Mode	Active Uplink	Low	Hard

TABLE V: Summary of vulnerabilities in ADS-C.

VII. Discussion

A. Overall Impact of ADS-C's Vulnerability

Assessing the impact of active attacks on ADS-C is challenging as we do not know how ATC or pilots would react to them. There are, however, some indications on what impact an active attack on ADS-C could have. For example, Mori mentions how ATC uses ADS-C data to predict future position of aircraft and that "estimation errors result in potential separation infringement" [20]. Such an estimation error could also be caused by a spoofed position. Additionally, it is likely that preventing ADS-C communication or virtual trajectory attacks could lead to inefficient maneuvering of aircraft and confusion at air traffic control. It is also imaginable that the consequences of attacks on ADS-C include delays and cancellations of flights, similar to a situation in August 2023, where the British National Air Traffic Services received data it could not process. As a consequence, almost 2'000 flights were canceled [6]. However, the existence of backup communication makes it highly unlikely that attacks on ADS-C seriously compromise aircraft's safety. Relating to this, Sathaye et al. conclude that attackers have a higher impact when combining attacks on multiple vital aircraft systems [28].

B. Countermeasures

The obvious measure to counter both passive and active attacks on ADS-C is to encrypt and authenticate messages using a *Public Key Infrastructure* (PKI). However, researchers on secure aviation communication also agree that introducing PKI would be time-consuming and expensive [27], [33], [31].

Another class of approaches are mitigation techniques that work alongside the existing system. This can, for example, be achieved through signal strength analysis [27]. This method relies on detecting jumps in the power of the received signals. Such a surge could be an indicator that the received signal originates from an attacker. This mechanism could be applied on both the ground station and the satellite receiver. Spoofing and replaying of message could also be detected by radio transmitting fingerprinting [30]. This strategy uses identifying information in the signal such as path loss or background noise to authenticate the signal's sender.

Yet another technique to prevent attacks relies on the satellite sending signals to multiple receivers. These receivers can then simply run a sanity check or perform a *Time Difference of Arrival* (TDoA) analysis, where the reception times are used to compute the direction of the source [27], [8].

VIII. Related Work

A. Wireless Communication in Aviation

With the rise of software defined radios, a modern threat model in wireless aviation systems has emerged, which moves beyond military electronic warfare and threatens all insecure legacy protocols [34], [32].

The most studied protocol in aviation is terrestrial ADS-B. McCallie et al., for example, highlight attacks on this protocol and the inherent risks of its implementation [19]. Another study by Schäfer et al. [29] implements attack primitives for ADS-B, such as eavesdropping, message injection, message deletion and message modification. These primitives, in turn, enable more elaborate attacks such as ghost aircraft injection, virtual trajectory modification, and aircraft spoofing. Recently, attacks have been shown in real certified avionics hardware [35].

Another protocol that has been subject to security researchers' attention is the above-mentioned CPDLC – a protocol used to transmit text-based messages between pilots and air traffic management. Smailes et al. demonstrate a Man-in-the-Middle attack on CPDLC and discuss its impact [30]. Sathaye et al., as mentioned above, even illustrate how attacks have the potential to influence a pilot's decision making by jamming and spoofing CPDLC and ADS-C messages [28].

While hobbyists have engaged with ADS-C [23], [22], the security research community has not done so even in the most recent surveys on aviation security [12]. The only exception is [28], in which Sathaye et al. discuss possible attacks on different layers and applications of aviation datalinks, briefly touching on ADS-C.

B. Satellite Communication

Pavur et al. [26] demonstrate eavesdropping on satellite communication with equipment as cheap as $400. Salkield et al. [27] highlight that satellite downlink communication can also be overshadowed with cheap equipment. In [33], the authors analyze the requirements to inject messages in the uplink direction. They do this in the context of SADS-B, a variation of ADS-B which makes use of satellite communication.

IX. Conclusion

In this paper, we performed an in-depth analysis of satellite-based air traffic control using the ADS-C protocol. We built and tested complete ADS-C transmitter pipelines for both the uplink and downlink direction. These transmitters have the capability to generate, encode, modulate, and transmit arbitrary ADS-C messages. We subsequently analyzed the possible impact of such attacks and found that they could be significant under the right circumstances.

Considering the importance of ADS-C for air traffic, it is surprising that this paper is the first to discuss and analyze the protocol's privacy and security. It is clear that there is still much work to be done to secure air traffic communication. We believe that in particular more realistic and practical work is needed that goes beyond theory and simulations. Only with increased attention can the responsible authorities be persuaded to secure aviation communication protocols.

References

[1] "RF CHANNEL CHARACTERISTICS." [Online]. Available: https://www.icao.int/safety/acp/Inactive%20working%20groups%20library/AMCP%203/item-3a03.pdf

[2] Airlines Electronic Engineering Committee, *ARINC CHARACTERISTIC 745-2: AUTOMATIC DEPENDENT SURVEILLANCE (ADS)*, 2nd ed., 1993.

[3] ——, *ARINC CHARACTERISTIC 724-9: AIRCRAFT COMMUNICATIONS ADDRESSING AND REPORTING SYSTEM (ACARS)*, 9th ed., 1998.

[4] ——, *Arinc Specification 622-4: ATS DATA LINK APPLICATIONS OVER ACARS AIR-GROUND NETWORK*, 4th ed., 2001.

[5] ——, *ARINC SPECIFICATION 618-8: AIR/GROUND CHARACTER-ORIENTED PROTOCOL SPECIFICATION*, 8th ed., 2016.

[6] S. H. By Katy Austin, "We can avoid flight chaos in future, says air traffic boss," *BBC*, 2023. [Online]. Available: https://www.bbc.com/news/uk-66654338

[7] A. Costin and A. Francillon, "Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," in *BLACKHAT 2012, July 21-26, 2012, Las Vegas, NV, USA*, EURECOM, Ed., Las Vegas, 2012.

[8] J. Dolan, M. Garcia, and G. Sirigu, "Aireon space based aircraft position validation and multilateration solution," in *Proceedings of the 2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC)*. IEEE, 2023.

[9] eroenbeijer, "sdr_25E.ini." [Online]. Available: https://github.com/jeroenbeijer/SDRReceiver/blob/master/sample_ini/sdr_25E.ini

[10] Eurocontrol, *EUROCONTROL Aviation Outlook 2050: Main Report*. Eurocontrol, 2022.

[11] Flightradar24, "We are aware of some erroneous signals [...]." [Online]. Available: https://twitter.com/flightradar24/status/1712763977061552527

[12] E. Habler, R. Bitton, and A. Shabtai, "Assessing Aircraft Security: A Comprehensive Survey and Methodology for Evaluation," *ACM Comput. Surv.*, jul 2023, just Accepted.

[13] International Civil Aviation Organization, *ICAO Doc 9925: Manual on the Aeronautical Mobile Satellite (Route) Service*, draft ed., 2007. [Online]. Available: http://www.icao.int/safety/acp/inactive%20working%20groups%20library/acp-wg-m-iridium-8/ird-swg08-wp07%20-%20old_amss_material_ch.4_plus_attachment.doc

[14] ——, *ICAO Doc 9925: Manual on the Aeronautical Mobile Satellite (Route) Service*, 1st ed., 2010.

[15] ——, *Air Traffic Services: Annex 11 to the Convention on International Civil Aviation*, 15th ed., 2018.

[16] jeroenbeijer, "SDRReceiver," 2023. [Online]. Available: https://github.com/jeroenbeijer/SDRReceiver

[17] T. Lemiech, "libacars." [Online]. Available: https://github.com/szpajder/libacars

[18] m-cramer Satellitenservices, "IMPORTANT ANNOUNCEMENT: Repointing BGAN Land Terminals #1." [Online]. Available: https://m-cramer-satellitenservices.de/support/network-alerts/alert-20230714-130444/

[19] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 2011.

[20] R. Mori, "Analysis of Speed Prediction Error on Oceanic Flights," *The Journal of Navigation*, vol. 72, no. 6, p. 1469–1480, 2019.

[21] nooelec, "1550MHz Active Inmarsat Antenna Bundle." [Online]. Available: https://www.nooelec.com/store/sdr/sdr-addons/inmarsat-antenna-bundle.html

[22] J. Olds, "JAERO," 2023. [Online]. Available: https://github.com/jontio/JAERO

[23] B. Orchard, "Decoding ADSC, ADSB, ACARS, VDL2, Iridium, HF-DL and other aircraft type messages." [Online]. Available: https://thebaldgeek.github.io/

[24] ——, "How to build an L-Band ground station." [Online]. Available: https://thebaldgeek.github.io/L-Band.html

[25] S. Pasupathy, "Minimum shift keying: A spectrally efficient modulation," *IEEE Communications Magazine*, vol. 17, no. 4, pp. 14–22, 1979.

[26] 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)*, 2020, pp. 1384–1400.

[27] E. Salkield, M. Szakály, J. Smailes, S. Köhler, S. Birnbach, M. Strohmeier, and I. Martinovic, "Satellite Spoofing from A to Z: On the Requirements of Satellite Downlink Overshadowing Attacks," ser. WiSec '23. New York, NY, USA: Association for Computing Machinery, 2023, p. 341–352.

[28] H. Sathaye, G. Noubir, and A. Ranganathan, "On the Implications of Spoofing and Jamming Aviation Datalink Applications," ser. ACSAC '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 548–560.

[29] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental Analysis of Attacks on Next Generation Air Traffic Communication," in *Applied Cryptography and Network Security*, M. Jacobson, M. Locasto, P. Mohassel, and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 253–271.

[30] J. Smailes, S. Köhler, S. Birnbach, M. Strohmeier, and I. Martinovic, "Watch this space: Securing satellite communication through resilient transmitter fingerprinting," in *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, 2023, pp. 608–621.

[31] J. Smailes, D. Moser, M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic, "You Talkin' to Me? Exploring Practical Attacks on Controller Pilot Data Link Communications," in *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*, ser. CPSS '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 53–64.

[32] M. Strohmeier, I. Martinovic, and V. Lenders, "Securing the air–ground link in aviation," *The Security of Critical Infrastructures: Risk, Resilience and Defense*, pp. 131–154, 2020.

[33] M. Strohmeier, D. Moser, M. Schäfer, V. Lenders, and I. Martinovic, "On the Applicability of Satellite-Based Air Traffic Control Communication for Security," *IEEE Communications Magazine*, vol. 57, no. 9, pp. 79–85, 2019.

[34] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On Perception and Reality in Wireless Air Traffic Communication Security," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 6, pp. 1338–1357, 2017.

[35] M. Strohmeier, G. Tresoldi, L. Granger, and V. Lenders, "Building an avionics laboratory for cybersecurity testing," in *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test*, 2022, pp. 10–18.

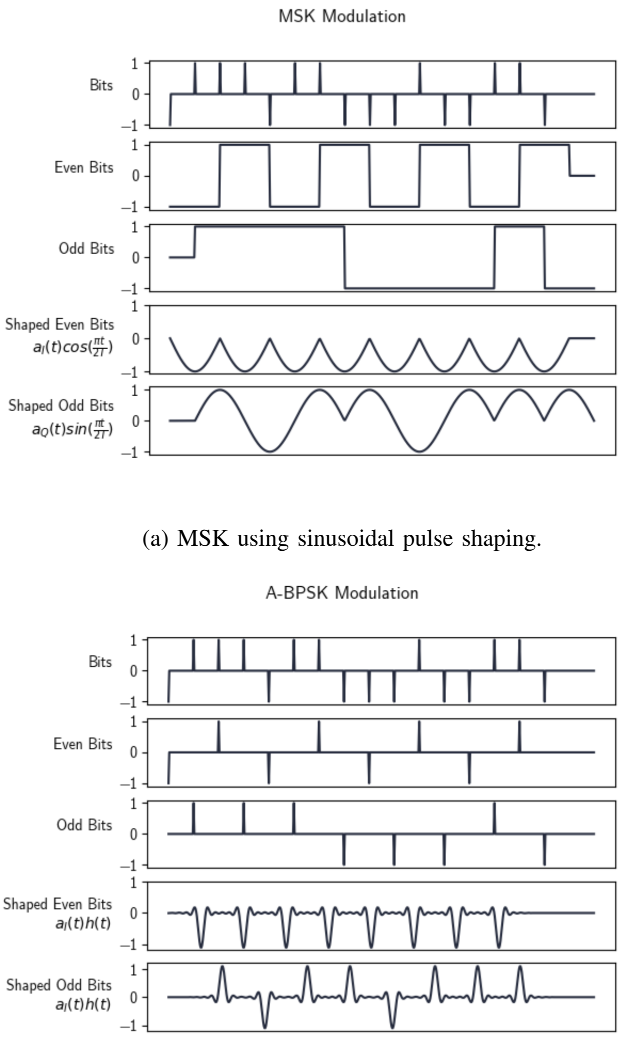
[36] United States Government Accountability Office, "GAO-19-532: AIR TRAFFIC CONTROL FAA's Analysis of Costs and Benefits Drove Its Plans to Improve Surveillance in U.S. Oceanic Airspace." [Online]. Available: https://www.gao.gov/assets/gao-19-532.pdf

[37] Universal Avionics, *Understanding Data Comm Systems with Domestic and Oceanic FANS 1/A+ and ATN B1 Services*, 2020.

[38] M. Xapelli, T. Lüscher, G. Tresoldi, M. Strohmeier, and V. Lenders, "A first look at leveraging the automatic dependent surveillance-contract protocol for open aviation research," in *Proceedings of the 11th OpenSky Symposium*, 2023.

Appendix A: A-BPSK

A-BPSK is a "modulation with shaped filters especially adapted to perform in an RF environment subject to fading" [1]. As the name implies, A-BPSK is a modulation scheme that encodes data by altering the phase of a signal with constant frequency. Specifically, A-BPSK maps a binary 0 to a phase shift of -90 degrees and a binary 1 to a phase shift of +90 degrees. Consequently, A-BPSK is similar to *Minimum Shift*



(a) MSK using sinusoidal pulse shaping.

(b) A-BPSK, using root raised cosine pulse shaping. $h(t)$ is a 40% root raised cosine filter.

Fig. 11: The first row illustrates the initial bits that are modulated. The second and third rows depict the even and odd bits of the initial sequence, respectively. The fourth and fifth row illustrate the bit sequences shaped by sinusoids (left) and by a 40% root raised cosine (right).

Keying (MSK). While MSK uses sinusoids for pulse shaping, A-BPSK uses a 40% root raised cosine filter.

MSK is described by Equation 1:

$$s(t) = a_I(t)cos(\frac{\pi t}{2T})cos2\pi f_c t + a_Q(t)sin(\frac{\pi t}{2T})sin2\pi f_c t \quad (1)$$

where $a_I(t)$ represents the even bits and $a_Q(t)$ represents the odd bits to be modulated [25]. When using IQ-modulation, the in phase and quadrature components are defined as follows:

$$I(t) = a_I(t)cos(\frac{\pi t}{2T}) \quad (2a)$$

$$R(t) = a_Q(t)sin(\frac{\pi t}{2T}) \quad (2b)$$

Replacing the sinusoidal pulse shaping with a root raised cosine shaping in Equation 2 results in the subsequent formulae:

$$I(t) = a_I(t)h(t) \quad (3a)$$

$$R(t) = a_Q(t)h(t) \quad (3b)$$

where $h(t)$ is a 40% root raised cosine filter. Thus, Equation 3 represents the quadrature and in-phase components of A-BPSK. A-BPSK improves the distortion caused by nonlinear amplification and hence increases performance in the aviation context.