

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Sliding into the Flight Deck's DMs: Practical Message Attacks on CPDLC

Mehdi Ziazi, *ETH Zurich;* Khalid Aleem, *Independent;* Harshad Sathaye, *ETH Zurich;* Martin Strohmeier, *Cyber-Defence Campus, armasuisse Science + Technology*

https://www.usenix.org/conference/usenixsecurity26/presentation/ziazi

This paper is included in the Proceedings of the 35th USENIX Security Symposium.

August 12–14, 2026 • Baltimore, MD, USA

ISBN 978-1-939133-58-8

Open access to the Proceedings of the 35th USENIX Security Symposium is sponsored by



جامعة الملك عبدالله للعلوم والتقنية

King Abdullah University of Science and Technology

ARTIFACT EVALUATED
USENIX
AVAILABLE

Sliding into the Flight Deck's DMs: Practical Message Attacks on CPDLC

Mehdi Ziazi
Department of Computer Science
ETH Zurich, Switzerland

Khalid Aleem
Independent
London, United Kingdom

Harshad Sathaye
Department of Computer Science
ETH Zurich, Switzerland

Martin Strohmeier
Cyber-Defence Campus
armasuisse S + T, Switzerland

Abstract

The Controller–Pilot Data Link Communications (CPDLC) system has become integral to modern air traffic management, particularly in high-density or oceanic airspace where voice communication is limited or unavailable. Designed to increase operational efficiency, CPDLC is an alternative to traditional VHF voice communication with standardized digital messages for altitude changes, heading adjustments, free-text messages, and frequency handovers. However, CPDLC does not implement encryption and relies primarily on protocol complexity and obscurity as a barrier to misuse.

In this work, we present a full-stack security analysis of CPDLC and showcase several vulnerabilities that allow hijacking ATC-Pilot link with rogue ground station attacks and large-scale denial of service attacks that are capable of disabling CPDLC services for all aircraft in radio range. As a proof-of-concept, we also introduce `cpdlc-gs`, a *first* SDR based full-stack CPDLC ground-station implementation capable of injecting uplink messages to issue fake CPDLC flight instructions and effective denial of service attacks. Furthermore, to evaluate `cpdlc-gs`, together with air navigation service providers and avionics manufacturers, we develop a novel, fully-functional test environment with real, certifiable hardware from Universal Avionics. Through such a setup we conceptualize and validate several attacks and demonstrate that even isolated rogue stations can pose a substantial threat, especially when pilots are under high workload or in degraded communication scenarios. Overall, we argue that the heavy reliance and global adoption of CPDLC make it a high value target, and that the lagging aviation datalink security standardization process needs to be urgently addressed.

1 Introduction

Modern air traffic control (ATC) increasingly relies on digital communications to manage growing volumes of aircraft with greater efficiency and safety. Among these systems, *Controller-Pilot Data Link Communications* (CPDLC) has become a critical component as it improves over traditional analog voice instructions with structured digital messages exchanged between aircraft and ground stations. CPDLC has gained widespread adoption due to its operational efficiency, reduced voice channel congestion, decreased human error, and environmental benefits such as lower CO_2 emissions [44].

CPDLC was standardized primarily with functionality in mind, and its development did not incorporate a robust threat model involving malicious actors. As a result, the protocol lacks essential security features, including encryption, authentication, and cryptographic message integrity. The security literature has already postulated several classes of radio-based attacks against CPDLC, particularly spoofing and injection [8, 38, 42]. However, most of this prior work focuses solely on the application layer of the CPDLC stack and all fail to demonstrate that they work in practice.

We argue that analyzing the application layer in isolation is insufficient to understand or execute real-world RF attacks. In practice, successful exploitation requires detailed knowledge of the full communication stack, from physical and data link layers to session and application logic. This necessitates dealing with a complex black-box network stack, reverse engineering undocumented checksums and proprietary implementations, and obtaining access to compliant avionics systems and operational procedures.

We develop a low-cost, software-defined radio (SDR) suite `cpdlc-gs` capable of implementing arbitrary attacks on the full protocol stack. Illustrated in Figure 1, we demonstrate how to conduct broadcast denial of service attacks and create rogue ground stations capable of issuing malicious commands to the pilot, which are safety-critical but cannot be detected or prevented by the system.

To further bridge theory and practice, we build a real-world test environment with certified avionics hardware and access to ground stations used by regulators for testing aircraft compliance. This unique aviation security testbed, developed in collaboration with avionics manufacturers, enables safe and reproducible experimentation under controlled conditions.

The implications of such attacks are severe. For denial

of service attacks, the fallback to redundant systems may not be immediate, particularly in oceanic airspace or during high-workload phases of flight. Worse, a rogue CPDLC station can issue malicious instructions that redirect aircraft into conflict zones, restricted airspace, or towards other aircraft. Unlike voice-based communications, which contain natural cues like tone, accent, and dialogue consistency that can help with spoofing detection [45], digital CPDLC messages are perceived as authoritative and generally acted upon without question. Pilots place a high level of trust in the system as demonstrated in recent surveys [7, 46, 49].

Although other aircraft systems have already been shown to be vulnerable to RF injection in practice [2,32,38,39], no prior public research has demonstrated successful CPDLC attacks in the wild. This work bridges that gap between theoretical attack surface and operationally viable exploits.
Our contributions are as follows:

- **System-level security analysis:** We present the first full-stack examination of CPDLC, identifying novel vulnerabilities beyond the application layer and evaluating their real-world exploitability.
- **SDR-based attack implementation:** We develop a commercial SDR suite capable of implementing arbitrary attacks on the protocol stack. We use it to design and test a range of novel DoS attacks and implement a full CPDLC ground station capable of issuing valid uplink messages to operational aircraft.
- **Real-world testbed integration:** We build a unique CPDLC avionics security lab with live network access and certified hardware, enabling safe, high-fidelity experimentation and impact assessment.
- **Mitigations and countermeasures:** We analyse the avionics datalink security standardisation process and discuss potential countermeasures from the literature.

2 Background

2.1 Limitations of Voice Communication in Air Traffic Control and the Rise of CPDLC

For decades, analog voice radio has served as the backbone of controller–pilot communication. Despite its widespread adoption, it is subject to inherent limitations. Voice channels are highly congested in busy airspace, leading to frequent transmission delays, overlaps, and radio blocking. Readback errors and miscommunications are common, especially under high workload or in low-quality radio environments [44].

To address these limitations, CPDLC has emerged as a digital alternative. It provides a structured text-based messaging protocol that reduces channel load, improves clarity, and supports communication when voice is unavailable or unreliable. It enables pilots and controllers to exchange standard messages such as altitude clearances, frequency handoffs, free-texts and route adjustments.

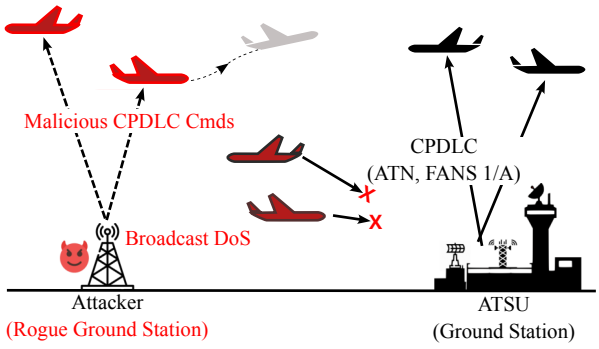


Figure 1: A schematic representation of aviation datalink infrastructure and proposed attacker's rogue ground station capable of injecting malicious CPDLC messages and launching broadcast DoS attacks.

CPDLC adoption has been steadily increasing in global airspace and is becoming standard through initiatives such as Europe's Link 2000+ program. Older aircraft are gradually being upgraded with CPDLC capabilities to comply with regulatory requirements, while new aircraft include it by default. As aviation authorities increasingly adopt digital communication systems, CPDLC is becoming a universal component of global air traffic control infrastructure.

2.2 CPDLC Implementations: FANS-1/A over ACARS vs. ATN-B1

CPDLC is currently deployed through two main implementations: **FANS-1/A+ over ACARS** and **ATN B1 over VDL Mode 2**. These systems serve different airspace needs and have different technical architectures, although both enable similar functionality at the application level.

FANS-1/A+, the earlier of the two, operates over the ACARS network using HF, VHF, or Satcom links. Although it provides lower data throughput, it remains essential for long-haul and transoceanic operations due to its wide compatibility with existing aircraft systems, particularly in the US, and relatively lightweight infrastructure.

ATN B1 CPDLC, in contrast, is used predominantly in continental and high-density airspace, particularly in Europe. It operates over VDL Mode 2, offering higher data rates, improved message integrity (via Protected Mode CPDLC), and more structured communication. Unlike FANS, it integrates directly with radar and transponder systems. ATN B1's architecture reflects the demands of a more interconnected and performance-driven data-link environment, with intricate link and session management, robust integrity features, and tightly

Table 1: PM-CPLDC ATN-B1 protocol stack

Layer 7 (Application)	-	CPDLC Message
Layer 6 (Presentation)	-	Protected PDU
Layer 6 (Presentation)	-	ICAO FED
Layer 5 (Session)	ATN CM	-
Layer 5 (Session)	ACSE X.227	-
Layer 5 (Session)	SPDU X.225	-
Layer 4 (Transport)	COTP X.224	
Layer 3 (Network)	CLNP X.233	
Layer 2 (Datalink)	X.25 Packet	
Layer 2 (Datalink)	AVLC Frame	
Layer 1 (PHY)	VDL Mode 2	
Layer 1 (PHY)	D8PSK @ 31.5 Kbps	

coupled ground systems. It has been mandatory in European airspace above FL285 (28,500 feet) since 2013.

While both implementations support similar message sets at the application layer, their protocol stacks, addressing mechanisms, and system integration are different. In this work, we analyze ATN B1's richer and more complex capabilities, which have so far been ignored by the security literature.

2.3 CPDLC Protocol Stack over ATN B1

CPDLC communication over ATN-B1 follows a classic OSI-based protocol stack illustrated in Table 1. In the following, we discuss the concrete instantiation of the stack and present the fully reverse engineered and previously undocumented CPDLC connection establishment in Figure 2.

VHF (Very High Frequency): Aviation uses the 117.975 to 137 MHz band, over which data and voice services are provided. Two primary avionic data links are carried over VHF: ACARS (Aircraft Communications Addressing and Reporting System) and VDL2 (VHF Digital Link mode 2). VDL2 is the newer system used in ATN-B1.

VDL2: VDL2 defines a single carrier-modulated channel in the VHF band, using Differential 8-Phase Shift Keying (D8PSK) at a symbol rate of 10.5 ksymbols/s. Each transmission begins with a ramp-up and preamble sequence, followed by a scrambled, error-corrected payload. The bitstream is first interleaved with Reed Solomon forward error correction, scrambled using a pseudo-noise (PN) sequence, and framed with standard HDLC delimiters (0x7E) and bit stuffing. The resulting waveform is shaped using a raised cosine filter (roll-off factor $\alpha = 0.6$).

Advanced Link Control (AVLC): AVLC is a modified High-Level Data Link Control (HDLC) protocol for aeronautical VHF links. It handles sequence numbering, data transfer (I frames), error recovery (U frames), basic flow control (S frames), and many other basic mechanisms.

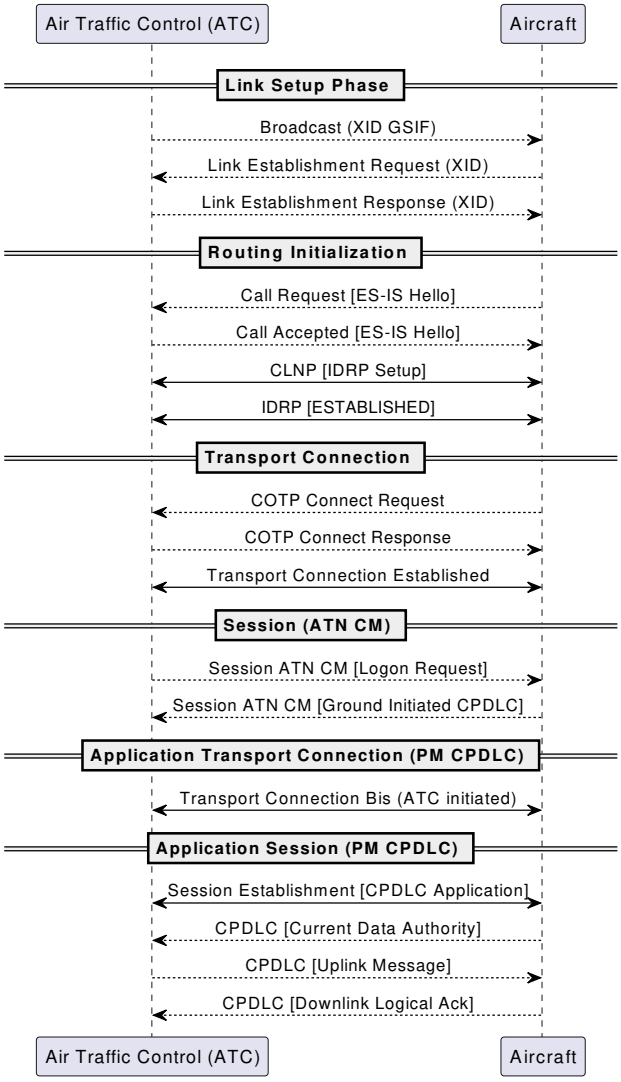


Figure 2: Simplified CPDLC connection establishment. At the end, the ground station is authenticated as the Current Data Authority to the aircraft and can send uplink messages.

Link Establishment: VDL2 uses XID (Exchange Identification) on AVLC U frames at the data link layer to negotiate link parameters. The ground station initiates the exchange by advertising capabilities such as supported frequencies, system capabilities, location, link layer parameters and ATN routing information. The aircraft responds with its own configuration, including modulation support and location. Once the negotiation completes, the higher level data is encapsulated in AVLC I frames.

X.25: X.25 operates on AVLC and establishes virtual circuits. It encapsulates data from the higher layer and supports

Work	DoS	Rogue GS	Real-World	FANS-1/A / ATN-B1	Lower Layer	Impl.	Certified HW
Di Marco et al. [5]	–	◐	–	CPDLC (generic)	–	◐	–
Eskilsson et al. [8]	–	–	◐	FANS-1/A	◐	✓	–
Smailes et al. [42]	–	✓	◐	CPDLC (generic)	–	◐	–
Lehto et al. [30]	–	–	◐	ATN-B1	–	◐	–
Orye et al. [35]	–	–	◐	ATN-B1	–	–	–
Sathaye et al. [38]	✓	–	◐	FANS-1/A	◐	✓	–
This work	✓	✓	✓	**ATN-B1 (full stack)**	✓	✓	✓

Table 2: CPDLC-related prior work vs. attack and evaluation dimensions.

logical channel multiplexing and basic flow control.

End System-to-Intermediate System (ES-IS): ES-IS is a discovery protocol to derive Network Service Access Point (NSAP) addresses from X.25 Data Terminal Equipment (DTE) addresses necessary for the network layer.

ConnectionLess Network Protocol (CLNP) X.233: CLNP provides NSAP-based addressing, routing, error reports, and Protocol Data Unit (PDU) lifetime control. It may use compressed headers for efficiency.

Inter Domain Routing Protocol (IDRP): IDRP is a connection-oriented routing information exchange protocol similar to BGP which is located within the network layer (CLNP). Each routing domain chooses its routing policies independently, insures that all its border intermediate systems calculate inter-domain paths which satisfy those policies and select the paths that it will advertise externally. This is achieved by making IDRP carry path information, routes and routes information, routing domains and many other fields.

Connection-Oriented Transport Protocol (COTP) X.224: COTP provides a reliable, connection-oriented transport service. It supports connection setup, error reports, flow control, and retransmission. It is functionally similar to TCP but defined within the OSI model. The COTP handshake results in one of 5 protocol classes (0 to 4), each ensuring an increasing level of integrity protection, error detection as well as additional options like the use of the ATN checksum.

X.225 - Session Layer: X.225 manages the dialog control. It uses Session Protocol Data Units (SPDUs) such as (Short) Connect and (Short) Refuse to initiate/reject and maintain sessions. The session layer is also responsible for defining the encoding of the higher ACSE layer.

ACSE (Association Control Service Element) X.227: ACSE establishes application associations. It supports connection, authentication, context negotiation, and access control for application protocols like CPDLC. The first application invoked upon a connection request/response will be the ATN Context Management application.

ATN Context Management (ATN CM): The ATN Context Management (CM) application facilitates the initial setup and maintenance of data link communication services between an aircraft and ground systems. It is responsible for the exchange of addressing information related to all ATN applications. The process begins when the aircraft's CM initiates a logon request to the ground CM system. Upon successful logon, the ground responds with the appropriate Transport Service Access Point (TSAP) addresses for the supported applications. Once received, the aircraft can establish communication with ground-based services, including CPDLC.

Protected Mode CPDLC: (PM) CPDLC uses Abstract Syntax Notation (ASN1) unaligned packet rules (UPER) encoding. A protected PDU encapsulates the transmitted CPDLC message with an additional protection checksum. The resulting protected PDU is finally encoded as an ICAO Fully Encoded Data (ICAO FED) and handed to the transport layer for transmission.

3 Related Work

The academic literature has seen the potential threat of insecure CPDLC since at least 2001 [34, 41], although practically all work has remained in the theoretical risk assessment phase and does either not engage with the high complexity of the lower layers or forego an implementation entirely.

Di Marco et al. [5] developed a security-testing framework for the generic CPDLC application layer and examine the packet injection and manipulation case in a simulated setting. Notably, they assume the MITM position within the local network or radio link as given. After debriefing air traffic controllers, they note that CPDLC attacks are very risky without out-of-band radio backup. Eskilsson et al. [8] craft and inject CPDLC messages on the legacy FANS-1/A, demonstrating the feasibility of over-the-air attacks in a simulated environment with SDRs, and using simulation on both ends of the network. While open libraries such as *libacars* are useful for first tests, transmitting CPDLC in this way to certified

avionics hardware without implementing lower layers and tracking the protocols' state machines will be unsuccessful in the real world. Smailes et al. [42] analyzed generic CPDLC protocol vulnerabilities and presented a rogue ground station concept with a real-world data collection but no implementation of the attack itself. Lehto et al. [30] conducted a first study on ATN-B1 CPDLC security, highlighting unauthenticated message risks based on passive data capture and analysis. It does not include discussion of the ATN-B1 stack or practical, real-world implementations. Similarly, Orye et al. [35] characterized large-scale CPDLC traffic over VDL2, revealing structural weaknesses and operational patterns that could enable targeted attacks. Finally, Sathaye et al. [38], who are closest to this work, demonstrated coordinated spoofing and reactive jamming attacks on aviation datalinks, discussing their implications for CPDLC security over the legacy FANS-1/A. They provide a proof-of-concept implementation for the higher layers of CPDLC and analyse these in the laboratory without a certified real-world network setup.

To date, no research has demonstrated a non-speculative, cross-layer, practical attack against CPDLC that includes physical transmission, data link negotiation, network routing, session establishment, and message delivery at the application layer. Even theoretical attacks tend to omit the complexity of real-world ATN-B1 operation, which includes strict adherence to protocol sequencing, encoding schemes, and compliance with aircraft-side state machines. Our work addresses all these shortcomings and `cpdlc-gs` presents the first SDR suite in which we implement a live, full-stack implementation of a malicious ground station capable of issuing valid CPDLC messages to certified avionics systems.

4 Threat Model and Challenges

4.1 Threat Model

In this paper, we consider an attacker whose primary objective is to cause a kinetic impact on the target aircraft, such as inducing a deviation from a safe flight trajectory leading to safety incidents, by exploiting vulnerabilities in the ATN-B1-based CPDLC communication stack.

We assume that the aircraft under attack is equipped with a standard-compliant ATN-B1 CPDLC system operating over VDL2,[1] and the flight crew is trained to interact with ATC using data link instructions. The system adheres to current operational procedures and maintains uplink and downlink exchanges in accordance with ICAO-defined message sets.

The attacker is assumed to have a fixed ground location from which they can transmit and receive VHF-band communications aimed at the victim aircraft. From a technical standpoint, the adversary is a skilled individual or group with deep protocol knowledge, including the capability to reverse engineer and manipulate the ATN/OSI stack and CPDLC message formats. The adversary is capable of leveraging affordable and widely available Commercial Off-The-Shelf equipment SDRs (e.g., a HackRF at $300), a basic VHF antenna ($50), RF amplifiers (e.g., 50W at $100), and commodity computing hardware within a total budget of the order of less than $1000.

Based on capabilities and intent, we identify three primary threat actors: competent individuals, non-state groups, and nation states. Competent individuals are skilled attackers acting independently, often motivated by ideology, curiosity, or a desire to expose systemic weaknesses. Non-state groups, such as hacktivists or organized collectives, may pursue broader agendas, aiming to disrupt aviation operations, provoke political response, or instill fear and broadcast extremist ideologies. Nation states may be interested in compromising the stability or safety of another country, especially in the current geopolitical climate. Attacking civilian (and some military) aviation infrastructure is a known certain way to achieve these goals.

4.2 Challenges

Although the ATN / OSI protocol stack is documented at a theoretical level in ICAO standards (available at a cost), real-world implementations, particularly those involving CPDLC over ATN-B1, remain largely proprietary, fragmented and opaque. To the best of our knowledge, there exists no demonstration of a successful, fully functional SDR framework capable of establishing and maintaining a multi-layer session with production avionics hardware, let alone exploiting it under adversarial conditions. This work fills that gap by introducing a custom SDR suite capable of arbitrary packet injection and full-stack emulation across all protocol layers. Several factors rendered our effort in creating such an attack non-trivial.

Undocumented Black-Box Systems

First, the lack of publicly available implementation details required extensive reverse engineering, using black-box testing to uncover protocol behavior, timing expectations, and error-handling logic. Each layer, from physical to application, features different types of undocumented synchronization constraints and opaque negotiation steps. The stack layers involve nuanced, undocumented, state machines, compressed headers, embedded sub-protocols, negotiations, and complex implementation, which had to be replicated precisely to avoid early termination by avionics software.

Integrity Mechanisms

Second, and more critically, the integrity mechanisms of Protected Mode CPDLC (PM-CPDLC, Sec. 10.5) and ATN checksum (Sec. 10.3) introduce protocol-level obscurity. The PM-CPDLC checksum computation depends on session parameters, yet the used algorithm is not documented (only an

[1] Currently, over 85% of all commercial flights in European airspace alone, or more than 600,000 flights just in June 2024 [12].

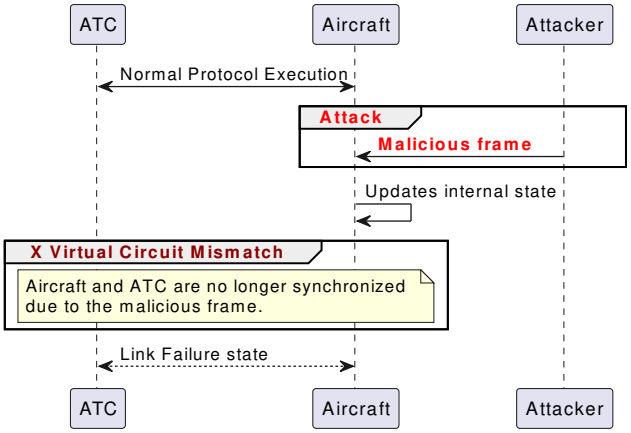


Figure 3: Generic DoS method targeting the aircraft. Injecting an unexpected malicious spoofed frame severs the connection.



Figure 4: Successful DoS recommending Voice usage.



Figure 5: Successful DoS – No service

earlier, different version is). Meanwhile, the ATN checksum, absent from COTP standards documents, requires accurate extraction of the NSAP addresses from the ES-IS exchange. Successfully sustaining a valid CPDLC connection thus required iterative emulation, contextual and dynamic parameter discovery, and reverse engineering of proprietary logic, all under tight timing constraints enforced by the protocol stack.

Timing and Synchronization Requirements

Lastly, maintaining stable and persistent interactions across all layers over extended periods is challenging. Unlike eavesdropping or one-shot broadcast injection of much simpler stateless aviation protocols [2], our requirement was to maintain a fully interactive ATN session, where the aircraft continuously accepted, processed, and responded to our input while resisting natural timeout and reauthentication behaviors. Achieving this in real time on COTS SDR hardware required a finely tuned software pipeline, timing control, and precise handling of state transitions within the ATN stack.

5 Practical Attacks on CPDLC

To our knowledge, the attacks presented in this work are the first to demonstrate practical wireless exploitation of the ATN-B1 CPDLC stack. Although previous research has explored theoretical vulnerabilities in aeronautical communications, our work is the first to operationalize attacks through full-stack emulation and adversarial interaction with production avionics under realistic conditions. These attacks target protocol-layer assumptions and implementation-specific behaviors across all the OSI stack, revealing systemic weaknesses not previously demonstrated in practice.

In particular, we show how an attacker can reliably desynchronize protocol state machines, disrupt virtual circuits, and emulate a fully functional rogue ground station capable of completing the multi-layer ATN/OSI handshake and establishing a CPDLC session with the aircraft. This represents a substantial escalation in capability compared to prior work and reveals critical gaps in the resilience of aviation communication systems. Our findings highlight the urgent need for hardening within the ATN-B1 operational architecture.

5.1 Denial of Service

First, we focus on DoS attacks at the protocol level, as opposed to traditional jamming, which simply involves saturating the frequency band, a well-studied approach in the literature (e.g., [40] in the aviation context). Protocol-level DoS attacks, on the contrary, exploit specific behaviors within the protocol stack to induce failure states without overwhelming the physical medium, making them stealthy and sustainable.

As illustrated in Figure 3, these attacks begin with the injection of a malicious frame, resulting in a state mismatch between the aircraft and the ATC. Depending on the crafted payload and the target, this forces the affected layers into a disconnect or timeout state, prompting a session teardown on the target layer and reestablishment, ultimately resulting in a link failure. After repeated cycles of teardown and reattempt, the entire connection eventually times out, requiring the pilot to manually reinitiate a Logon Request to the ATC.

If retries fail, the avionics system advises the pilot to “contact ATC by voice” (see Figure 4) and label the associated ATC facility with a “No service” status (see Figure 5), effectively achieving DoS without the need for RF jamming.

In the following sections, we outline several types of malicious frames that can be used to reliably trigger this behavior and analyze their potential for targeted protocol-level DoS. Finally, we note that these DoS attacks are equally effective against legitimate ATC ground stations, underscoring their high severity and protocol-level generality. Their ability to arbitrarily disrupt sessions regardless of the target highlights a critical vulnerability in the ATN-B1 communication stack.

DST ADDR (4 B)	SRC ADDR (4 B)	LCF 0x97 (1 B)	LCF AC (1 B)	LCF GS (1 B)	0x8 (1 B)	FCS (2 B)

Figure 6: Malicious AVLC U FRMR structure

5.1.1 Malicious AVLC Frame Reject (FRMR) Injection

The FRMR response reports a protocol error when a received frame is unacceptable. It includes a copy of the rejected control field, current sequence numbers, and specific error flags identifying issues such as unknown frame types, oversized fields, or invalid sequence numbers. We use this error handling mechanism for a DoS attack by injecting the AVLC FRMR shown in Figure 6 into the protocol execution (Figure 7).

The target frame's control link is referenced within the malicious AVLC FRMR, prompting the aircraft to respond with an AVLC UA (Unnumbered Acknowledgment). This response in turn triggers an AVLC Frame Reject (FRMR) from the ATC system. The FRMR response forces the affected layer into a disconnect or timeout state, prompting a session teardown on the target layer and reestablishment. We find that several types of frames can be exploited in this manner, particularly those involved in connection establishment or in sub-protocols that rely on timeouts and inactivity timers.

First, targeting COTP's Connect Request/Confirm and Acknowledgment frames induces a disconnect request due to a protocol error from the ATC, causing the transport layer to abort the session. Second, interfering with IDRP (Inter-Domain Routing Protocol) exchanges (Open/Update/KeepAlive) can push its finite state machine (FSM) into its "Closed" state, effectively severing the routing association between the aircraft and ground systems. Third, the X.25 Receive Ready (X.25 RR) frame is a supervisory frame used in the LAPB (Link Access Procedure, Balanced) layer of the X.25 protocol. It is used to signal that the receiver is ready to accept additional data and to transmit the expected sequence number through the N(R) field. Although X.25 RR frames do not carry payload data, they are critical for maintaining reliable data flow and session liveliness. Because they are exchanged frequently across all layers and subprotocols, X.25 RR frames represent an ideal target for persistent and protocol-agnostic DoS.

5.1.2 Broadcast DoS

One particularly effective and low-complexity attack targets the VDL Mode 2 link management procedures by exploiting the behavior of the Datalink Entity (DLE) and its coordination with the Link Management Entity (LME), both modeled as FSM (see Appendix Section 10.2). In standard operation, each VDL management instance instantiates a DLE under the control of its corresponding LME. Upon receiving an AVLC Unnumbered Disconnect (U DISC) frame, the DLE

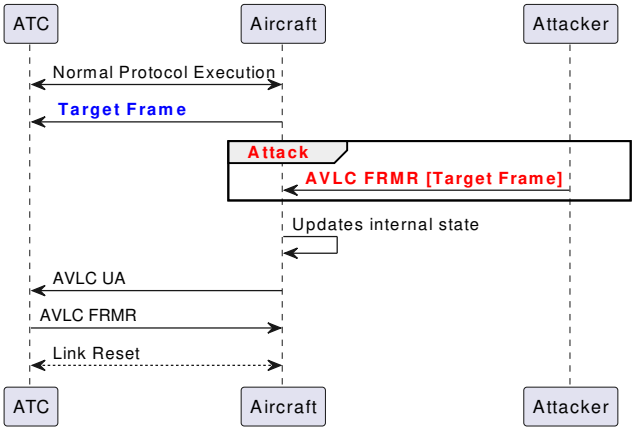


Figure 7: AVLC FRMR injection targeting the aircraft.

transitions to the Asynchronous Disconnected Mode (ADM) and notifies the LME, which enters the Link Unavailable state.

Crucially, if the AVLC U DISC is transmitted using the broadcast ICAO address 0xFFFFFF, **all aircraft currently associated with the spoofed sender address will disconnect**, regardless of their current status.

This mechanism enables a universal and immediate DoS of all dependent communication links, forcing affected aircraft to reinitialize the entire ATN stack from the physical layer up. The result is a full reset of the communication stack, requiring aircraft to restart the entire ATN session from the GSIF acquisition stage onward (ie. wait for periodic broadcast from ATC). This technique is broadly applicable, requires no interaction, and offers a reliable, low-effort denial-of-service vector against all reachable aircraft sharing the same ground station identity. Since the AVLC U DISC is a stateless frame, as shown in Figure 8, the attacker can repeat this disruption indefinitely, maintaining continuous DoS of sessions effortlessly with single packets.

DST addr (4 B)	SRC addr (4 B)	LCF=0x43 (1 B)	FCS (2 B)

Figure 8: AVLC U DISC structure

5.1.3 Control Flow Injection

We outline two complementary techniques for triggering DoS conditions by injecting valid but malicious protocol frames, hijacking the control flow. Both approaches exploit weaknesses in flow control and session management, and lead to protocol teardown, link resets, or full session reestablishment.

1. **Incrementing the AVLC I / X.25 Data Sender Sequence:** This method targets the AVLC/X.25 layers by injecting control flow frames, such as X.25 Receive

Ready (RR) or ES-IS Hello PDUs, which carry a correct payload but result in incrementing the AVLC I / X.25 sender sequence number. When the aircraft receives these frames, it updates its expected sequence state accordingly. This causes subsequent legitimate ATC transmissions to appear out of sync, causing a protocol violation leading to a link reset, then clear, in addition to a FRMR from the ATC.

2. **Disrupting the Virtual Circuit:** This method interferes higher in the stack with session management via well-formed teardown or reset frames. Examples include:

   (a) X.25 Reset Request: resets to zero the sender and receiver sequence numbers.

   (b) X.25 Clear Request: tears down the virtual circuit.

   (c) COTP Disconnect Request: aborts the transport-layer connection;

   (d) IDRP CEASE PDU: transitions the IDRP FSM into "CLOSED" state.

   These frames exploit the protocol's own mechanisms to negotiate connections parameters, trigger recovery procedures or fatal state transitions.

   The result is an FRMR from ATC, which cascades into a link reset or session teardown. Since this desynchronization propagates upward through the stack, the entire communication channel requires full re-establishment.

Despite its precision, Control Flow DoS requires carefully timed injections between legitimate exchanges, sequence numbers tracking, and fast parameter extraction and prediction, making this method less reliable to execute.

5.1.4 Malformed Frame Injection

Malformed frames can affect different protocol layers. At the AVLC/X.25 layers, injecting frames with incorrect sequence numbers reliably triggers protocol errors. At higher layers, malformed frames must be crafted with the correct link state. While lower-layer manipulation is always effective, higher-layer behavior depends on negotiated CLNP parameters, such as the Error Report flag, and the selected COTP protocol class. If CLNP Error Report is set, frames with invalid header fields, such as incorrect local reference numbers or PDU identifiers, trigger explicit error reports from the aircraft in addition to a link reset. Alternatively, malformed COTP or IDRP messages that bypass error reporting, such as invalid user data fields like an all-zero ATN checksum, are implicitly rejected, eliciting an X.25 RR and again causing a link state mismatch and reset. As with earlier methods, this approach still requires careful tracking of sequence numbers and suffers from reliability issues due to timing sensitivity and limited impact, making the previous methods in Sections 5.1.1 and 5.1.2 easier to execute.

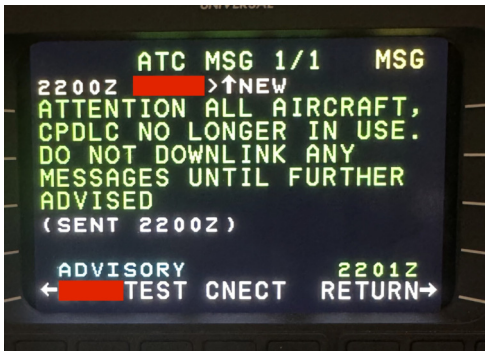


Figure 9: Rogue station transmission example.

5.2 Rogue Ground Station / Evil Twin

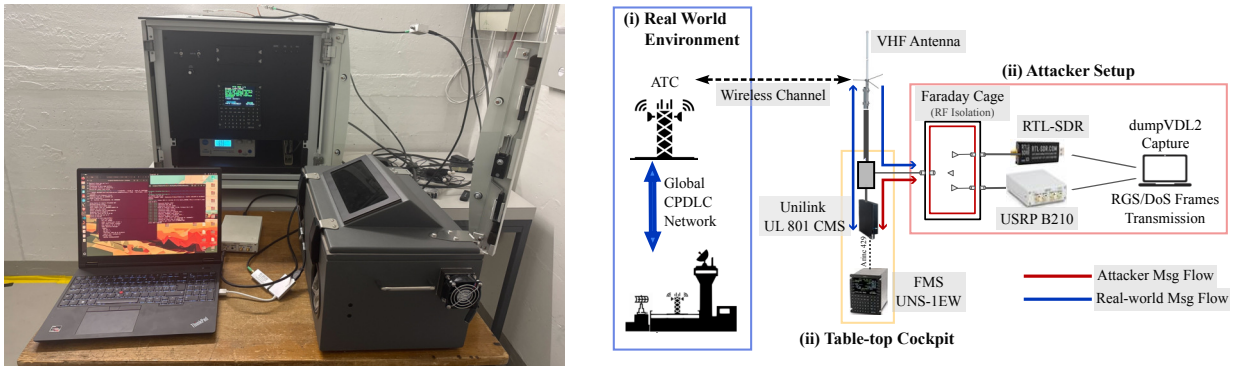
We leverage `cpdlc-gs` to implement a Rogue Ground Station (RGS) capable of issuing valid CPDLC messages to certified avionics hardware similar to a mobile phone network IMSI catcher. The RGS operates as a FSM, sequentially completing each layer's connection procedure across the ATN stack and keeping state indefinitely, closely following Figure 2.

The process begins with the broadcast of a Ground Station Information Frame (GSIF), advertising VDLM2 operation with D8PSK modulation at 136.975 MHz. Accompanying this broadcast is a series of AVLC U frames used to negotiate key link-layer parameters. Establishing a valid link-layer presence requires operational implementations of both AVLC and X.25, including support for various packet types and ACARS payload encapsulation. We then engage the ES-IS (End System to Intermediate System) subprotocol, encapsulated within X.25 Call Request and Call Accepted packets. During this exchange, NSAP addresses are inferred from DTE addresses, and further negotiation occurs on compression schemes, window sizes, and traffic class permissions.

Using the resolved NSAP, we proceed to initiate an IDRP session at the network layer. As this represents an End System to Boundary Intermediate System (ES-BIS) connection, the simple checksum authentication method is selected. Since our RGS does not route beyond itself, it simply emulates sufficient routing behavior by offering enough credits and keeping the aircraft's IDRP FSM in the ACCEPT state.

Following this, the RGS establishes a transport connection using COTP. TSAPs are exchanged and parameters negotiated, with COTP messages encapsulated in compressed CLNP frames that include a mandatory ATN checksum. We select Protocol Class 4 (Error Detection and Recovery), which offers the most robust features among the five defined classes.

Upon completing the transport connection, the session layer is used to receive the aircraft's CPDLC Logon Request, issued by the Context Management (CM) application. This message specifies the aircraft's CALLSIGN and departure/arrival airports. We respond with appropriate context parameters, including derivation of the PM-CPDLC checksum parameters.



(a) (b)

Figure 10: (a) Photo and (b) Schematic of the attack and evaluation setup. (i) Real-world environment including a test ground station managed by local aviation authority, (ii) a table-top cockpit includes type certified avionics and (iii) attacker setup including SDRs for RX/TX of *real* CPDLC messages.

Once the CPDLC session is established, the RGS asserts itself as the current data authority and proceeds to transmit its uplink messages to the aircraft, exemplified in Figure 9, effectively masquerading as legitimate ground station.

6 Building a Live Real-World Commercial Aircraft CPDLC Environment

6.1 From Concept to Deployment

Our test and evaluation test bed emerged from a multi-year effort to reproduce operational CPDLC in a safe but realistic environment in order to bring prior theoretical research on postulated security vulnerabilities into the real world. Working together with Skyguide, the Swiss Air Navigation Service Provider (ANSP), and EUROCONTROL, a European supranational aviation institution running a CPDLC backend available for aircraft testing [9], we installed a VHF data-link antenna and a GPS antenna on the roof of ETH Zurich, securing line-of-sight radio coverage to the Skyguide's surveillance site overseeing Zurich Kloten airport.

Installing certified hardware and connecting to the operational CPDLC network over the air (albeit to a test ground station) required regulatory coordination with all entities and appropriate safety testing. Multiple debugging rounds, covering firmware updates, operator clearances, time synchronization, and protocol trace analysis were necessary before the avionics stack completed a first CPDLC log-on with the operator's ground station. Inspired by various previous avionics lab setups from the literature [3, 51], we repurposed authentic and type-certified flight hardware for research, ultimately investing in more than $200,000 worth of flightworthy avionics components. The result is a unique bench-top "aircraft" that can exchange CPDLC messages wirelessly over the real VDL 2 network just as a pilot would while remaining safely and comfortably inside the laboratory.

6.2 Laboratory Configuration

Figure 10a shows a photograph of the hardware setup, while Figure 10b shows the full system layout. We first describe the avionics line-replaceable units (LRUs).

UNS-1Ew FMS. In service, the UNS-1Ew is the aircraft's primary *flight management system*. Its GPS receiver supplies position, velocity, and time which is merged with a worldwide navigation database for navigation. The color 5-inch Control Display Unit lets crew enter flight plans, check performance predictions, tune radios, and view, acknowledge, and respond to CPDLC messages. When coupled to an autopilot, the UNS-1Ew can drive lateral and vertical navigation modes all the way from take-off through precision-approach guidance. It also acts as the human–machine interface for FANS 1/A+ and ATN B1 CPDLC, automatically routing message traffic to the CMU while displaying clearances.

UniLink UL-801 CMU. The UniLink UL-801 is the *communications management unit* that handles all air–ground datalink. It contains a VDL2 transceiver and a optional Iridium SatCom unit, allowing seamless switchover between VHF and satellite channels. The UL-801 supports ACARS, FANS 1/A+, ADS-C, and ATN B1 sessions: it performs protocol framing, security checks, and network management, and it multiplexes messages between the cockpit (FMS), airline operations centers, and ATC facilities. The unit can simultaneously maintain multiple logical connections across these entities and links. Flight crews rarely interact with the UL-801 directly; instead, they see its status through the FMS, which issues logon requests, displays incoming ATC instructions, and records acknowledgements. In an aircraft, the UL-801 is typically installed in an avionics bay, with only its built-in test status shown to pilots.

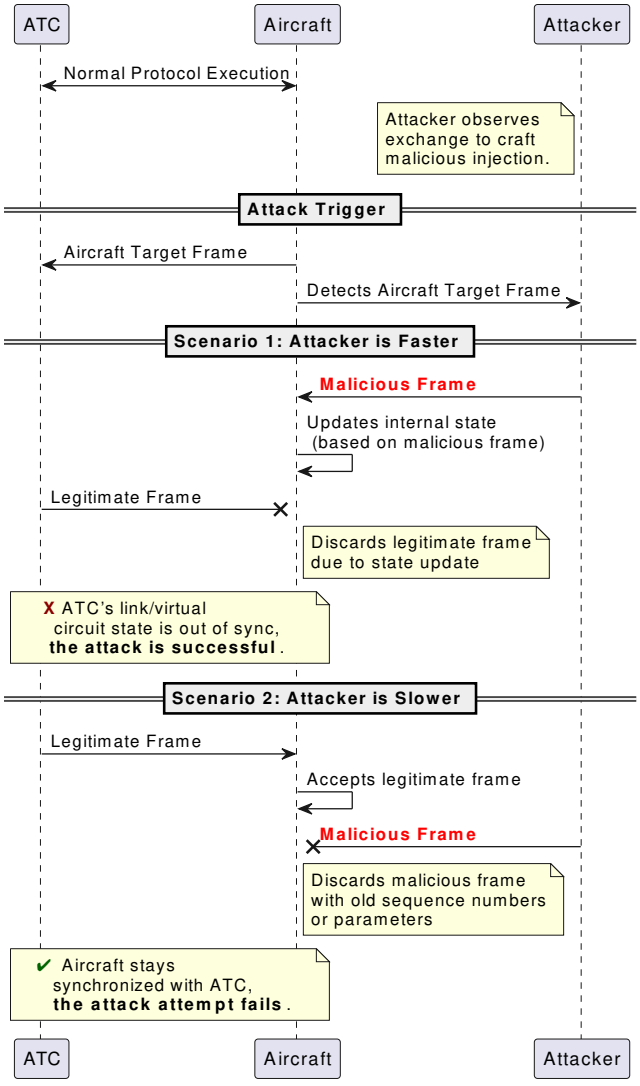


Figure 11: Race condition for state-based DoS methods, the attacker must reach the aircraft faster than the ground station.

Peripherals Two high-speed ARINC 429 channels link the FMS and CMU; additional RS-422 ports support maintenance and configuration. We do not exploit any direct databus access in our work but remain exclusively on the RF interface. A GPS antenna feeds the FMS position and time synchronization, while a VHF antenna on the building rooftop connects to the CMU. All LRUs operate from a 28V DC supply. Control of the unit is handled only via the FMS display and interface.

Certifiability With fully type-certified components, our setup has the timing, alerting, wireless communication, and session management of an in-service aircraft CPDLC installation. This fidelity lets us observe real avionics behavior under authentic over-the-air conditions. This authenticity is an essential foundation for the credibility of the attacks testing in the next section. Previous attacks shown in theory or simulations only have not convinced aviation stakeholders to take action in many cases [33]. We crucially note that our testbed is only an example instance: the vulnerabilities presented are not exclusive to any manufacturer, airline, or ANSP but inherent to the standard.

6.3 Attack Evaluation Test Setup

Figure 10b shows the test setup, divided into normal air-ground operations and the attacker, plus a monitoring loop.

Live Aircraft Ground Setup To verify correct real-world functioning of our avionics setup, we connect via the VHF antenna over the air to a VDL2 ground station in approx. 11.5 km distance. Skyguide allowlisted the 24-bit transponder ID in order for us to connect to the ATN ground network.[2] The network then routes our messages to EUROCONTROL's automated ground testing backend, which we select via debug functions in the FMS.

Attack Setup and Monitoring Loop For the attack setup, we chose the maximum realism while adhering to all safety requirements. The UniLink's wireless interface was split, and routed into a Faraday cage to a second VHF antenna. Here, all wireless signals within the whole loop were constantly monitored by an RTL-SDR using dumpvdl2 [31] to create logs for reverse engineering and analysis. Any attack traffic for both DoS and RGS was injected over the air using an Ettus USRP B210 and routed exclusively to the UniLink FMS, with no leakage to the outside world possible.

7 Evaluation

We now evaluate the attacks described in Section 5.

7.1 DoS Attacks on CPDLC

We test all DoS attacks by establishing a standard connection to the legitimate automated ground test station first, which is then disrupted by injecting DoS frames to the UniLink FMS. No tests were conducted on legitimate ground stations, as we could not guarantee zero leakage to unaffected parties.

7.1.1 Race Conditions

State-dependent DoS methods (Sections 5.1.1, 5.1.3, and 5.1.4) are subject to race conditions due to the protocol's state update procedures. As shown in Figure 11, upon transmission of a frame by the aircraft, both legitimate ATC entity and attacker can respond. The attacker, having observed the

[2] A malicious actor could simply use the ID of any existing CPDLC-equipped aircraft to circumvent this allowlist.

Table 3: Summary of novel DoS attacks on CPDLC with their characteristics.

Attack	Broadcast	State Dependence	Timing Sensitivity	Impact
AVLC FRMR Injection (5.1.1)	No	Moderate – must track link layer sequence numbers and link-layer state	Moderate – must preempt ATC frames but low overhead and compact frames	Moderate – depends on accurate tracking & fast transmission
AVLC U DISC (5.1.2)	Yes	Low – stateless	Low – not subject to race conditions	High – deterministic & reliable
Control Flow Injection (5.1.3)	No	High – higher-layer state variables	High – narrow timing windows	Low – operationally fragile
Malformed Payload Injection (5.1.4)	No	High – higher-layer protocol state	High – tight injection timing	Lower – more illustrative

aircraft's transmission, forges a response with valid sequence numbers and parameters. If this forged frame arrives prior to the legitimate ATC response, the aircraft updates its internal state based on the attacker's input and rejects the subsequent ATC frame. However, if the ATC response is first received, the aircraft state progresses along the legitimate path and the attacker's later injection is discarded. The feasibility of the attack is therefore contingent on the adversary's ability to preempt the ATC's response in time, which in practice depends on factors such as propagation delay, processing latency, and the attacker's relative proximity to the aircraft compared to ATC. Here, the basic model is not different from existing wireless attacks on aviation discussed in prior work [40].

In contrast to timing-sensitive injections, the AVLC U DISC–based teardown (Section 5.1.2) is state-independent and not subject to race conditions. Because the frame is defined as a stateless primitive, its processing is unconditional: upon receipt, the DLE immediately transitions to the Asynchronous Disconnected Mode (see Figure 14, Appendix) and propagates this event to the LME. The LME then transitions to the Link Unavailable state (see Figure 13, Appendix), resulting in a link teardown irrespective of any concurrent or pending protocol exchanges. The attack works because of the priority given to AVLC U DISC processing in the DLE and LME FSMs, making it deterministic and reliable. Our test system disconnects, no matter which transponder address is set, confirming the broadcast character of the attack.

7.1.2 Impact

The DoS attack can instantaneously sever ATN B1 data links (notably CPDLC) between multiple aircraft and their controlling ATC, forcing an abrupt and unplanned reversion to voice communications. In high-density terminal sectors, where voice channels are already saturated, degraded, or completely unavailable, this sudden loss of data link can overwhelm controller capacity within minutes, halt or stop the timely delivery of clearances, and in some cases eliminate ATC contact altogether. When executed strategically, the attack can sustain a sector-wide data link blackout, trapping pilots and controllers in a degraded operational mode for hours. During critical flight phases such as climb, descent, or active conflict resolution, the loss of CPDLC not only delays but can completely prevent the exchange of life-preserving instructions, collapsing the safety margins that modern CPDLC procedures depend upon and leaving flight crews to manage separation with minimal support under rapidly deteriorating conditions, in the worst case relying on the equally insecure collision avoidance systems as a last line of defense [32].

7.2 Rogue Ground Stations

We use `cpdlc-gs` to set up a RGS and takeover the connection from the legitimate ground station. Once a RGS completes the ATN/OSI handshake and establishes a CPDLC session, it gains the same operational privileges as a legitimate ATC, enabling it to issue uplinks indistinguishable from authentic clearances. Because these messages are fully compliant and originate from a seemingly valid ATN peer, flight crews are likely to action them without hesitation, particularly in high workload phases or sectors with limited VHF voice coverage. We identify the following plausible high-impact scenarios:

- **Lateral Deviation:** The RGS issues a `UM79 PROCEED DIRECT` message, diverting the aircraft toward a waypoint that places it in an active holding stack, into a conflicting arrival stream, or inside restricted airspace. The instruction appears operationally reasonable yet forces a trajectory that compromises separation and creates incidents as described by the FAA [15].
- **Altitude Deviation:** A `UM21 CLIMB TO` or `UM20 DESCEND TO` clearance directs the aircraft to an altitude already assigned to another aircraft in the sector. Believing the clearance is valid, the crew initiates the maneuver, potentially triggering an imminent loss of separation and emergency TCAS advisories at the right timing.
- **Malicious Step-Descent:** In procedural, non-radar-controlled airspace, the RGS transmits a step descent clearance supposedly for fuel efficiency. In reality, it

places the aircraft in adverse weather, turbulence, or opposite direction traffic, where the absence of radar makes conflict detection slower and less reliable.

- **Terminal Phase Manipulation** – During approach, a `UM80 CLEARED VIA` instruction changes the approach procedure to one incompatible with current traffic flow, forcing rushed cockpit reconfigurations and increasing runway occupancy conflicts.
- **Descent Initiation in Terminal Area:** The RGS instructs an early descent into an approach path without clearance, increasing collision risk with aircraft on the final approach or in conflict with the departure flows.
- **Speed Adjustments:** A false `MAINTAIN [speed]` instruction slows an aircraft within a high-density arrival stream, compressing in-trail spacing and risking separation breaches.
- **Emergency Diversion:** A fabricated `DIVERT TO [alternate airport]` clearance, framed as a response to weather or traffic congestion, causes significant operational disruption and forces the crew into complex in-flight decision-making.
- **Contradictory Clearance:** The RGS issues a `UM169` free-text instruction that conflicts with an existing ATC clearance (e.g., "CHANGE ROUTE IMMEDIATELY"), creating confusion in the cockpit and increasing the likelihood of human error or miscommunication [16].
- **Trust Erosion:** A fabricated `UM169` free-text indicating a fabricated emergency (e.g., 9/11 type) or fuel/performance alert, forcing the crew to execute emergency checklists, coordinate with ATC, and possibly divert. The attackers creativity to undermine the trust in the system is practically unlimited.

In each case, the malicious uplink exploits the inherent trust placed in CPDLC (confirmed by surveys [7, 46, 49] and conversations with commercial pilots and controllers during disclosure) and the operational assumption that any (seemingly) authenticated ground peer is legitimate. The danger lies not only in the immediacy of the unsafe maneuver but also in the ability to interleave false instructions with genuine ATC traffic, delaying detection and increasing the likelihood of compliance until the operational damage is already underway.

7.3 Real-World Attack Constraints

7.3.1 RGS Positioning

While no race conditions apply to the RGS attack in a strict sense, one constraint stems from the spatial and radio-frequency relationship between the RGS, the targeted aircraft, and the legitimate ground station impersonated. For the RGS to operate without interference, both the RGS and the aircraft must be positioned far enough from the legitimate ground station so that the transmissions are undetected. If the legitimate station remains within effective range, it may respond to each packet with an AVLC U FRMR. Unlike the DoS strategy outlined in Section 5.1.1, this will not cause our carefully crafted RGS to reset the link as a legitimate ground station would, but the anomaly could theoretically be detected at the level of the legitimate station. Only if stealth and detection are a concern, reactive jamming or message deletion as discussed by Schaefer et al. [40] would become a necessary consideration.

7.3.2 Redundancy as Constraints on RGS

ATC safety relies on multiple, independent, human-in-the-loop layers, affecting the impact of a RGS. Without claim of completeness, we discuss relevant scenarios and how they apply to CPDLC attacks.

- **Radar Surveillance and Safety Net Systems**
  Primary/secondary radar (SSR) and ADS-B feed ATC services such as Short-Term Conflict Alert, Minimum Safe Altitude Warning, and Approach Path Monitoring. While independent of CPDLC, SSR and ADS-B have been proven susceptible to spoofing and DoS, allowing a coordinated attacker to potentially distort surveillance inputs and weaken these safety nets [40, 43].
- **Voice Communication (VHF/121.5 MHz)**
  VHF is the primary fallback, and also vulnerable to spoofing and jamming. A malicious CPDLC uplink can redirect crews to attacker-controlled frequencies, effectively isolating the aircraft from the real controller, e.g. denying the standard 121.5 MHz frequency. Such coordinated disruption could at least delay ATC detection and enable execution of rogue clearances.
- **Traffic Collision Avoidance System (TCAS)**
  TCAS provides collision avoidance through active interrogation of nearby aircraft transponders and issuing Traffic and Resolution Advisories, operating independently of CPDLC and ground systems. Although TCAS principally mitigates catastrophic separation loss caused by CPDLC spoofing as a last line of defense, recent work [32] proves it vulnerable to spoofing and DoS.

Beyond safety, the *detection* of a RGS by ATC depends on whether the attack occurs as a takeover (the RGS severs the existing link), or as a standalone RGS. With the latter, detection hinges on how CPDLC usage is expected or enforced in that specific airspace. Critically, the execution window before detection is defined by ATC reaction time, degradation of the redundancy layers, and crew recognition of inconsistencies. This impact is difficult to define and generalize theoretically, but by delaying detection across *all* vulnerable layers, an attacker may successfully achieve operational disruption.

7.3.3 Power Budget

For all CPDLC attacks, we calculate the necessary power budget as theoretical estimates intended to illustrate conceptual feasibility. For safety and legal reasons these are not validated through empirical over-the-air measurements. We assume free-space propagation with path loss

$$L_{\mathrm{FS,dB}} = 32.44 + 20\log_{10}(d_{\mathrm{km}}) + 20\log_{10}(f_{\mathrm{MHz}}),$$

where d_{km} is the distance in kilometers and f_{MHz} is the frequency in megahertz. The avionics VHF receiver sensitivity is $S_{\min} = -93$ dBm [20]. Successful reception thus requires

$$P_t + G_t + G_r - L_{\mathrm{sys}} - L_{\mathrm{FS,dB}} \geq S_{\min} + M,$$

where P_t is the attacker transmit power (in dBm), G_t and G_r are the antenna gains at the transmitter and receiver (in dBi), L_{sys} accounts for system losses (in dB), and M is the desired link margin, which acts as a safety buffer (in dB).

For $f = 137\,\mathrm{MHz}$, $M = 10\,\mathrm{dB}$, aircraft antenna gain $G_r = 0$ dBi, and typical attacker parameters $P_t = 44\,\mathrm{dBm}$ (25 W), $G_t = 6\,\mathrm{dBi}$, and $L_{\mathrm{sys}} = 2\,\mathrm{dB}$, the free-space range is $d_{\max} \approx 1{,}380\,\mathrm{km}$. Thus, only the VHF line-of-sight to an aircraft at 36,000 ft altitude from a 10 m mast limits the attack range to roughly 380 km. At this distance, the required transmit power is only $\sim 40\,\mathrm{dBm}$ (9–10 W), so even a 25 W transmitter provides a comfortable buffer. Even with a 0 dBi transmit antenna and 4–6 dB of losses, 25 W still supports approximately 280–350 km with a 10 dB link margin.. The reception of messages from aircraft is similarly easy with up to 300 km range reported by Smailes et al. [42] on cheap equipment.

8 Discussion

8.1 Limitations

The RGS (Section 5.2) is implemented as a FSM specifically tailored for maintaining a single ATN-B1 CPDLC connection with one aircraft at a time. While this architecture simplifies state management and enables the development effort to focus on reverse engineering the protocol stack, it does not inherently scale to scenarios involving multiple concurrent aircraft connections. Supporting multiple sessions with this design would require instantiating FSMs for each aircraft. In a naïve sequential processing model, packets are dispatched to each FSM in turn; as the number of active aircraft grows, cumulative latency can become non-trivial, raising the likelihood of timeouts given the multiple timing sensitivities of many protocol layers. Consequently, concurrency models, such as multithreading, multiprocessing, or event-driven asynchronous handling, would be necessary, for example. With the protocol stack now fully reverse engineered, however, more efficient and purpose-built approaches could be designed to overcome these scalability constraints. However, this was out of scope for our proof of concept.

Moreover, one of the most critical integrity scenarios concerns oceanic CPDLC communications. These rely on satellite channels external to the analysed ATN-B1 infrastructure and are therefore outside the scope of this paper. Finally, for anyone to independently, safely, and legally reproduce this work, it is necessary to partner with aviation authorities to conduct any similar effort. We note that our own system will remain operational for demonstration for the foreseeable future, and we welcome collaboration or testing opportunities with other countries and ANSPs.

8.2 Root Cause: Aviation Design Philosophy

The absence of cryptographic authentication in aviation communications is rooted in the sector's design philosophy. Historically, the focus has been on safety, interoperability, and long-term reliability rather than security. Aviation systems follow extremely long development, certification, and testing cycles, which enable the continued use of legacy protocols to ensure backward compatibility across diverse stakeholders, including OEMs, aircraft manufacturers, ANSPs. This emphasis on compatibility makes the introduction of disruptive technologies such as public-key infrastructures (PKI) challenging, despite their technical feasibility, even without considering the geopolitical difficulty of such an infrastructure. Furthermore, aviation communications were historically considered difficult to attack due to the complexity and cost of the technology, leading to a form of "security through obscurity."

8.3 Mitigations and Countermeasures

8.3.1 Aviation Datalink Standards Development

Early concerns about the security of datalink services, inlcuding CPDLC, have led to two standards proposals. The Secure Dialogue Service (SDS) emerged first, Early concepts were built in the 2010s, culminating in the inclusion of SDS in ICAO Doc 9896 (ATN/IPS SARPs) and related guidance material [21]. SDS defines cryptographic mechanisms for securing ATN over IP-based networks, ensuring authentication, integrity, and confidentiality in air–ground communications without fundamentally altering CPDLC message semantics [21]. Public minutes indicate SDS has been dropped in favour of Datagram Transport Layer Security (DTLS).

DTLS, the datagram-oriented variant of TLS, provides end-to-end security over unreliable transport layers like UDP [37]. DTLS is referenced in ICAO discussions for securing ATN/IPS services in recent years, including CPDLC over IP, due to its ability to offer mutual authentication and replay protection in a connectionless environment [19]. While DTLS has seen deployment in Internet protocols, its aviation adoption remains at a conceptual and prototype stage [19]. Hence, it is not currently possible to say whether all discovered vulnerabilities in this paper would be mitigated by DTLS but we hope to inform the ongoing work with this study.

According to the ICAO Global Air Navigation Plan, initial operational trials of DTLS are expected not before the early 2030s [22]. This timeline aligns with previous CNS/ATM rollouts, where initial operational deployments typically lag standard finalization by a decade or more. Boeing and Airbus mention cost as a main obstacle in 2014 and projected best-case development programmes to take 9 years [1].

Internet Protocol Suite Over AVLC Following disclosure discussions with a leading aircraft manufacturer, deploying Internet Protocol Suite (ATN/IPS) [6] over AVLC (IOA) could help mitigate several security risks inherent in legacy data links. Leveraging native IPsec encryption, certificate-based authentication, and integrity protection, IPS could address all attacks targeting higher layers. Additionally, network-layer filtering and access control may prevent unauthorized or malformed traffic from reaching critical avionics systems. However, practical effectiveness and mitigation of full-stack attacks depends on implementation details, key management procedures, and practical integration with AVLC without introducing unacceptable latency or overhead. There is no timeline for the deployment of IPS over AVLC.

8.3.2 Existing CPDLC Security Research

In the academic community, there have been few proposals on securing CPDLC so far, potentially hindered by the obscurity and complexity of the aviation datalink ecosystem. Gurtov et al. [17] proposed cryptographic solutions such as HIP and ECC-based schemes to enhance CPDLC security. Strohmeier et al. [50] surveyed air–ground datalink vulnerabilities, including CPDLC, and recommended stronger authentication and integrity protections. Khan et al. [28] introduced AKAASH, an authentication and handover protocol for CPDLC, and validated it through formal and informal analysis. Beena & Sugathan [27] formally verified CPDLC-based authentication protocols (including AKAASH) using Tamarin to prove security properties under defined assumptions.

8.3.3 Physical Layer Security and Intrusion Detection

While only encryption-based authentication can provide the guarantees necessary to formally and effectively secure a datalink system such as CPDLC, basic spectrum monitoring schemes could be employed to detect malicious ground stations. These are already in use in aviation to monitor compliance of aircraft transponders, GPS interference, or channel congestion [10, 11].

Academic physical layer security research can form the basis for Intrusion Detection Systems for ATN-B1 CPDLC as analog characteristics tied to hardware and aircraft motion are difficult to forge. Strohmeier et al. demonstrate that RSS–distance consistency and antenna-specific modulation artifacts can detect aircraft spoofing in real time [47], while Danev et al. show that hardware imperfections yield stable radiometric fingerprints resistant to identity cloning [4]. Multilateration using TDoA, Doppler, RSS or beamforming further validates message origin and filters out signals violating real-world kinematics [48]. Machine learning advances strengthen these capabilities: Wang et al. extract aircraft-specific RF signatures from ADS-B even in few-shot conditions [52], and Hiles et al. present a generic RF-fingerprinting framework that generalizes across diverse domains [18]. Federated learning additionally enables collaborative IDS models without sharing sensitive CPDLC data [29]. Such monitoring could also be deployed via distributed sensor networks, as shown by Jansen et al.'s Crowd-GPS-Sec system [26]. Coupled with reactive jamming as an emergency containment mechanism [53], an IDS tailored to ATN-B1 offers a potential mitigation path that remains compatible with certified avionics.

If RGS or DoS attacks are detected, reactive jamming [53] could be employed as defense, followed by localization and neutralization of the attack.

9 Conclusion

We present the first practical, full-stack attack framework against ATN-B1 CPDLC, built on a custom SDR suite `cpdlc-gs` and validated in a live environment with certified avionics hardware. We demonstrate DoS attacks and a fully functional rogue ground station capable of issuing authentic CPDLC clearances, proving that operational exploitation is feasible with commodity hardware. Our findings invalidate the industry assumption of security-through-complexity and expose a critical gap in aviation datalink security, as cryptographic protections in new standards remain always a decade away. This demonstrates the urgent need for monitoring and an accelerated security standardization process before these weaknesses translate into real-world incidents – a risk highlighted by disclosure discussions suggests that views on CPDLC security remain divided within the industry.

Acknowledgements

We thank Miroslav Šmid, Georg Riedler and Christian Schusser from QCM AG, Isabelle Herail from EUROCONTROL, and Luc Chevalley from Skyguide for their invaluable support. We further thank Dr. Timo Warns from Airbus and First Officer Urs Hasselwander for their review of the paper.

Ethical Considerations

Stakeholders

The primary stakeholders of our research are passengers, flight crews and air traffic controllers, whose safety and work depend on the integrity, availability, and trustworthiness of

CPDLC. ANSPs and airlines are directly impacted as operators responsible for maintaining safe and continuous operations, and may face operational, financial, and reputational consequences if vulnerabilities are exploited or if mitigations require system changes. Avionics and aircraft manufacturers, as well as standards bodies such as ICAO, RTCA, and EUROCAE, are stakeholders responsible for system design, certification, and long-term evolution, and may be impacted by the need to revise assumptions, standards, or deployed systems. Regulators and oversight authorities are stakeholders tasked with balancing safety, security, and operational feasibility, and this research affects their risk models and prioritization decisions. Finally, society at large is an indirect stakeholder, as it relies on the continued safety and resilience of global aviation infrastructure and bears the consequences of systemic aviation failures.

Impacts

Ethical Principles

Our work was guided by the ethical principles articulated in the Menlo Report: Beneficence was considered by weighing the safety and security benefits of exposing and helping to fix realistic vulnerabilities against the potential harm of increased attacker awareness. Respect for Persons was addressed by avoiding experimentation on unwitting individuals, avoiding the collection of personal data, and ensuring that no pilots, controllers, or passengers were placed at risk or used as subjects during our work. Justice was considered by ensuring that the risks and benefits of the research are not unfairly concentrated on particular groups, especially marginalised ones, and that safety improvements benefit the aviation system broadly rather than only, say, a specific country. Respect for Law and Public Interest was upheld by conducting all experiments in compliance with applicable regulations, coordinating with authorities, and prioritizing aviation safety and public trust.

Harms and Mitigations

Theoretical harms from this research fall into both tangible and rights-based categories. Tangible harms could include increased risk of malicious exploitation, operational disruption, financial costs associated with mitigation, or reputational harm to aviation stakeholders. Rights-based harms could arise if individuals were unknowingly subjected to experimentation, if private communications were intercepted, or if safety was compromised without consent. In this work, no direct tangible harms occurred due to mitigations taken. Experiments were conducted exclusively in controlled environments using certified equipment, without interaction with live operational aircraft or production ATC systems. No personal data was collected, intercepted, or analyzed, and no individuals' rights to privacy or informed consent were violated. Coordinated disclosure was conducted prior to publication with relevant stakeholders, including regulators, air navigation service providers, manufacturers, airlines, pilot associations, and aviation security organizations. To mitigate misuse risk by actors not yet capable of such actions anyway, exploit code is not publicly released. The remaining potential harm is indirect and prospective: publication may lower the barrier for malicious actors by confirming feasibility. This risk is acknowledged but contextualized by the fact that the attack classes are already well known within the computer security community and possibly exploitable by capable adversaries. Finally, as is accepted for any vulnerability disclosure, reputational harms for manufacturers are possible as their products are not seen as secure. This, however, is a direct ethical benefit as large defence and aerospace manufacturers can thus be pressured into action of actually improving the system.

Decision

Some potential harms remain unmitigated, particularly the possibility that awareness may also reach malicious actors. This risk is explicitly acknowledged and weighed in our decision to publish. In contrast, from a beneficence perspective, the expected benefits are substantial: correcting long-standing false assumptions and inaction within aviation, enabling evidence-based risk assessment, and hopefully kick-starting mitigation and standardization efforts. These benefits are not hypothetical; the work has already led to active discussion within relevant working groups capable of implementing change, which was not occurring during two decades prior to this research. We explicitly considered the alternative of not publishing or delaying publication until mitigations are widely deployed, potentially many years. However, given that these vulnerabilities have been theoretically known for decades without prompting action, and given that capable adversaries plausibly already possess the necessary capabilities, withholding empirical evidence would primarily delay defensive efforts rather than reduce attacker risk. We therefore assume that the likelihood of adversary awareness is already high, while the likelihood of mitigation without compelling evidence is low. Under these assumptions, publication with responsible disclosure and harm mitigation is the more ethical path. We plan to embargo the research until August 2026, one year after our disclosure, and significantly longer than standard vulnerability disclosure recommendations. All in all, under our analysis, proceeding with the research does not infringe on the rights of any stakeholder group. Importantly, both beneficence-based and rights-based analyses lead to the same conclusion: conducting and publishing the research is ethically justified.

Ongoing Disclosure

Our coordinated disclosure to airlines, manufacturers, pilots' groups, ANSPs, and security organizations was met with

unusually constructive engagement. A major European airline noted that the findings align with long-standing industry concerns and initiated an internal risk assessment review. An airframe manufacturer emphasized involving CSPs and datalink-stack implementers and will raise the work within the RTCA/EUROCAE standard bodies to evaluate how emerging protections (e.g., IOA/IPS over AVLC) map to the demonstrated attacks. Pilots' associations welcomed the empirical confirmation of spoofability, noting that past discussions often relied on assumptions rather than evidence. The Aviation ISAC distributed the work to its Product Security Community of Interest, which includes manufacturers, ANSPs, airlines, and airports, and offered formal recognition to the authors for contributing the analysis. Overall, disclosure responses were consistently positive: stakeholders broadly accepted the risks and expressed interest in moving toward more concrete mitigations. Further talks with more stakeholders are ongoing.

Open Science

We support the principles of open science and reproducibility, and wherever possible, we make our methodology and supporting materials available. However, the exploit code itself cannot be publicly released due to the high safety impact and the inability to fully address the vulnerability in a short timeframe. Premature disclosure could endanger aircraft operations and passenger safety. Therefore, we have opted for a responsible disclosure process, working closely with aviation authorities, manufacturers, and industry partners to ensure appropriate mitigations. In this case, we strongly believe the potential harm from misuse significantly outweighs the benefits of full code release and precedent from prior critical vulnerabilities in aviation support our approach.

While the attack implementation remains restricted, we provide sanitized attack logs to enable transparency and facilitate academic verification without introducing undue risk. All shared logs are thoroughly anonymized and stripped of any operational identifiers to prevent leakage of sensitive or safety-critical information and deanonymization of the authors. The logs are available at https://doi.org/10.5281/zenodo.17964693

References

[1] Boeing & Airbus. Boeing–airbus perspective on data link security. Information Paper, ICAO ACP-WG-I-17 Meeting, July 2014. ICAO ACP Working Group I.

[2] Andrei Costin and Aurélien Francillon. Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *Black Hat USA*, 2012.

[3] Sam Crow, Brown Farinholt, Brian Johannesmeyer, Karl Koscher, Stephen Checkoway, Stefan Savage, Aaron Schulman, Alex C Snoeren, and Kirill Levchenko. Triton: A software-reconfigurable federated avionics testbed. In *12th USENIX Workshop on Cyber Security Experimentation and Test (CSET 19)*, 2019.

[4] Boris Danev, Davide Zanetti, and Srdjan Capkun. On physical-layer identification of wireless devices. *ACM Comput. Surv.*, 45(1), December 2012.

[5] Doris Di Marco, Alessandro Manzo, Marco Ivaldi, and John Hird. Security testing with controller-pilot data link communications. In *11th Int Conference on Availability, Reliability and Security (ARES)*, pages 526–531, 2016.

[6] European Union Aviation Safety Agency (EASA). EUROCAE Study: ATN/OSI and ATN/IPS Comparison. Technical Report FC19 SC.003, EASA, 2016.

[7] Eric Ekström. Cybersecurity Challenges to Airlines - A Literature Review of Risk & Compliance. Master's thesis, Lund University, 2025.

[8] Sofie Eskilsson, Hanna Gustafsson, Suleman Khan, and Andrei Gurtov. Demonstrating ADS-B and CPDLC attacks with software-defined radio. In *Integrated Comm., Navigation and Surveillance Conf. (ICNS)*, 2020.

[9] EUROCONTROL. Controller-pilot datalink communications ground automated tool (CPDLC GAT). https://www.eurocontrol.int/tool/controller-pilot-datalink-communications-ground-automated-tool, 2011.

[10] EUROCONTROL. Surveillance avionics monitoring. https://www.eurocontrol.int/function/surveillance-avionics-monitoring, 2024.

[11] EUROCONTROL. Surveillance RF Environment Monitoring (1030/1090 MHz). https://www.eurocontrol.int/service/surveillance-rf-/environment-monitoring-10301090-mhz, 2024.

[12] EUROCONTROL. Data link network operational status report. Technical Report Data link Network Operational Status Report, The European Organisation for the Safety of Air Navigation (EUROCONTROL), January 2025.

[13] European Telecommunications Standards Institute. Draft ETSI EN 301 841-2 V1.2.0 (2019-02): VDL Mode 2; Technical characteristics and methods of measurement for ground-based equipment; Part 2: Upper layers. Draft standard, ETSI, 2019.

[14] Federal Aviation Administration (FAA). Selection of cyclic redundancy code and checksum algorithms to ensure critical data integrity. Technical Report DOT/FAA/TC-14/49, FAAn, March 2015.

[15] Federal Aviation Administration (FAA). Safety Alert for Operators (SAFO) 23005: Recommended Procedures for Controller–Pilot Data Link Communications (CPDLC) and Partial Re-route Clearances (Revised Initial UM79 uplink message). Technical report, FAA, August 2023.

[16] Federal Aviation Administration (FAA). Advisory Circular 91-70D: Oceanic and Remote Continental Airspace Operations. Advisory Circular AC 91-70D, FAA, April 2025.

[17] Andrei Gurtov, Tatiana Polishchuk, and Max Wernberg. Controller–pilot data link communication security. *Sensors*, 18(5), 2018.

[18] Alex Hiles and Bashar I. Ahmad. A generic machine learning framework for radio frequency fingerprinting. *arXiv 2510.09775*, 2025. https://arxiv.org/abs/2510.09775.

[19] ICAO Aeronautical Communications Panel Working Group I. ICAO ACP Working Group I Meeting Papers, 2016–2023.

[20] International Civil Aviation Organization. Updates on space-based vhf communication. Working Paper FSMP-WG/11 WP/17, ICAO, Virtual Meeting, February 2021.

[21] International Civil Aviation Organization (ICAO). ATN/IPS SARPs and ATN Security Concepts. Doc 9896, ICAO, 2023.

[22] International Civil Aviation Organization (ICAO). Global Air Navigation Plan (GANP) 2023–2040. Technical report, ICAO, 2023. Roadmap for CNS/ATM modernization including ATN/IPS and CPDLC.

[23] International Telecommunication Union (ITU). X.680: Information Technology – Abstract Syntax Notation One (ASN.1): Specification of Basic Notation. Technical report, July 2002.

[24] International Telecommunication Union (ITU). X.690: Information Technology – ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Technical report, July 2002.

[25] International Telecommunication Union (ITU). X.691: Information Technology – ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER). Technical report, July 2002.

[26] Kai Jansen, Matthias Schäfer, Daniel Moser, Vincent Lenders, Christina Pöpper, and Jens Schmitt. Crowd-gps-sec: Leveraging crowdsourcing to detect and localize gps spoofing attacks. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 1018–1031, 2018.

[27] Aswathi Karunakaran Beena and Devika Sugathan. Formal analysis of security protocol in civil aviation using tamarin. Master's thesis, Linköping University, 2024.

[28] Suleman Khan, Gurjot Singh Gaba, An Braeken, Pardeep Kumar, and Andrei Gurtov. Akaash: A realizable authentication, key agreement, and secure handover approach for controller-pilot data link communications. *Int. Journal of Critical Infrastructure Protection*, 2023.

[29] Suleman Khan, Gurjot Singh Gaba, and Andrei Gurtov. A federated learning based security for controller-pilot data link communication. In *33rd Congress of the Int. Council of the Aeronautical Sciences (ICAS)*, 2022.

[30] André Lehto, Isak Sestorp, Suleman Khan, and Andrei V. Gurtov. Controller pilot data link communication security: A practical study. *2021 Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2021.

[31] Tomasz (szpajder) Lemiech. dumpvdl2: Vdl mode 2 message decoder and protocol analyzer. GitHub repository, 2024. Version 2.4.0 released October 19, 2024.

[32] Giacomo Longo, Martin Strohmeier, Enrico Russo, Alessio Merlo, and Vincent Lenders. On a collision course: Unveiling wireless attacks to the aircraft traffic collision avoidance system (TCAS). In *33rd USENIX Security Symposium (USENIX Security 24)*, 2024.

[33] Matt Thurber. Hackers, FAA Disagree Over ADS-B Vulnerability. *AIN*, August 2012. https://www.ainonline.com/aviation-news/air-transport/2012-08-21/hackers-faa-disagree-over-ads-b-vulnerability.

[34] Tom McParland, Vic Patel, and WJ Hughes. Securing air-ground communications. In *20th Digital Avionics Systems Conference (DASC)*, volume 2. IEEE, 2001.

[35] Erwin Orye, Gabor Visky, and Olaf Maennel. Analysing the actual use of controller–pilot data link communications. In *10th OpenSky Symposium*. MDPI, 2022.

[36] Radio Technical Commission for Aeronautics (RTCA). Do-224 signal-in-space minimum aviation system performance standards (masps) for advanced vhf digital data communications including compatibility with digital voice techniques. Revision d, RTCA, 2018. DO-224.

[37] E. Rescorla and H. Tschofenig. The Datagram Transport Layer Security (DTLS) Protocol Version 1.3. RFC 9147, IETF, 2022.

[38] Harshad Sathaye, Guevara Noubir, and Aanjhan Ranganathan. On the implications of spoofing and jamming aviation datalink applications. In *38th Annual Computer Security Applications Conference*, 2022.

[39] Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir. Wireless attacks on aircraft instrument landing systems. In *28th USENIX Security*, pages 357–372, 2019.

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

[41] Mohamed Slim, MS Ben Mahmoud, Nicolas Larrieu, and Alain Pirovano. An aeronautical data link security overview. In *2009 IEEE/AIAA 28th Digital Avionics Systems Conference*, pages 4–A. IEEE, 2009.

[42] Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. You talkin' to me? exploring practical attacks on controller pilot data link communications. In *7th ACM on Cyber-Physical System Security Workshop (CPSS)*, 2021.

[43] Matthew Smith, Martin Strohmeier, Jonathan Harman, Vincent Lenders, and Ivan Martinovic. A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems. In *Proceedings 2020 Network and Distributed System Security Symposium*. Internet Society, 2020.

[44] Jon Standley. CPDLC Spreads Its Wings. *Air Traffic Technology International*, March 2024.

[45] Tim H Stelkens-Kobsch, Andreas Hasselberg, Thorsten Mühlhausen, Nils Carstengerdes, Michael Finke, and Constantijn Neeteson. Towards a more secure atc voice communications system. In *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*. IEEE, 2015.

[46] Paul E. Storck. Benefits of commercial data link security. In *2013 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, pages 1–6, 2013.

[47] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. Intrusion detection for airborne communication using phy-layer information. In *Detection of Intrusions and Malware, and Vulnerability Assessment*, 2015.

[48] Martin Strohmeier, Ivan Martinovic, and Vincent Lenders. *Securing the Air–Ground Link in Aviation*, pages 131–154. Springer, Cham, 2020.

[49] Martin Strohmeier, Anna K Niedbala, Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Surveying aviation professionals on the security of the air traffic control system. In *International Workshop on Cyber Security for Intelligent Transportation Systems*, pages 135–152. Springer, 2018.

[50] Martin Strohmeier, Matthias Schäfer, Rui Pinheiro, Vincent Lenders, and Ivan Martinovic. On perception and reality in wireless air traffic communication security. *IEEE transactions on intelligent transportation systems*, 18(6):1338–1357, 2016.

[51] Martin Strohmeier, Giorgio Tresoldi, Leeloo Granger, and Vincent Lenders. Building an avionics laboratory for cybersecurity testing. In *15th Workshop on Cyber Security Experimentation and Test (CSET 22)*, 2022.

[52] Yu Wang, Guan Gui, Yun Lin, Hsiao-Chun Wu, Chau Yuen, and Fumiyuki Adachi. Few-shot specific emitter identification via deep metric ensemble learning. *IEEE Internet of Things Journal*, 9(24):24980–24994, 2022.

[53] Matthias Wilhelm, Ivan Martinovic, Jens B Schmitt, and Vincent Lenders. Short paper: Reactive jamming in wireless networks: How realistic is the threat? In *Proceedings of the fourth ACM conference on Wireless network security*, pages 47–52, 2011.

10 Appendix

This appendix provides additional technical details regarding CPDLC over ATN-B1.

10.1 AVLC: Specializing HDLC for Aviation

Aviation VHF Link Control (AVLC), documented in [36], is a specialized derivative of HDLC designed for aeronautical data link communications. It operates through three distinct frame types: Information frames (I-frames), which carry user data from the network layer while optionally including flow and error control information; Supervisory frames (S-frames), which provide flow and error control functions when piggybacking on data is not possible or appropriate; and Unnumbered frames (U-frames), which serve many purposes such as link establishment, management, and termination, with some variants including information fields. The implementation of our RGS, along with the DoS attack methods presented in this work, are extensively ased on AVLC primitives. As demonstrated in Sections 5.1.1 and 5.1.2, familiarity with these primitives alone is sufficient to cause substantial disruptions in ATN-B1 CPDLC communications. Figure 12 depicts the generic structure of an AVLC frame.

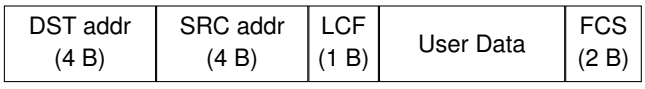


Figure 12: AVLC Frame Structure

The three AVLC frame types (U, I, and S) primarily differ in the computation of the Link Control Field (LCF) and the

handling of the user data field. For example, an I-frame maintains sender and receiver sequence numbers within the LCF, whereas a U-frame DISC employs a fixed LCF. This illustration provides a simplified view; in practice, AVLC frames carry additional information, such as ground/air identification, address type encoding, command/response semantics, and poll/forward indicators within the encding of addresses and LCF. Understanding these distinctions is essential for both the implementation and the exploitation of AVLC-based communication.

10.2 Datalink State Machines as Attack Vector

The physical layer is managed by the VDL Management Entity (VME), which oversees the establishment, maintenance, and termination of VDL connections. This is achieved by instantiating, interacting with, and deleting a Link Management Engines (LME) for each connection. The LME (Figure 13) is responsible for link initialization, maintenance, monitoring, termination, and channel management. Once a connection reaches the Link Connected State, meaning that the XID Link Establishment Request and Link Establishment Response have been successfully exchanged, the LME creates a Data Link Entity (DLE) (Figure 14), which then handles the data transfer and error recovery. As illustrated in Figure 13, when the LME is in the Link Connected State, the receipt of a disconnect frame, notified by the DLE, triggers termination of the DLE and an transition to the Link Unavailable State, independent of the state of higher-layer connections, active virtual circuits, or concurrent sub-protocol sessions. This behavior makes the Data Link state machines an exceptionally trivial yet powerful attack vector, as the disconnect frame is both stateless and structurally simple. Therefore, it can be injected at any point during an active connection without requiring sequence number tracking, parameter prediction, or synchronization. This property is exploited in Section 5.1.2, where it is further combined with the fact that an aircraft will accept frames not only addressed directly to it, but also to the broadcast address 0xFFFFFF. The outcome is an escalation from a single targeted DoS to a global disruption, simultaneously affecting all aircraft connected to the impersonated ground station.

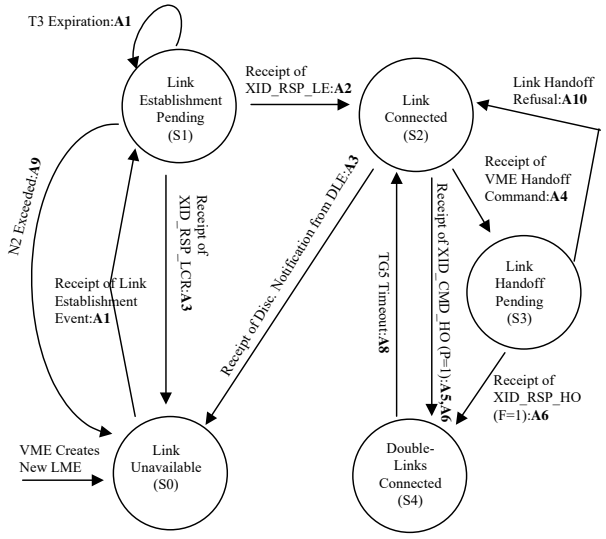


Figure 13: LME FSM [13]

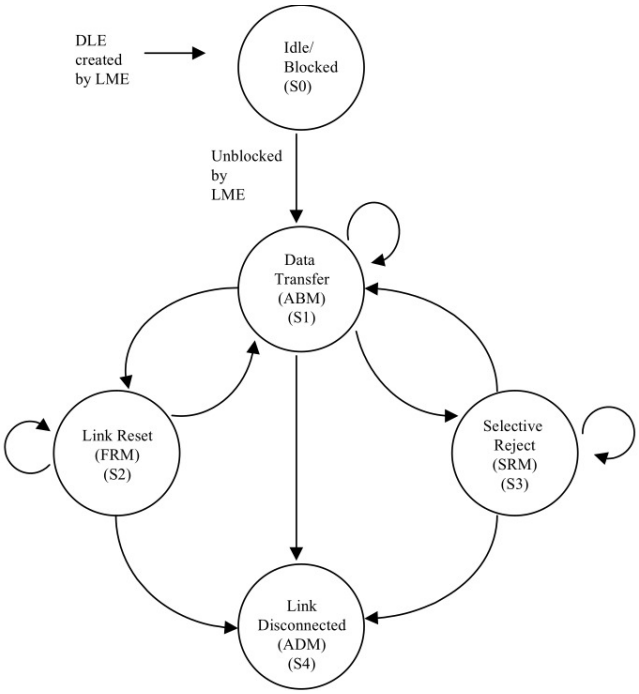


Figure 14: DLE FSM [13]

10.3 ATN-32 checksum

ATN B1/CPDLC and related ATN air–ground protocols refer to a common "ATN message checksum" [14] rather than redefining a checksum in each layer. This appendix captures the exact arithmetic model and update rule used by that checksum.

Definition. Given a message $M = (m_1, \ldots, m_n)$ of n octets ($m_i \in \{0, \ldots, 255\}$), ATN-32 maintains four 8-bit running sums (C_0, C_1, C_2, C_3). Addition is performed in one's-complement with a post-add mapping $\texttt{0xFF} \mapsto \texttt{0x00}$ or equivalently modulo 255.

Algorithm. Initialize $C_0 = C_1 = C_2 = C_3 = 0$. For each byte m_i in order:

$$C_0 \leftarrow C_0 + m_i,$$
$$C_1 \leftarrow C_1 + C_0,$$
$$C_2 \leftarrow C_2 + C_1,$$
$$C_3 \leftarrow C_3 + C_2,$$

The 32-bit FCS is then computed as (X_0, X_1, X_2, X_3) and derived as follows:

$$X_0 = -(C_0 + C_1 + C_2 + C_3),$$
$$X_1 = C_1 + 2C_2 + 3C_3,$$
$$X_2 = -(C_2 + 3C_3),$$
$$X_3 = C_3.$$

Relation to Fletcher. ATN-32 is a Fletcher-like checksum using four cascaded 8-bit sums rather than Fletcher-32's two 16-bit sums. It is order-sensitive and provides higher Hamming distance for short PDUs, but degrades at larger lengths (≈ 6112 bits). Implementations should therefore not assume strong error-detection guarantees for long PDUs.

10.4 Abstract Syntax Notation One (ASN.1)

Abstract Syntax Notation One (ASN.1) [23] is an international standard that defines a platform-independent language to specify data structures in communication protocols. It separates the abstract syntax (description of the data) from transfer syntax, enabling a single message definition to be consistently exchanged across heterogeneous systems and multiple encodings. Several encoding rules exist to map ASN.1-defined data structures into binary or textual representations.

Within the ATN/OSI stack, ASN.1 with UPER encoding is used to define and serialize exchanges such as (PM)CPDLC exchanges and the session layer X.227 SPDU. Unlike Basic Encoding Rules (BER), Canonical Encoding Rules (CER), or Distinguished Encoding Rules (DER), which are relatively verbose [24], PER/UPER were designed for bandwidth-constrained environments [25], relying on compact bit-level encodings suitable for aviation VHF datalinks.

10.5 PM CPDLC Checksum

The Protected Mode (PM) CPDLC checksum is defined in terms of the ATN-32 checksum algorithm described in Section 10.3. Its role is to provide integrity protection for the set of critical identifiers that bind a CPDLC messages to a specific operational context.

Formally, the procedure constructs an ASN.1 structure known as the Content Protected Message (CPM). The CPM is assembled from the CPDLC message payload together with the relevant contextual identifiers, namely: the flight identification, the ground facility designation, and the aircraft ICAO 24-bit address. This ASN.1 structure is then encoded using the aligned variant of the Packed Encoding Rules (PER/UPER) (Section 10.4). The resulting bit string is passed as input to the ATN-32 checksum process (Section 10.3), and the four-octet output $(X_0, \ldots, X_3)$ of that algorithm constitutes the PM CPDLC checksum value.

In effect, the PM CPDLC checksum mechanism leverages the established ATN checksum to ensure that the integrity verification step is consistent across the ATN protocol stack, while extending the coverage to include the operational identifiers required to identify CPDLC communications.

10.6 Injection timings

The results in Table 4, derived from observations of legitimate traffic, indicate that State-dependent DoS methods (Sections 5.1.1, 5.1.3, and 5.1.4) are constrained by narrow timing windows, which become increasingly tighter with the higher the target layer, since **all the timing windows of the lower layers should be satisfied as well**. Exploiting higher-layer states further requires detailed knowledge of the protocol's operation; for example, an IDRP UPDATE PDU can create a short-lived opportunity for a control flow injection with an IDRP CEASE PDU, but only if the attacker can anticipate all the lower layer variables and align with protocol-specific behavior. Attacks against lower layers involve fewer state variables, making synchronization comparatively simpler, though still technically challenging. Overall, these values suggest that while higher layers state-dependent DoS attacks and injections are possible, their success hinges on precise knowledge of protocol timings and careful optimization, leaving them operationally fragile – especially considering the high variance observed in timing measurements.

Type	Median Δt (s)
COTP	0.837
IDRP	0.228
CLNP	0.686
X.25 Data	0.381
AVLC I	0.306

Table 4: Median parameters update time by layer.

10.7 Note on Denial-of-Service Techniques

Our analysis shows that any anomalous frames in the exchange can trigger protocol side effects, making them candidates for denial-of-service (DoS). In Subsection 5.1, we focus on the most relevant and hazardous cases, classifying them and analyzing their side effects and practical impact. Although some frames are easier to exploit or have higher impact, the attack surface remains broad, and even less convenient cases represent viable disruption vectors.

More broadly, the ATN-B1 design philosophy (Section 8.2) reflects a reliance on obscurity and complexity rather than explicit security mechanisms. While the protocols are generally robust against errors, even attackers with limited system knowledge can induce disturbances using commercial off-the-shelf equipment. A skilled adversary with deeper protocol understanding can exert disproportionate influence, potentially leading to critical disruption.