On the Implications of Spoofing and Jamming Aviation Datalink Applications

Harshad Sathaye, Guevara Noubir, Aanjhan Ranganathan
Khoury College of Computer Sciences
Northeastern University, Boston, USA

ABSTRACT

Aviation datalink applications such as controller-pilot datalink communications (CPDLC) and automatic dependent surveillance-contract (ADS-C) were designed to supplement existing communication systems to accommodate increasing air traffic. These applications are typically used to provide departure clearance, en-route services such as altitude and flight plan changes, air traffic surveillance and reporting, and radio frequency assignments. Unlike most attacks proposed so far where the attacker influences decision-making through manipulated instruments, attacks on aviation datalink provide adversaries with a new attack vector to influence the flight crew's decision-making through direct instructions. In this work, we perform a security analysis of these applications and outline the requirements for executing a successful attack. Specifically, we propose a coordinated multi-aircraft attack and show how an adversary capable of spoofing datalink messages and reactive jamming can influence the flight crew's decision-making. Through geospatial analysis of historical flight data, we identify 48 vulnerable regions where an attacker has a 90% chance of encountering favorable conditions for coordinated multi-aircraft attacks. Next, we implement a reactive jammer that ensures stealthy attack execution by targeting messages from a specific aircraft with a reaction time of 1.48 ms and 98.85% jamming success. Even though by themselves these attacks have a lower probability of endangering the safety of the aircraft, the threat is magnified when combined with attacks on other avionics. Finally, we discuss the possibility of executing integrated attacks on aircraft system as a whole emphasizing the importance of securing individual components in the aviation ecosystem.

ACM Reference Format:
Harshad Sathaye, Guevara Noubir, Aanjhan Ranganathan. 2022. On the Implications of Spoofing and Jamming Aviation Datalink Applications. In *Annual Computer Security Applications Conference (ACSAC '22), December 5–9, 2022, Austin, TX, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3564625.3564651

1 INTRODUCTION

Air traffic controllers (ATC) ensure the safe and efficient flow of air traffic on the ground and during flight. ATCs frequently provide instructions and receive reports from the aircraft present in their airspace. In 2021, ATCs around the world handled more than 19 million flights [25] [1]. Traditionally, all instructions and reporting took place over voice communication channels. However, with the increasing air traffic density, voice communication channels are becoming a bottleneck. For example, according to Boeing [2], it can take up to 20 to 45 mins to make a position report through the voice channel, i.e., waiting for one's turn to interact with the ATC in congested airspace directly impacting the flow of air traffic. Noisy radio frequency channels further force the aircraft to be operated at sub-optimal altitude and speeds. In fact, such drawbacks of voice communication have led to several accidents [50].

As a result, there are several ongoing efforts (e.g., NextGen in the US [21]) to modernize air transportation systems across the world using new technologies with the goal of increasing the safety, efficiency, and resiliency of the global airspace. One of the technologies is the controller pilot data link communication (CPDLC) which enables the exchange of messages between the pilot and the ATC. The ATCs can issue flight plan updates, altitude and speed changes, radio frequency channel assignments, etc. to the pilots using CPDLC. CPDLC also allows pilots to respond to messages, request new clearances, or simply report statuses back to the ATC. Even though CPDLC and ADS-C are complementary systems to voice communications and are used for strategic and non-emergency communications, their importance is increasing and in some scenarios, it is replacing voice communications. Moreover, today, certain airspaces require the aircraft to be equipped with aviation datalink capability [1, 11]. Over the years, the adoption of this datalink has enabled the controllers to reduce aircraft separation by being able to allow more aircraft to share the airspace. To date, aviation datalink applications have saved 2.28 million minutes of radio time [41].

As compared to popular aviation systems like instrument landing system (ILS) [53], automatic dependent surveillance-broadcast (ADS-B) [17, 54, 63], global positioning system (GPS) [65, 67], and collision avoidance systems [61], only a few works have explored the security aspects of aviation datalink. Most notably, [59, 70] lay down strategies to exploit the lack of authentication, however, they do not elaborate on the feasibility and impact of the attack. Furthermore, the attacks proposed in the above works can be trivially detected, and the requirements of introducing stealthy CPDLC manipulation were not considered. Also, there exists no proof-of-concept implementation and evaluation of the attacks. To this end, in this work, we make the following contributions.

- We systematically analyze the security guarantees of often overlooked aviation datalink applications and present a spoof and jam attack strategy to inject malicious messages stealthily. We demonstrate strategies that manipulate commonly used message elements like transponder codes, instrument calibration settings, departure clearances, and voice contact frequencies to influence the crew's decision-making.

[1] pre-covid traffic in 2019 was 38.9 million flights

[2] https://www.boeing.com/commercial/aeromagazine/aero_02/textonly/fo02txt.html

ACSAC '22, December 5–9, 2022, Austin, TX, USA

ACM ISBN 978-1-4503-9759-9/22/12…$15.00
https://doi.org/10.1145/3564625.3564651

- Next, we propose a coordinated attack that targets multiple aircraft with intersecting trajectories. We craft CPDLC messages with appropriate altitude and optionally waypoint change instructions to force multiple aircraft to cross each other at the same altitude.
- To facilitate these attacks we implement and evaluate an aircraft communications, addressing, and reporting system (ACARS) message spoofer and a reactive jammer. The reactive jammer can achieve a 1.48 ms reaction time and 98.85% jamming success. Thus allowing the attacker to avoid detection. To the best of our knowledge, this is the first work presenting a reactive jammer for aviation datalink applications using the ACARS network.
- We analyze air traffic data from 2021 and identify 48 regions with a 90% chance of spotting at least one such intersection in a day. A condition that is favorable for coordinated attacks.

Aviation datalink applications complement existing communication and surveillance systems. An advantage of datalink attacks is that they can directly provide instructions to the flight crew and are most effective when combined with attacks on other avionics.

2 BACKGROUND

Aviation datalink encompasses technologies that provide a direct controller-pilot datalink and enable safe, efficient, and accurate operations. Aviation datalink applications are based on two major implementations: i) Traditional ACARS network or ii) modern aeronautical telecommunications network developed by the international civil aviation organization (ICAO) and adopted by Eurocontrol as the primary datalink infrastructure [2]. ACARS is a communication system that links aircraft with ground stations. Primarily, ACARS uses very high frequency (VHF) Datalink Mode A/0 physical layer technology to deliver messages. VHF radios strictly require line-of-sight operations. This limits VHF coverage only up to 200 miles. To overcome the coverage limitation of VHF radios, an HF datalink, and SATCOM links were added to the ACARS network.

Initially, ACARS was used to exchange data like weather information, aircraft maintenance reports, gate assignments, and passenger information with the airline's operational control. Support for datalink applications that provide air traffic control services was added under the future air navigation systems (FANS) structure conceptualized by ICAO; Boeing developed FANS 1, after which Airbus developed FANS A. These systems together are referred to as FANS 1/A [24]. FANS 1/A applications are designed to utilize existing ACARS networks. They support VHF Datalink Mode A/0 transmissions used by traditional ACARS applications for domestic and oceanic operations and newer VHF Datalink Mode 2.

Aeronautical telecommunications network (ATN) is a network of interconnected systems that efficiently facilitate the exchange of information between concerned entities through ground-ground and air-ground sub-networks. Unlike FANS 1/A, ATN baseline 1 (B1) provides a CPDLC implementation that supports only the VHF Datalink Mode 2 for message transmission. However, in the future, there are plans to adopt an IP-based network to further improve message delivery and integrity. As part of their Single European Sky initiative, Eurocontrol has adopted ATN B1 as the primary datalink implementation. ATN B1 operations are restricted to Europe. On the other hand, FANS 1/A is the primary datalink implementation adopted in America and most other places. Figure 1 provides a graphical representation of the aviation datalink ecosystem.

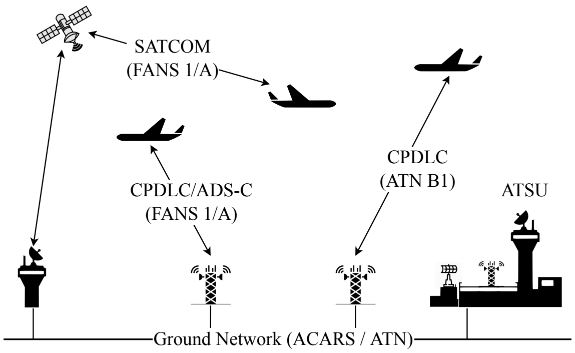


Figure 1: A graphic representation of aviation datalink ecosystem and its various components. The ground station radios use either the ACARS network or ATN. However, there are systems that support both networks.

Both implementations are supported by two major datalink applications, CPDLC and ADS-C. Even though these networks are not interoperable, avionics are designed to provide a seamless transition. These applications provide a direct communications link between a pilot and ATC and enable the transmission of ATC commands and surveillance messages more efficiently. CPDLC is a data link that enables air traffic controllers and pilots to exchange messages traditionally sent over voice channels such as en-route services, flight plan amendments, departure clearances, and instructions to execute specific instructions maneuvers like changing the altitude. Not to be confused with ADS-B, ADS-C is a system where an aircraft initiates a contract with one or more Air Traffic Services Unit (ATSU) and periodically sends out various reports that contain the aircraft's position, speed, altitude, route predictions, airframe data, and meteorological data to one or more ATSU. It is important to note that ATN B1 does not support ADS-C application [26]. This work focuses on FANS 1/A applications and targets specific CPDLC, and ADS-C messages exchanged using the ACARS network. ATN B1 and FANS 1/A support different message sets. However, these attacks can be used against ATN B1 applications with some changes.

3 SECURITY ANALYSIS OF AVIATION DATALINK APPLICATIONS

3.1 Attacker Goal and Assumptions

We consider an attacker capable of intercepting, injecting, and reactively jamming ACARS messages. The attacker has certain physical layer restrictions like transmit power and radio coverage. VHF signal reception requires strict line-of-sight communication; this restricts the coverage of an attacker. For example, even though an attacker with a radio set located on the ground can communicate with a high-flying plane that is 400 km away, being closer to the ground, it can only communicate with an air traffic controller 15 to 30 km away. However, the attacker can use high-flying drones to increase radio coverage. Furthermore, to better plan the attack and determine an optimal location, we consider that the attacker has

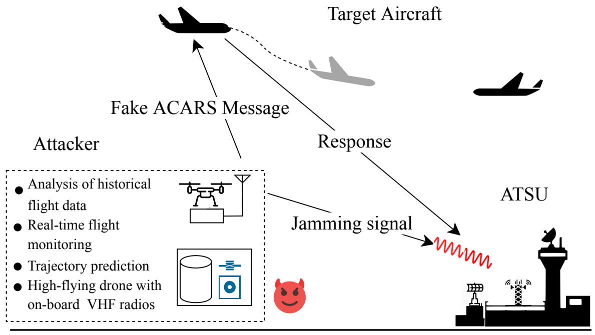

Target Aircraft
Fake ACARS Message
Attacker
Response
ATSU
Jamming signal
● Analysis of historical flight data
● Real-time flight monitoring
● Trajectory prediction
● High-flying drone with on-board VHF radios

Figure 2: A graphical representation of the proposed attack. Real-time flight monitoring and trajectory prediction allow the attacker to plan the transmission of fake ACARS messages. The reactive jammer transmits a jamming signal to prevent the ATSU from receiving the response.

access to historical and live air traffic data through services like Opensky network [55], FlightAware, or live over-the-air ADS-B transmissions. The attacker is equipped with a software-defined radio (SDR) capable of transmitting and receiving VHF voice signals and ACARS signals that use airband frequencies from 118 MHz to 137 MHz. For example, commercial off-the-shelf SDRs like USRP B210, HackRF, PlutoSDR, and LimeSDR. Minimum cost of the attack will be roughly $864, PlutoSDR [6] ($199), VHF Antenna [3] ($85 x2), and VHF amplifier [7] ($495). Optionally an attacker can use more sophisticated devices which will increase the cost.

In existing attacks on various avionics, the attacker aims to influence the flight crew's decision-making by attacking various navigation and surveillance aids. The proposed datalink attacks provide a more direct way of manipulation through targeted instructions in the form of CPDLC messages which can jeopardize the aircraft's safety and security. For example, forcing the flight crew to change the flight path that brings their aircraft close to a passing aircraft or providing them with incorrect instrument calibration values. An attack is considered successful if the flight crew accepts the CPDLC messages and executes the malicious instructions. Figure 2 provides a graphical representation of a generic attack scenario and various components required for a successful attack.

3.2 Attack Prerequisites

To spoof CPDLC messages, the attacker needs to know the identity of the aircraft's current data authority (CDA). It is the ATSU that is currently authorized to send CPDLC commands to the aircraft. An aircraft will accept CPDLC commands only if issued by an ATSU, designated as the CDA. Commands from any other ATSUs are rejected by the onboard software, and the aircraft will automatically send a *DM63 - NOT CURRENT DATA AUTHORITY* message [27]. To execute specific multi-aircraft attacks, the attacker will also require route predictions and position estimates to calculate the closest point of approach necessary for determining the time of the attack.

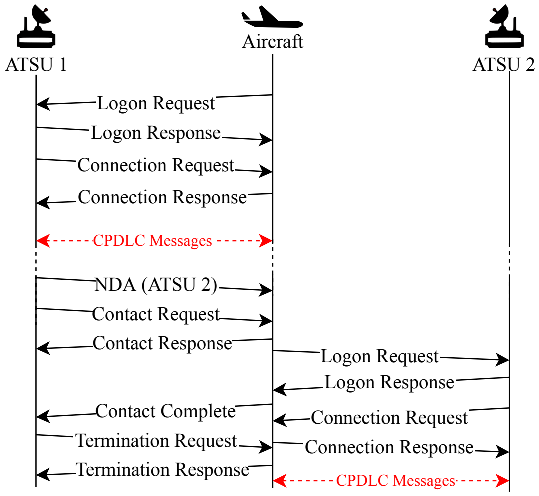


Figure 3: A sequence of CPDLC connection management messages exchanged between the aircraft and multiple ATSUs. The aircraft follows this sequence of messages until it reaches its destination.

CDA Identity: An aircraft supports two connections at any time, one active and one inactive connection. It establishes an active connection after completing the logon and the connection procedure. Figure 3 shows the sequence of CPDLC messages exchanged during these procedures. Before departure, the flight crew initiates the logon procedure by entering the ATSU's ICAO identifier. After receiving the logon request, the ATSU correlates the flight plan and responds with a logon confirmation, followed by a connection request. The ATSU automatically rejects the logon request if the flight plan correlation fails [28]. If the aircraft doesn't have an active connection, the aircraft responds with a connection confirmation and establishes an active connection. The ATSU with which the aircraft establishes an active connection is called the CDA. If the aircraft already has an active connection and if the ATSU is the next data authority (NDA), i.e., the next ATSU according to the filed flight plan or as decided by the CDA, the aircraft establishes an inactive connection. However, if the ATSU is neither the CDA nor the NDA, FANS 1/A equipped aircraft will send a connection reject message followed by the identity of its CDA. ATN B1 aircraft, on the other hand, will only send a *DM107 NOT AUTHORIZED NEXT DATA AUTHORITY* message [29]. This way, an attacker can find out the identity of the CDA that it needs to impersonate to initiate CPDLC message exchanges.

Route predictions: An ATSU may initiate one or more ADS-C contracts with the aircraft by sending an ADS-C contract request. These contracts include a report group that contains route predictions and such a report is optional. To receive route predictions, the attacker can initiate a periodic contract or request a one-time contract that contains the required route predictions and position estimates. It is important to note that all ADS-C functions, including signing up for contracts and reporting do not require flight crew intervention [30]. An aircraft may simultaneously have contracts with multiple ATSUs. The ATSUs are unaware of any other contract held by the

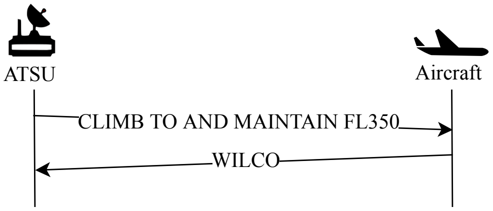


Figure 4: A sequence of CPDLC dialogue between ATSU and the aircraft. The ATSU instructs the aircraft to climb and maintain an altitude of 35000 ft. The flight crew confirms by sending *WILCO,* which means that the flight crew has accepted the instruction.

aircraft. This allows the attacker to stealthily initiate contracts by impersonating an ATSU.

3.3 Spoofing CPDLC Messages

Depending on the intended effect of the attack, there are two ways to execute an attack: i) The attacker impersonates an ATSU and sends a malicious instruction to the aircraft, and jams the response to prevent the legitimate ATSU from receiving the message. This is useful when the injected messages contain commands that require the flight crew to execute maneuvers, e.g., when the attacker wants to modify the aircraft's trajectory. ii) The attacker first intercepts and jams a request from the aircraft preventing the legitimate ATSU from receiving the request. Next, the attacker sends a malicious response by impersonating the legitimate ATSU. Such a strategy is useful when the attacker wants to manipulate the ATSU's response. This is beneficial when the attacker wants to spoof route clearance or digital automatic terminal information service (D-ATIS) data.

Once the attacker impersonates the CDA, the aircraft's onboard computer will accept any CPDLC command that it receives from the attacker. Through CPDLC messages, controllers can provide mission-critical instructions to the flight crew, including commands to modify the flight path and assign instrument calibration values. Refer to Figure 4 for an example of a CPDLC dialogue between the controller and the flight crew. A typical flight goes through three distinct phases, i) the departure phase, ii) the cruise phase, and iii) the arrival phase. ACARS, in some capacity, is used in every flight phase for exchanging crucial information that the flight crew requires for maintaining safety. Figure 5 gives an overview of the data that the attacker can manipulate in each flight stage.

Based on the source and the destination, CPDLC messages are categorized as: i) downlink (DMxx) and ii) uplink (UMxx). In Section 4.1 we provide more details on the structure of uplink and downlink CPDLC messages. Downlink messages are sent from the aircraft down to the ATSU, and uplink messages are sent from the ATSU up to the aircraft. Each message contains a four-character message-id that enables the receiver to sequence and rearrange the messages. These messages follow a syntax similar to regular voice communications and are often used instead of analog voice channels, e.g., (go) *DIRECT TO [position].* CPDLC provides 81 downlink and 183 uplink message types [31]. These messages are integrated into the flight management system (FMS), and uplink messages that amend flight plans are automatically loaded into the FMS upon flight crew approval [32]. This allows an attacker to send specific messages that can automatically amend the existing flight plan after flight crew approval. ACARS messages contain a 16-bit cyclic redundancy checksum (CRC) that allows error detection through a message integrity check. Additionally, CPDLC messages contain an application-level CRC to verify the integrity of the transmitted CPDLC commands. If the CRC check fails at the ACARS level for a transmission initiated by the aircraft, the ground station will ignore the message. However, if the CRC check fails at the CPDLC level, the ground station will send a CPDLC error response [18]. CRC values are sensitive to bit flips, and an attacker can prevent the receiver from receiving a packet by corrupting a small portion of the message. This provides an opportunity for the attacker to jam the transmitted messages.

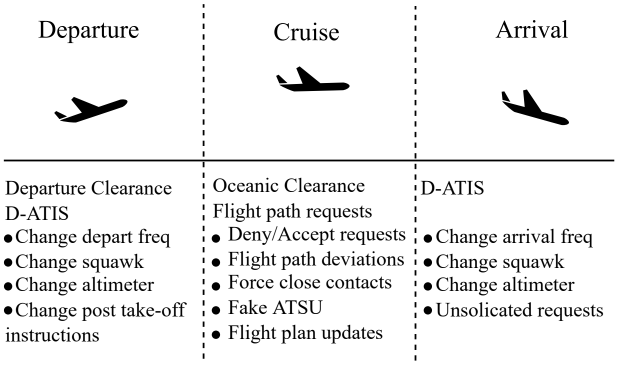


Figure 5: Using a combination of ACARS message injection and jamming, an attacker can modify instructions and procedures specific to a flight stage.

3.4 Jamming CPDLC and ADS-C Messages

Through an analysis of CPDLC and ADS-C messages, we learn that, despite the lack of security controls, as a result of strict message structure, limited request/response options, and mandatory response from the flight crew, simply spoofing ACARS messages to influence the flight crew's decision-making is not enough as even minor suspicion will cause them to clarify instructions over a voice channel. Moreover, to avoid detection through unexpected messages, along with message spoofing, the attacker should also be able to jam messages. Continuous jamming will cause a denial of service attack as the ATSU will not receive any messages thus raising alarms.To prevent such detection, the attacker needs a reactive jammer capable of jamming only specific messages from particular flights to avoid such a situation and ensure a successful attack.

Response Jamming: CPDLC message exchange follows a specific pattern and structure. The flight crew has to select from hard-coded request/response options determined by the communication management and jam the WILCO response request. A set of predetermined responses ensure that the message structure remains intact and prevents the flight crew from transmitting inappropriate responses. The following options are considered as appropriate responses, i) *DM 0* WILCO - Will Comply, ii) *DM 1* UNABLE, iii) *DM 2* STANDBY, iv) *DM 3* ROGER, v) *DM 4* AFFIRM, and vi) *DM 5*

NEGATIVE [33]. The spoofed instructions should be convincing, as even a minor suspicion can cause the flight crew to decline the commands and contact the ATSU over a voice channel. According to the operational guidelines, when the ATSU receives unexpected messages including inappropriate responses or no response at all, the ATSU is required to follow up and investigate over a voice channel [34]. All messages are broadcast, and the ATSU will receive and respond to all the messages addressed to it. Hence the attacker should actively monitor ACARS communications and jam appropriate requests and responses to avoid detection.

ADS-C Report Jamming: There are three types of contracts, i) periodic contract, which requires the aircraft to periodically send the specified information, ii) demand contract, where the ATSU requests a one-time report. And iii) event contract, where the aircraft automatically reports if the specified event occurs. The ATSU specifies the reporting interval from 64 to 4096 seconds for periodic contracts. These periodic reports contain aircraft position reports, waypoint predictions, airframe data, and meteorological information [35]. The attacker can leverage these predictions to coordinate attacks between multiple aircraft as described in Section 3.6.

When an aircraft enters into an event contract with an ATSU, the FMS automatically sends an event report to the ATSU when a particular event occurs. Based on airspace requirements, the ATSU must establish event contracts for the following events [36, 37]. These are i) the addition of a new waypoint, ii) the aircraft crosses the provided horizontal and vertical bounds, and iii) when the aircraft exceeds the vertical rate limit.

Apart from the above-mentioned events, optionally, an ATSU may require additional periodic reports that reflect the aircraft's movements and waypoint predictions. These reports help the controllers avoid potential mid-air close contacts and maintain established separation minima in busy airspace with tight separation limits. It is essential for an attacker to know about active contracts agreed by the aircraft as these reports may indicate any maneuvers executed by the flight crew based on spoofed CPDLC messages. This may alert the air traffic controllers and can lead to attack detection. To prevent this, the attacker needs to jam ADS-C reports that may indicate the execution of unauthorized maneuvers.

3.5 Single Aircraft Attacks

Clearance Manipulation: At the beginning of the departure phase, the flight crew requests information that helps them prepare the FMS for departure. The flight crew specifically requests the pre-departure clearance (PDC) and D-ATIS. Refer to the appendix for an example of the PDC message.[3]. PDC is a set of post-take-off instructions specific to a particular flight. Usually, it includes the climb via waypoint, the filed flight plan, post-take-off altitude, and frequency for post-take-off voice contact. It also contains a 4-digit squawk code used to identify the aircraft on the secondary surveillance RADAR screens. The flight crew is responsible for manually configuring their transponder to use the correct squawk code. D-ATIS contains information that is common to all aircraft. It includes the most recent weather report and other warnings regarding potential obstructions around the airport. The attacker can jam PDC message requests and replace legitimate responses with malicious messages containing incorrect squawk code. Changing the squawk code can lead to confusion and disruption of situational awareness as ATCs will provide the right instructions to the wrong flight. In [64], a survey performed by the authors indicates that 54.82% of the participating controllers feel that incorrect labels on the RADAR screen can cause a major loss of situational awareness.

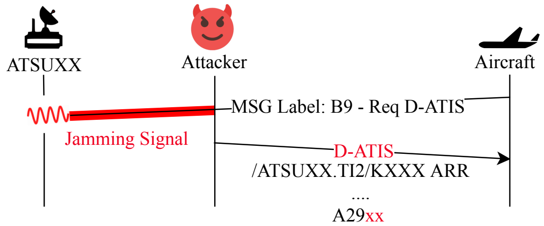


Figure 6: A sequence of message exchanges in an altimeter change attack forces the approaching aircraft to set the altimeter incorrectly. The approaching aircraft sends a request to receive ATIS information with a *B9* label. The attacker intercepts the message and jams it. The attacker then sends a fake ATIS message with a modified altimeter value.

Altimeter Setting Manipulation: According to a Boeing report [14], the arrival phase is the most accident-prone phase. The arrival phase starts when the flight crew receives instructions from the ATC to descend once it gets closer to the airport. The ATC assigns a runway, and the flight crew follows the stated approach procedures. During this phase, the flight crew puts in a request for arrival D-ATIS which has information regarding the current approach and runways. Most importantly, it has the correct altimeter setting for the destination airport. To get the correct altitude [4], it is important to re-calibrate the altimeter before landing [20] and is mandatory In this attack, the attacker intercepts and jams the flight crew's request to receive D-ATIS. Followed by the injection of a malicious D-ATIS message with a modified four-digit altimeter setting where a single-digit error results in a discrepancy of 10 ft in altitude. Refer to Figure 6 for the sequence of message exchanges for manipulating the altimeter setting. Flying with an incorrect altimeter can lead to a *controlled flight into terrain* event, which can be dangerous [10].

VHF Voice Man-in-The-Middle. Pilots and controllers will often revert to VHF voice for communicating time-sensitive and safety-critical information. Controllers will also revert to voice when they receive inappropriate or unexpected messages. Often, pilots are required to verbally check in with the controllers, especially when transferring from one controller region to another controller region. In case the controllers require the pilots to monitor a certain frequency, the controller will send a *UM120* [38] CPDLC message that instructs the pilots to tune and monitor the specified frequency. An attacker can leverage this message type to execute a man-in-the-middle attack and establish a VHF voice relay between a controller and the flight crew. Figure 7 shows the message exchange and the attack concept. The attacker sets up a rogue VHF voice transceiver station on an unused voice channel. If the controller decides to reach out to the flight crew, unaware of the rogue channel, the controllers

[3] Contents redacted to preserve anonymity

[4] Altitude relative to the approaching airport

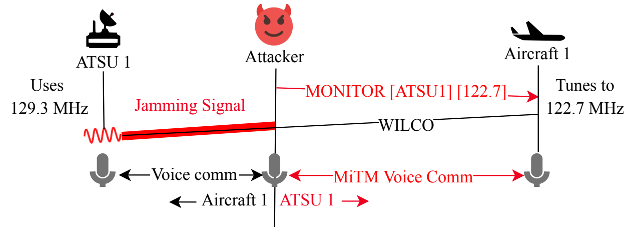


Figure 7: A sequence of message exchanges in a VHF voice man-in-the-middle attack. The attacker sets up a VHF voice station and instructs the aircraft to select the attacker's frequency instead of ATSU's. Next, the attacker relays manipulated voice communications between ATSU and the aircraft.

will use their regular channel. The attacker then responds to the controller as the victim aircraft's flight crew. This attack requires the attacker to set up a VHF voice station. The attacker also needs to be fluent in aviation phraseology and grammar.

3.6 Coordinated Multi-Aircraft Attacks

In this category of attacks, the attacker targets multiple aircraft and executes a coordinated flight path manipulation. As a result, the target aircraft come close in time and space. Flight routes are planned such that flights maintain lateral and vertical separation. However, flight paths frequently intersect. In this case, the flights cross each other while maintaining strict vertical separation. Through our analysis of flight data from 2021, we found 592,224 flight crossings, with the lateral separation between the aircraft being <100m. An opportunistic attacker can target these crossings and launch coordinated attacks instructing the flights to change their altitude to violate the vertical separation mandate. Alternatively, if the flight paths do not intersect, the attacker can add custom waypoints such that the flight paths cross at a point selected by the attacker.

The attacker prepares for the attack by finding a region that frequently sees intersections and positions itself to minimize jamming costs as described in Section 5. To send instructions to the flight crew through CPDLC messages, the attacker needs to impersonate the respective aircraft's current data authority. Depending on the location, each aircraft may be connected to a different ATSU. An attacker can determine the ATSU by monitoring CPDLC message exchanges or, as explained in Section 3.2. Once the attacker knows the CDA of both flights, the attacker can proceed with CPDLC message transmission and jamming.

The attacker's goal in this attack is to force multiple aircraft to cross at the same altitude while in close proximity to each other. This requires the attacker to estimate the closest approach point or the time and place the flights will cross. The attacker can estimate the closest approach point through trajectory prediction, which is challenging. Neither speed nor direction is constant. Even minor changes to either can lead to significant errors over time. The attacker can initiate an ADS-C contract to circumvent this problem wherein the aircraft periodically sends out route predictions. It is important to note that initiation of ADS-C contracts *does not* require flight crew approval. In [22] the authors examine the accuracy of these predictions. ATCs often rely on these predictions to maintain aircraft separation as these predictions serve as an early warning system for potential close contacts.

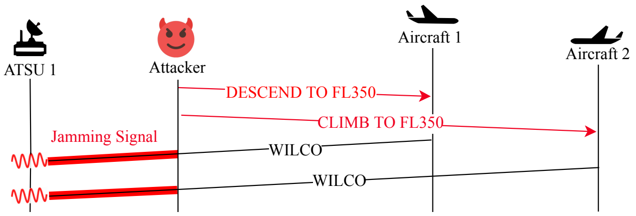


Figure 8: A sequence of message exchanges in an altitude change attack forces two crossing aircraft to change altitude and fly at the same flight level. The attacker uses the reactive jamming technique to detect and jam the WILCO response to prevent the ATSU from receiving it.

After establishing the closest point of approach, depending on each aircraft's current altitude, the attacker sends *UM20 CLIMB TO AND MAINTAIN [altitude]* and *UM23 DESCEND TO AND MAINTAIN[altitude]* messages. These messages instruct the flight crew to reach the desired altitude. A report presented in 2019 [40] reports that Anchorage center, one of the 22 air route traffic control centers in the US, handled approximately 175 altitude change requests using datalink applications per day. If the flight crew accepts the requests, they send a *WILCO* message to the ATC and perform the requested maneuver. However, in some cases, the flight crew may decide to decline the request or negotiate and suggest an alternative. As mentioned earlier, the attacker must jam the flight crew's response to avoid detection. Refer to Figure 8 for a sequence of messages exchanged in this attack.

Similarly, an attacker can send instructions to change the route by manipulating the next waypoint. For example, the attacker can send a *UM63 AT [time] CROSS [position] AT AND MAINTAIN [altitude] AT [speed]* message that provides precise instructions on when to cross a position, at what altitude, and at what speed. However, CPDLC messages with multiple instructions may raise suspicion and may require further clarification.

4 PROOF-OF-CONCEPT IMPLEMENTATION

To realize the attacks proposed earlier, we implement and evaluate an ACARS message spoofer and a reactive jammer capable of jamming specific messages from predetermined aircraft. This implementation serves as a proof-of-concept for the most important component of the proposed attacks.

4.1 ACARS Message Spoofer

To realize the proposed attacks, the primary requirement of the attacker is the ability to spoof ACARS messages. ACARS uses a 2400 bps packet-like system that uses a Telex format for short messages. It uses a VHF carrier in the airband for data transmission. ACARS uses a modulation technique called as minimum shift keying (MSK). In the MSK scheme used for ACARS, a 1200 Hz tone marks a bit switch, and a 2400 Hz tone indicates that the bit remains unchanged. The MSK-encoded data is modulated onto a VHF carrier using amplitude modulation (AM) to use standard aircraft radio equipment. At 48000 samples/sec, each symbol is 416.67$\mu secs$

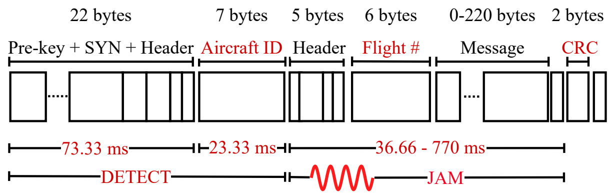


Figure 9: Time constraints: the reactive jammer has 36.66 to 770 ms (depending on the message length) to detect an incoming message, check the aircraft ID, and initiate the transmission to jam the ACARS packet.

The ACARS transmitter takes in a text message of at most 220 characters. Each 7-bit ASCII character is protected with an odd parity bit and is transmitted with the least significant bit first. A CCITT polynomial is used to calculate a 16-bit CRC. This checksum ensures the integrity of the entire message. Once the message is formatted correctly and the CRC appended, the data undergoes MSK modulation. The amplitude modulation technique modulates the baseband MSK signal onto a VHF carrier. In our transmitter design, we first create the ACARS packet according to the packet structure[5] and then modulate the data as per the specifications using a GNURadio [12] flowgraph.

GNURadio supports multiple RF-frontends. In our evaluation, we use a USRP B210 from Ettus. The transmitter design is based on various publicly available resources [5, 23]. CPDLC messages follow a specific message structure based on the regulation specified in [18]. It also provides an Abstract Syntax Notation One (ASN.1) structure for defining these messages. To encode/decode message strings, these messages use ISO/IEC 8825-2:1996 Packet Encoding Rules (PER) - Basic Unaligned [18]. Like the ACARS message, the CPDLC message string contains a separate 16-bit CRC value, specifically to detect errors at the application level.

The attacker also requires a receiver to intercept legitimate messages along with the message spoofer. Multiple open-source projects [42, 43, 56] provide the necessary software to receive and decode messages. From these, we use *acarsdec* [42], a popular ACARS decoder program. *Acarsdec* is a program written in C language that interfaces with an RTL-SDR. Along with ACARS messages, with the *libacars* [44] library, it can also decode FANS 1/A CPDLC and ADS-C messages. We evaluate and verify the ACARS message format and CPDLC structure using these tools.

4.2 ACARS Message Jammer

An essential component of our attack strategy is the message jammer. A jammer is an RF transmitter that transmits noise that disrupts wireless communications. For this attack, we implement two types of jammers, i) a random noise transmitting jammer and ii) a pulse jammer that transmits a short high powered pulse that distorts the message bits such that the receiver fails CRC checks and rejects the received packet. To evaluate our jammer's performance and effectiveness, we conducted experiments to check the ACARS receiver's packet reception rate. The experimental setup is as follows. We use a USRP B210 as the transmitter and an RTL-SDR with *acarsdec* as the receiver to perform these experiments. The transmitted signal contains the ACARS message. This message is combined with the jamming signal using a combiner and is fed directly into the receiver. It is important to note that all these experiments were conducted over hard-wired devices.

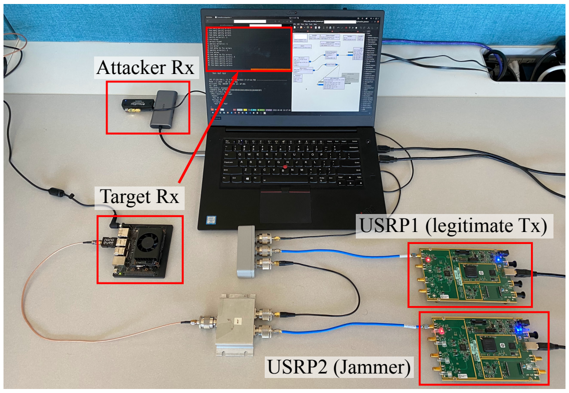


Figure 10: Reactive jammer evaluation setup. USRP1 transmits the legitimate message, and the attacker and target receivers simultaneously receive the messages. However, the attacker starts the jammer when it detects a message from a specific aircraft.

Unlike conventional jammers that jam regardless of transmission, a reactive jammer waits and jams only when it detects specific messages. In the past, researchers have explored and evaluated reactive jammers in the context of wireless networks [16, 47, 66]. In [68], authors demonstrate a reactive jamming that can achieve a reaction time of a few microseconds. There are lesser time constraints in the context of ACARS.Figure 9 shows the time constraints for jamming an ACARS packet.

We implement the reactive jammer using a combination of custom GNURadio blocks and an open-source software-defined ACARS receiver. Specifically, we modify the signal flow within Acarsdec to send a jamming signal to the jammer once it detects an ACARS message from the target aircraft. With a "start jamming" signal, our modified version of Acarsdec also sends a "stop jamming" signal as soon as it receives the entire message. Figure 10 shows a photo of the actual reactive jammer evaluation setup. The attacker can use strategic antenna placement and interference cancellation to avoid receiving its jamming signal. It is essential to stop the jamming signal because a prolonged transmission can draw out attention, and as a result, the attacker can be detected. This way, the attacker keeps the jamming duration short.

5 EXPERIMENTAL EVALUATION

An attacker needs to strategically position itself such that it minimizes the cost of attack and improves the odds of successful attack execution. Specifically, the attacker needs to choose carefully surveyed locations that facilitate relaxed power requirements for jamming and has a high probability of seeing an intersection as described in Section 3.6. To identify such regions we perform a geospatial analysis to justify the attacker position, specifically spoofer/jammer placement. This analysis also helps the attacker

[5] Refer to Table 1 in the appendix for detailed structure.

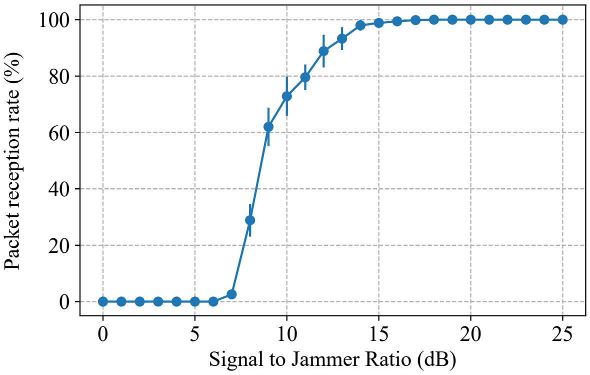


Figure 11: Packet reception rate for a jammer that implements a random noise source at various signal jammer ratios.

to determine a suitable location for executing coordinated multi-aircraft attacks by assessing the probability of intersecting routes.

5.1 ACARS Jammer Performance

We evaluate the jammer performance primarily through the packet reception rate across 10 iterations of each experiment. We first evaluate two types of jamming signal sources, i) noise jammer and ii) pulse jammer. We determine the ideal type of signal for the reactive jammer based on this evaluation. Given the legal limitations associated with the wireless transmission of ACARS messages, we ensure that there is no signal leakage by hardwiring the test equipment.

Noise Jammer: For the noise jammer we use the random noise source from GNURadio. The noise source is configured to generate random Gaussian noise. In the jammer evaluation experiment, we evaluate the packet reception rate for each signal-to-jammer ratio (SJR) value. From Figure 11 it can be seen that the packet reception rate is almost 0% for 6 dB SJR.

Pulse Jammer: Noise jammer requires continuous transmission at the specified power level. However, with a pulse jammer, an attacker can transmit high powered pulse for a shorter duration as compared to transmitting noise. As per the modulation scheme, change in frequency marks bit transition, an attacker can jam by transmitting a pulse that forces the receiver to compute a wrong CRC by either distorting the bit transitions or by distorting the bits themselves. To evaluate this technique, we analyzed the effect of pulse duration and power advantage on the packet reception rate of ACARS transmissions (Figure 12). An 11.66 ms pulse with 3 dB power advantage or a 6.25 ms pulse with a 10 dB power advantage is sufficient to achieve 97% jamming success.

Reactive Jammer: Based on the evaluation of the two jamming signal sources, we set the jammer source as random noise with 6 dB SJR. To evaluate the effectiveness of our reactive jammer, we perform an experiment where we measure the receiver's packet reception rate for messages with a length of 5 characters to 75 characters. This experiment's average packet reception rate was *98.85%* with 0.657 standard deviation. In this implementation, all the processing is done on the host PC running Ubuntu 20.04, with an 8^{th} Generation Intel Core i7 processor and 32 GB of RAM. Since the reactive jammer is implemented on the host PC, background OS tasks, processes, and operations add latency and cause processing overhead. As a result, the reactive jammer's turnaround time is *1.48 ms* which is sufficient for successfully jamming ACARS messages. The performance of the reactive jammer can be further improved by moving reactive jammer logic to an FPGA onboard a USRP or a suitable software-defined radio as described in [68].

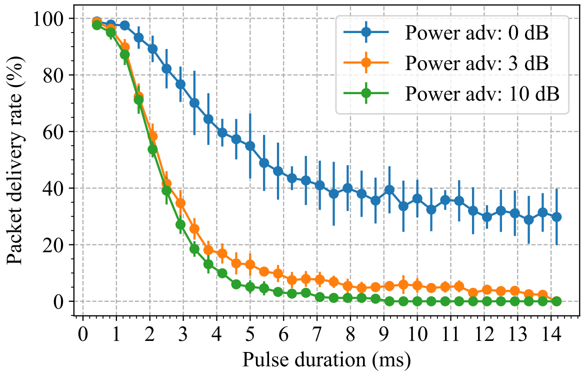


Figure 12: Packet reception rate for pulse jamming with varying pulse duration (ms) and power advantage (dB) that the attacker has over the legitimate signal as received by the target receiver.

5.2 Spoofer/Jammer Placement

To model power requirements for successful jamming, we use Friis's transmission eq. (1) that provides the received power level based on the specified transmitter configuration.

$$P_r = P_t + G_t + G_r + 20log_{10}\left(\frac{\lambda}{4\pi d}\right) \quad (1)$$

where P_r is the received power (dBm), P_t is the transmitted power (dBm), G_r receiver antenna gain (dBi), G_t is the transmitter antenna gain (dBi), λ is the wavelength of the carrier, and d is the distance between receiver and the transmitter. For this analysis we consider typical ground-station and airborne equipment with output power of 25W [13], receiver antenna gain of 2.15 dBi [13], aircraft's transmitter antenna gain as -1 dBi [51], attacker's transmitter antenna gain as 3 dBi, and attacker transmit power of 25W. Using these specifications[6], we calculate the SJR at the target ATSU as a function of its distance to the aircraft and the attacker. Figure 13 shows the SJR at various aircraft and attacker distances from the ATSU. For example, an attacker located 20 km from the ATSU can successfully jam messages from an aircraft as close as 4.8 km. This is sufficient because at 4.8 km, the aircraft is already on the final approach, and at this point, the flight crew is no longer relying on CPDLC messages. As the ratio of aircraft - ATSU distance and attacker - ATSU distance increases, the SJR at the ATSU decreases. It is important to note that, from the jammer's perspective, lower SJR means higher jammer success. This analysis also shows that it is more cost-effective for an attacker to jam at the ATSU rather

[6] Antenna gains may change depending on the specific antenna model

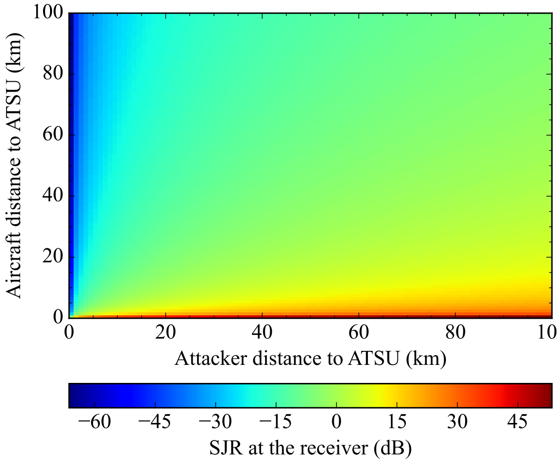


Figure 13: A heatmap showing the signal-to-jammer ratio at the receiver as a function of the target aircraft's distance to the ATSU and the attacker's distance to the ATSU. (Lower is in favor of the attacker)

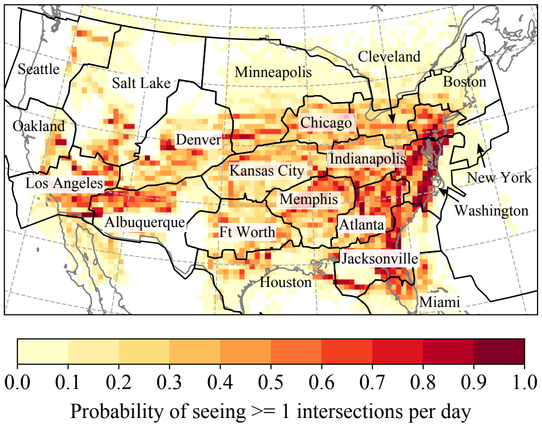


Figure 14: Probability of seeing at least one intersection/day in the US airspace. Probability is based on air traffic data from the year 2021. It also shows the boundary of air traffic centers that provide en-route services.

than jamming at the aircraft. Thus, being near the airport is more beneficial for the attacker but far enough to avoid detection by commercial RF interference detection systems like [9].

5.3 Probability of Intersecting Routes

analyzed To execute coordinated attacks on multiple aircraft, it is essential to identify regions that see flights whose trajectories intersect in time and space. We use publicly available ADS-B data obtained through Opensky Network [55] to identify and analyze such regions. Opensky Network is a crowd-sourced network of over 3500 sensors that have gathered over 25 trillion ADS-B, Mode-S, TCAS, and FLARM messages from more than 440,000 aircraft since 2013. We leverage this vast historical dataset and make use of custom SQL queries to obtain aircraft pairs such that their reported positions at the same time are within a 1000 m^2 bounding box. As a result of the lack of coverage, Opensky's data can be noisy. Hence, we further filter the data and remove duplicates.

Next, we divide the continental US into approximately 50 x 50 km cells and map each intersection to these cells. These dimensions were chosen keeping in mind the radio coverage of the attacker. This analysis identifies the most favorable regions for an attacker to set up and launch coordinated attacks. We performed this analysis on flight data from the year 2021; we saw a total of 592,224 intersections such that horizontal separation between aircraft < 100 m and altitude > 5000 m. Figure 14 shows the probability[7] of seeing at least one intersection per day in the respective cell. 0.91% of all the intersections occur in a single cell with an average of 15 intersections a day. 6.44% of intersections happen in the top 10 cells with the most frequent intersections. This map contains an overlay of airspace boundaries of centers that provide en-route services. Based on these boundaries and the locations of ground stations, an attacker can strategically choose a location by combining the jammer performance data obtained from Figure 13 and the region-wise probability of seeing intersections. To further improve the odds, we analyzed the hourly distribution of intersections for these top 10 cells and found that maximum intersections occur between 12 Hrs to 22 Hrs (UTC). Through this, we determine that the attacker has a better chance of succeeding if they target regions that consistently see at least one intersection/day.

6 DISCUSSION

Impact and Integrated Attacks: When successful, these attacks will directly influence the flight crew's decision-making and lead to mishaps. The aviation ecosystem is built on multiple redundancies and fallback mechanisms. There is always one other system that the pilots can use to complete the mission. Thus, in reality, the odds of a *standalone* attack on aviation datalink applications jeopardizing the safety of an aircraft are low. However, these attacks will have a high impact when integrated with attacks on other mission-critical avionics like ILS, GPS, and collision avoidance systems. For example, the described coordinated multi-aircraft attack along with attacks on the collision-avoidance system as shown in [61] and altimeter manipulation along with GPS [65, 69] and ILS [53] spoofing. An attacker can also spoof ADS-B and Mode-S to mask aircraft movement. Such integrated attacks target individual avionics, thus defeating the safety and security offered by redundant systems.

Countermeasures: These attacks require precise coordination and synchronization between various units. In addition, pilots are trained to detect discrepancies in their data. Even if they are instructed to follow the instruments, they rely on instincts. Contradictory to the instruments, if something doesn't feel right, pilots will execute fallback mechanisms as demanded by the training. A comprehensive countermeasure uses the public key infrastructure (PKI) for message signing that assures the sender and the receiver's identity. However, to maintain seamless interoperability, implementing resource-intensive solutions like PKI is complicated and expensive.

[7] Areas that do not see any intersection are marked as white.

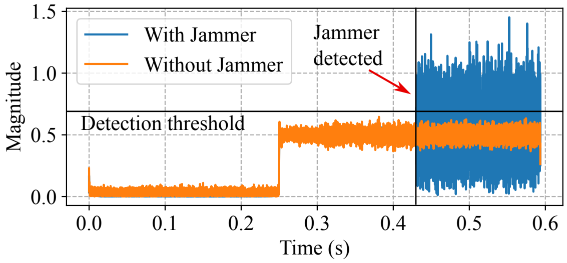


Figure 15: Reactive jammer detection (PoC). The receiver sets a threshold for envelop magnitude and bit error. It raises the alarm when both values cross the set threshold.

The proposed reactive jammer is stealthy as it transmits only for the duration of the message. Based on our analysis, we propose a reactive jamming scheme similar to [62]. In this scheme, we perform physical and application layer checks to detect a reactive jammer by correlating bit errors and the magnitude of the signal's envelope for the duration of each bit. Under a reactive jamming attack, the jammer corrupts only a portion of the message. This means the receiver successfully decodes a part of the message. In a non-adversarial setting, the receiver will experience a uniform signal magnitude. However, when the reactive jammer starts, the receiver will experience a sudden increase in the envelop magnitude and the number of bit errors. Figure 15 shows a PoC of this technique. Once jamming is detected, the controllers can contact the victim aircraft over a voice channel. Such a countermeasure can be implemented purely in software with minimal signal processing.

7 RELATED WORK

The aviation industry includes a variety of analog and digital RF communication and navigation systems. System developers and manufacturers have failed to consider security as an integral part of the system design. As a result, these systems are vulnerable to cyber-physical attacks that can cause serious damage. Strohmeier et al. in [64] show the vulnerabilities present in modern aviation systems. In recent years, researchers have repeatedly demonstrated the ability to spoof GPS [4, 8, 48, 58, 65, 69], ADS-B [17, 45, 54, 63], ILS [53] and even collision avoidance systems [61].

However, there is very limited work that investigates the security guarantees of aviation datalink applications. The work closest to ours is [59]. The authors provide an overview of attack strategies and propose a MiTM attack that specifically targets the handover process. They also suggest cryptographic solutions for securing aviation datalink. They suggest the need for selective jamming, however, they do not study the feasibility and performance of such a jammer. In our work, we describe specific attack scenarios that exploit certain message sets as well as provide a PoC and performance evaluation of the reactive jammer that enables these attacks.

In [70], the authors present message monitoring, entity camouflage, and MiTM attacks. However, they fail to consider the required message acknowledgment and flight crew input. Even though such a strategy is effective, the ATSU will detect the attack. [15, 19] describe the possibility of using software-defined radios to enable an attacker to transmit fabricated messages. Specifically, [15] presents an attack targeting the manipulation of take-off speed recommendations, including speeds that the flight crew should use for a safe and efficient take-off. Authors in [57] present an analysis of CPDLC communications, specifically in the context of ATN B1 application that is predominantly used only in Europe. In [60], the authors specifically focus on privacy issues associated with ACARS transmissions. These works show that aviation datalink applications are not only vulnerable to invasive, message manipulation attacks, but also to disclosure of privileged information.

Researchers have proposed various application-layer solutions to secure ACARS messages. Most notably in [46, 52], authors have proposed cryptographic solutions that use a symmetric session key for data encryption and PKI for authenticating and validating entities. Based on these proposals, Aeronautical Radio INC (ARINC) has developed industry standards 823 P1/2 that provides guidelines for ACARS message security (AMS) [49] Currently, AMS is used explicitly by the US military. Similarly, in [39] the authors propose a secure CPDLC scheme that leverages Elliptic curve cryptography. They evaluate their protocol and provide formal verification using ProVerif, a Dolev-Yao attacker model-based security verification tool. In [59], authors also suggest various non-cryptographic detection techniques that use the aircraft's geo-location to determine if a certain connection is valid.

8 CONCLUSION

In this work, we performed a security analysis of aviation datalink applications like CPDLC and ADS-C. Specifically, we outlined the requirements for executing a successful attack that has the potential of influencing the pilots' decision-making. We described attacks that target individual aircraft as well as coordinated attacks that simultaneously target multiple aircraft. A geospatial analysis of historical air-traffic data identified 48 vulnerable regions where an attacker has a 90% chance of encountering favorable conditions for coordinated multi-aircraft attacks. We also proposed a reactive jammer to enable the stealthy execution of these attacks. Through experiments and real-world implementation, we demonstrated and evaluated the performance of a reactive jammer that can selectively jam specific messages from a particular aircraft with a reaction time of 1.48 ms and 98.85% jamming success. Through this work, we aim to raise awareness regarding the risks associated with even complimentary systems. The proposed attacks, when combined with attacks on other avionics, magnifies the threat. And till date, these critical systems remain vulnerable and qualify as prime targets.

ACKNOWLEDGMENTS

This work was partially supported by grants NAVY/N00014-20-1-2124, NCAE-Cyber Research Program, and NSF/DGE-1661532.

REFERENCES

[1] 2009. *Commission Regulation (EC) No 29/2009 of 16 January 2009 laying down requirements on data link services for the single European sky (Text with EEA relevance)2009.* http://data.europa.eu/eli/reg/2009/29/oj/eng.

[2] 2009. EUROCONTROL SPECIFICATION on Data Link Services. https://www.eurocontrol.int/sites/default/files/publication/files/20090128-dls-spec-v2.1.pdf.

[3] 2013. BRC HP-50-A 118-136 MHZ AIRBAND BAND BASE ANTENNA. https://buyantenna.com/index.php?route=product/product&product_id=555.

[4] 2013. UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

[5] 2016. ACARS. https://www.wavecom.ch/content/ext/DecoderOnlineHelp/default.htm#!worddocuments/acars.htm.

[6] 2017. ADALM-PLUTO. https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html#eb-overview.

[7] 2017. ZHL-03-5WF+ High Power Amplifier, 60 - 300 MHz. https://www.minicircuits.com/WebStore/dashboard.html?model=ZHL-03-5WF%2B.

[8] 2019. How Hackers Can Take Over Your Car's GPS. https://www.bloomberg.com/news/articles/2019-06-19/threat-of-gps-spoofing-for-autonomous-cars-seen-as-overblown.

[9] 2020. AIRPORT-SHIELD - Protection against radio interferences in airports. https://www.loginshowroom.com/c-esm-comint/airport-shield-interference-detection-and-geolocalisation/.

[10] 2020. Incorrect altimeter setting results in CFIT. https://generalaviationnews.com/2020/10/19/incorrect-altimeter-setting-results-in-cfit/.

[11] 2020. North Atlantic Data Link Mandate March 2020 Update. https://www.faa.gov/air_traffic/publications/internationalnotices/intl_2_20002.html.

[12] 2022. GNURadio. https://www.gnuradio.org/.

[13] ASRI. 2009. Aeronautical Frequency Committee (AFC) VHF Ground Station Installation Guidelines. https://asri.aero/wp-content/uploads/2012/07/VhfStationGuidelines.pdf.

[14] Boeing. 2021. STATISTICAL SUMMARY OF COMMERCIAL JET AIRPLANE ACCIDENTS Worldwide Operations | 1959 – 2020. https://www.boeing.com/resources/boeingdotcom/company/about_bca/pdf/statsum.pdf.

[15] Corentin Bresteau, Simon Guigui, Paul Berthier, and José M Fernandez. 2018. On the security of aeronautical datalink communications: Problems and solutions. In *2018 Integrated Communications, Navigation, Surveillance Conference (ICNS)*.

[16] Gonglong Chen and Wei Dong. 2018. Jamcloak: Reactive jamming attack over cross-technology communication links. In *2018 IEEE 26th International Conference on Network Protocols (ICNP)*.

[17] Andrei Costin and Aurélien Francillon. 2012. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *black hat USA* (2012).

[18] Dave Allen, Martine Blaize, Serge Bagieu, Tom Kraft, Peter Skaves, Anne-Sophie Luce, Tony Martin, Mark Joseph, Elizabeth Noon, Marc Barrere. 1998. Interoperability Requirements for ATS Applications Using ARINC 622 Data Communication Document. https://www.asas-tn.org/library/standardisationsbodies/eurocae/g1-019.pdf/preview_popup/file.

[19] Sofie Eskilsson, Hanna Gustafsson, Suleman Khan, and Andrei Gurtov. 2020. Demonstrating ADS-B and CPDLC Attacks with Software-Defined Radio. In *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*.

[20] FAA. 2022. Barometric Altimeter Errors and Setting Procedures. https://www.faa.gov/air_traffic/publications/atpubs/aim_html/chap7_section_2.html.

[21] FAA. 2022. Next Generation Air Transportation System (NextGen). https://www.faa.gov/nextgen/

[22] Christine Falk, Lauren Martin, and Theresa Brewer-Dougherty. 2009. Examination of Airborne Position-Time Estimates From Enroute Automatic Dependent Surveillance. In *AIAA Guidance, Navigation, and Control Conference*.

[23] Jaroslav Henner. 2010. ACARS (Aircraft Communications Addressing and Reporting System). (2010).

[24] Honeywell Aerospace. 2014. Review of Aviation Mandates. https://pages3.honeywell.com/rs/honeywell3/images/hon___aviation_mandates_whitepaper_d3b_revised.PDF.

[25] IATA. 2021. Industry Statistics Fact Sheet. https://www.iata.org/en/iata-repository/publications/economic-reports/airline-industry-economic-performance---october-2021---data-tables/.

[26] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 4.5.

[27] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 2.2.4.7.1.

[28] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 3.1.2.

[29] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 2.2.4.3.2.

[30] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 2.2.6.3.2.

[31] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter Appendix A.3/4.

[32] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 5.3.5.

[33] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 2.2.5.2.5.

[34] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter E4.2.1.1.

[35] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 2.2.6.5.

[36] ICAO. 2014. Global Operational Data Link Document (GOLD) 2^{nd} Edition.

[37] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 2.2.6.3.6.

[38] ICAO. 2014. *Global Operational Data Link Document (GOLD) 2^{nd} Edition*. Chapter 4.2.3.3.

[39] Suleman Khan, Andrei Gurtov, An Breaken, and Pardeep Kumar. 2021. A Security Model for Controller-Pilot Data Communication Link. In *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*.

[40] Anthony Klancher. 2019. FAA Anchorage ARTCC Facility Update. https://www.faa.gov/sites/faa.gov/files/about/office_org/headquarters_offices/ato/IPACG45.zip.

[41] L3Harris Technologies, Inc. 2022. FEDERAL AVIATION ADMINISTRATION (FAA) DATA COMMUNICATIONS (DATA COMM) USER INFORMATION. https://www.l3harris.com/datacomm.

[42] Thierry Leconte. 2016. An ACARS SDR decoder for airspy and rtl-sdr. https://github.com/TLeconte/acarsdec.

[43] Tomasz Lemiech. 2017. VDL Mode 2 message decoder and protocol analyzer. https://github.com/szpajder/dumpvdl2.

[44] Tomasz Lemiech. 2018. libacars. https://github.com/szpajder/libacars.

[45] Donald L McCallie. 2011. *Exploring Potential ADS-B Vulnerabilites in the FAA's Nextgen Air Transportation System*. Technical Report. AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH DEPT OF ELECTRICAL AND COMPUTER ENGINEERING.

[46] Tom McParland. 2004. Application Level Security Considerations. In *Aeronautical Communication Panel Working Group N – Networking Subgroup N4 - Security*.

[47] Danh Nguyen, Cem Sahin, Boris Shishkin, Nagarajan Kandasamy, and Kapil R Dandekar. 2014. A real-time and protocol-aware reactive jamming framework built on software-defined radios. In *Proceedings of the 2014 ACM workshop on Software radio implementation forum*.

[48] Juhwan Noh, Yujin Kwon, Yunmok Son, Hocheol Shin, Dohyun Kim, Jaeyeong Choi, and Yongdae Kim. 2019. Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Transactions on Privacy and Security (TOPS)* (2019).

[49] Michael Olive. 2009. ACARS Message Security (AMS) as a Vehicle for Validation of ICAO Doc. 9880 Part IV-B Security, Requirements. *ICAO ACP WG-M Meeting 14 M Meeting 14* (2009).

[50] Anna Patty. 2016. Fatal consequences of miscommunication between pilots and air traffic controllers. *The Sydney Morning Herald* (2016). https://www.smh.com.au/business/workplace/the-fatal-consequences-of-miscommunication-between-pilots-and-air-traffic-controllers-20160928-grq1d9.html.

[51] Claude Pichavant. 2021. VHF antenna radio patterns to support ITU WRC-23 Agenda Item 1.7 on Space-based VHF. https://www.icao.int/safety/FSMP/MeetingDocs/FSMP%20WG11/WP/FSMP-WG11-WP11_Airbus_VHF%20antenna%20pattern%20to%20support%20ITU%20WRC-23%20AI%201.7.doc.

[52] Aloke Roy. 2004. Secure aircraft communications addressing and reporting system (ACARS). US Patent 6,677,888.

[53] Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir. 2019. Wireless attacks on aircraft instrument landing systems. In *28th USENIX Security Symposium (USENIX Security 19)*.

[54] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. 2013. Experimental analysis of attacks on next generation air traffic communication. In *International Conference on Applied Cryptography and Network Security*.

[55] Matthias Schäfer, Martin Strohmeier, Vincent Lenders, Ivan Martinovic, and Matthias Wilhelm. 2014. Bringing up OpenSky: A large-scale ADS-B sensor network for research. In *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*.

[56] SDRPlay. 2017. Decoding ACARS messages using SDRuno and MultiPSK. https://www.sdrplay.com/docs/SDRuno_ACARS.pdf.

[57] Isak Sestorp and André Lehto. 2019. CPDLC in Practice: a Dissection of the Controller Pilot Data Link Communication Security.

[58] Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. 2012. Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle. (2012).

[59] Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2021. You talkin't to me? Exploring Practical Attacks on Controller Pilot Data Link Communications. In *Proceedings of the 7th ACM on Cyber-Physical System Security Workshop*.

[60] Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2018. Undermining privacy in the aircraft communications addressing and reporting system (ACARS). *Proceedings on Privacy Enhancing Technologies* (2018).

[61] Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2022. Understanding realistic attacks on airborne collision avoidance systems. *Journal of Transportation Security* (2022).

[62] Mario Strasser, Boris Danev, and Srdjan Čapkun. 2010. Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks (TOSN)* (2010).

[63] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2014. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Communications Surveys & Tutorials* (2014).

[64] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. 2016. On perception and reality in wireless air traffic communication security. *IEEE transactions on intelligent transportation systems* (2016).

[65] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. 2011. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security.*

[66] Mathy Vanhoef and Frank Piessens. 2014. Advanced Wi-Fi attacks using commodity hardware. In *Proceedings of the 30th Annual Computer Security Applications Conference.*

[67] Jon S Warner and Roger G Johnston. 2002. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *Journal of security administration* (2002).

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

[69] Kexiong Curtis Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang. 2018. All your {GPS} are belong to us: Towards stealthy manipulation of road navigation systems. In *27th USENIX security symposium (USENIX security 18).*

[70] Ru Zhang, Gongshen Liu, Jianyi Liu, and Jan P Nees. 2017. Analysis of message attacks in aviation data-link communication. *IEEE Access* (2017).

ABBREVIATIONS

ACARS aircraft communications, addressing, and reporting system
ADS-B automatic dependent surveillance-broadcast
ADS-C automatic dependent surveillance-contract
AMS ACARS message security
ARINC Aeronautical Radio INC
ATC Air traffic controllers
ATN Aeronautical telecommunications network
ATSU Air Traffic Services Unit
CDA current data authority
CPDLC controller-pilot datalink communications
CRC cyclic redundancy checksum
D-ATIS digital automatic terminal information service
FMS flight management system
FANS future air navigation systems
GPS global positioning system
ICAO international civil aviation organization
ILS instrument landing system
MSK minimum shift keying
NDA next data authority
PER Packet Encoding Rules
PDC pre-departure clearance
SJR signal-to-jammer ratio
VHF very high frequency

APPENDIX

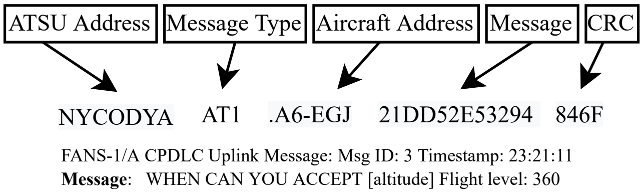

ATSU Address
Message Type
Aircraft Address
Message
CRC
NYCODYA
AT1
.A6-EGJ
21DD52E53294
846F
FANS-1/A CPDLC Uplink Message: Msg ID: 3 Timestamp: 23:21:11
Message: WHEN CAN YOU ACCEPT [altitude] Flight level: 360

Figure 16: The message structure for a CPDLC message and an example CPDLC message received during our analysis and evaluation.

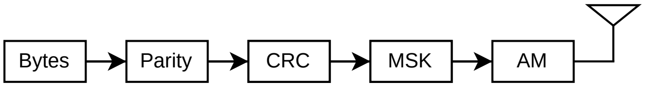
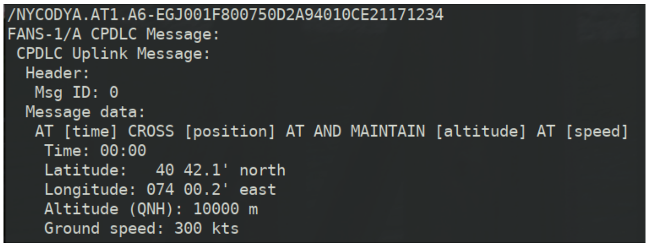
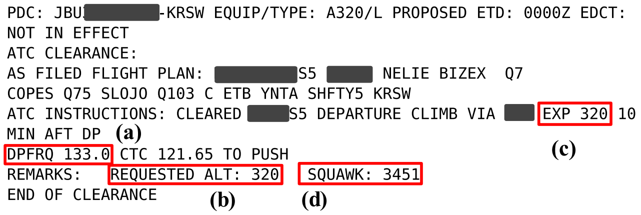


Figure 17: Block diagram of ACARS transmitter.



```
/NYCODYA.AT1.A6-EGJ001F800750D2A94010CE21171234
FANS-1/A CPDLC Message:
 CPDLC Uplink Message:
  Header:
   Msg ID: 0
  Message data:
   AT [time] CROSS [position] AT AND MAINTAIN [altitude] AT [speed]
    Time: 00:00
    Latitude:   40 42.1' north
    Longitude: 074 00.2' east
    Altitude (QNH): 10000 m
    Ground speed: 300 kts
```

Figure 18: A UM63 command to instruct an aircraft to set the following waypoint location and altitude as received and decoded by *acarsdec* and *libacars*. It also provides instructions on the target speed, and time the aircraft should cross the waypoint.



```
PDC: JBU[redacted]-KRSW EQUIP/TYPE: A320/L PROPOSED ETD: 0000Z EDCT:
NOT IN EFFECT
ATC CLEARANCE:
AS FILED FLIGHT PLAN: [redacted]S5 [redacted] NELIE BIZEX  Q7
COPES Q75 SLOJO Q103 C ETB YNTA SHFTY5 KRSW
ATC INSTRUCTIONS: CLEARED [redacted]S5 DEPARTURE CLIMB VIA [redacted] EXP 320 10
MIN AFT DP
DPFRQ 133.0 CTC 121.65 TO PUSH
REMARKS:   REQUESTED ALT: 320  SQUAWK: 3451
END OF CLEARANCE
```

Figure 19: An example PDC that we intercepted. (a) mentions the departure and the ground frequency in (MHz) that the flight crew should contact, (b) and (c) shows the requested altitude and the approved altitude. (d) shows the assigned squawk code.