You talkin' to me? Exploring Practical Attacks on Controller Pilot Data Link Communications

Joshua Smailes
University of Oxford
Oxford, UK
joshua.smailes@cs.ox.ac.uk

Daniel Moser*
Cyber-Defence Campus,
armasuisse Science + Technology
Zurich, Switzerland
daniel.moser@inf.ethz.ch

Matthew Smith
University of Oxford
Oxford, UK
matthew.smith@cs.ox.ac.uk

Martin Strohmeier†
Cyber-Defence Campus,
armasuisse Science + Technology
Zurich, Switzerland
martin.strohmeier@armasuisse.ch

Vincent Lenders
Cyber-Defence Campus,
armasuisse Science + Technology
Zurich, Switzerland
vincent.lenders@armasuisse.ch

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

ABSTRACT

Worldwide, voice-based Air Traffic Control (ATC) communications are gradually being replaced with data link-based equivalents, namely the Controller Pilot Data Link Communications (CPDLC) system. This helps to manage the high levels of congestion on voice-based ATC—under modern traffic levels these analog voice channels are extremely busy, especially at times of peak traffic. CPDLC offers the ability to conduct most ATC actions in the form of digital text-based messages.

As with voice-based ATC, CPDLC has no built-in security mechanisms. Furthermore, the links which carry CPDLC do not have security mechanisms either. In this paper, we analyze the susceptibility of CPDLC to attacks by a software-defined radio (SDR)-equipped attacker. Crucially, this is different to attacks on aviation surveillance systems, as it requires the attacker to comply with a larger authentication protocol.

We identify attacks on CPDLC, including a man-in-the-middle attack on the protocol. This attack enables a take-over of an aircraft's communication on an attacker-specified frequency, after which arbitrary CPDLC commands can be transmitted to the target without alerting the legitimate controller. We empirically assess the likely effectiveness of this attack through a data collection and analysis exercise. In order to counteract this type of attack, we propose three countermeasures of different complexities, including logical checks and a public key infrastructure approach. We also estimate to what extent these countermeasures can be implemented without altering the underlying protocol.

CCS CONCEPTS

• **Security and privacy** → **Systems security**; • **Networks** → *Network protocols*; • **Computer systems organization** → *Embedded and cyber-physical systems.*

KEYWORDS

security, aviation, transportation, cpdlc, air traffic control

ACM Reference Format:
Joshua Smailes, Daniel Moser, Matthew Smith, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. 2021. You talkin' to me? Exploring Practical Attacks on Controller Pilot Data Link Communications. In *Proceedings of the 7th ACM Cyber-Physical System Security Workshop (CPSS '21), June 7, 2021, Virtual Event, Hong Kong*. ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3457339.3457985

1 INTRODUCTION

The aviation industry is in constant global operation, moving vast numbers of passengers around—4.3 billion in 2018 alone [27]. The continued operation of this industry relies on a high degree of safety while minimising delays.

Air traffic control (ATC) is crucial in ensuring flights are safe and efficient. Airspace is split up into regions manageable by individual Air Traffic Control Operators (ATCOs). These operators direct aircraft within their region, keeping aircraft safely separated, helping them to avoid unfavorable weather, and ensuring that the airspace is operating as efficiently as possible given weather conditions.

Reliable communications between an aircraft and the ATCO are fundamental to this task. Traditionally conducted via voice over the very high frequency (VHF) spectrum, most messages are well-structured and use a standard phraseology for maximum efficiency.

However, the systems struggle with capacity issues; many aircraft share the same channels, and operation is half-duplex (communications in both directions occur over the same frequency). As a result, communication within an ATC region must be sequential, leading to delays in sharing crucial messages and causing clashes with other transmissions. This situation has been deemed unsustainable by aviation authorities who have created modernization programs to handle increasing capacity more efficiently whilst also reducing delay and emissions.

*Also with ETH Zurich.
†Also with University of Oxford.

CPSS '21, June 7, 2021, Virtual Event, Hong Kong

ACM ISBN 978-1-4503-8402-5/21/06…$15.00
https://doi.org/10.1145/3457339.3457985

For ATC communications, this modernization includes moving from analog voice communications to digital data link communications. This move is achieved primarily through the use of the novel Controller Pilot Data Link Communications (CPDLC) system, which allows an ATCO to interact with far more aircraft over a given time period. It uses structured text-based messages delivered over existing data links to match commands used in ATC exchanges. In some areas, such as Maastricht Upper Area Control, CPDLC is already required in order to pass through the airspace [5].

However, CPDLC has no security mechanisms of its own as part of its design, and so inherits the security of the data links it runs on [11, 37]. Research has shown that typically these links are also not secured, or when they are, security is weak [44, 45]. Despite this, we cannot simply presume that attacks on these links will directly affect CPDLC due to its complexity and human component, as has been demonstrated for some ATC technologies in previous research [46].

To demonstrate the severity of this lack of security, we show how an attacker can carry out a practical man-in-the-middle (MITM) attack on CPDLC. This attack allows the adversary to 'capture' a target aircraft on a false CPDLC connection to an attacker-controlled false ATC station. Until either the flight crew or real ATCOs identify the attack, the attacker can issue instructions to the aircraft as if they were a legitimate ATCO. We verify the scale of this attack by measuring the MITM opportunities in the deployed operational CPDLC system used by commercial aircraft. With this attack in mind, we propose viable countermeasures, ranging from logical checks to the use of public key cryptography, none of which require a full system redesign.

Contributions. Our contributions in this paper include:

- We exploit basic wireless message injection and jamming attacks to design a realistic man-in-the-middle attack on CPDLC and analyze the potential impact,
- We measure the real-world incidence of the vulnerable message exchanges, to gauge how scalable and widespread the opportunities for such attacks may be,
- We propose and analyze the effectiveness of three fundamental categories of countermeasures which can help mitigate such attacks on CPDLC.

We describe the background in Sec. 2 before outlining our attacker model in Sec. 3. We then detail the attacks in Sec. 4, including a real-world analysis of the required message exchanges. We describe our proposed countermeasures in Sec. 5, discuss our findings in Sec. 6 and conclude in Sec. 7.

2 BACKGROUND

The primary purpose of ATC is to instruct pilots on movement around controlled airspace; to do so requires clear, low-latency, uninterrupted communication. Such communication includes requesting the aircraft's position or heading, instructing an aircraft to alter its heading or altitude, enabling or disabling data link services, and eventually handing over communication to the next ATC sector.

The continuous operation of ATC communication is critical in maintaining both safety and efficiency. In the case of communication failure, aircraft must be given additional separation to minimise risk of collision, and in some situations are requested to land when possible [43]. Due to this high required margin of safety, small errors or deviations from the agreed course can cause large delays and potentially pose a threat to the safety of the flight crew or passengers.

2.1 Voice-based Air Traffic Control

Traditionally, ATC has been conducted over voice communications—specifically, analogue radio in the space of 117.975-137 MHz. Airspace is divided into sectors (both geographically and by altitude), and each ATCO manages a specific sector. Each sector has one or more radio frequencies associated with it; pilots entering a given ATC zone tune their radio transponder to the respective controller frequency in order to connect. Frequency reuse within a geographic region is carefully managed, and sectors using the same frequency are usually separated by long distances [28].

To reduce confusion and keep communication times to a minimum, flight crew communicate with ATC using a well-defined standard phraseology. This means that most exchanges follow a standard pattern, such as establishing a new connection, signing off an old connection, or issuing and receiving commands [7]. This helps with clarity, particularly if the connection is poor or there is a language barrier; the vast majority of ATC communication occurs in English, so it is important to keep communications as simple as possible for non-native speakers.

As all communications within a given sector occur over the same frequencies, the system can cope with a limited number of aircraft only and is often congested. A number of efforts have been made to improve this, namely by reducing the channel spacing or bandwidth—in Europe, for example, high traffic density led to a shift from 25 kHz channels to instead using voice channels with a bandwidth of 8.33 kHz, also spaced at 8.33 kHz [36, 38].

However, given the limited frequency range and the diminishing returns on further reducing bandwidth, other solutions were needed. One approach might be to reduce the size of congested sectors, but this would increase the number of handovers required and make frequency spacing amongst nearby sectors more difficult.

Security. VHF does not implement any security; anybody with a radio transceiver tuned to the relevant frequencies can receive and transmit freely. ATCOs can only correlate the content of voice communications from an aircraft with available radar returns and provided flight plans [7]. As there are no mechanisms to prevent malicious actors from impersonating ATCs or aircraft, hoax callers have previously caused delays by forcing aircraft to abort landing and loop back around [40, 53]. Some methods have been proposed to address this problem, while keeping the open, robust, and globally-compatible nature of the system; either through watermarking or anomaly detection. Of the former, some works such as [6, 12, 13] propose inserting a small watermark on a voice signal, either in the non-audible portion or through alternative modulations. This allows the insertion of authentication data, but requires modification of the standard VHF physical layer. For anomaly detection, the authors in [47] propose both stress detection and voice-based authentication for individuals. Enrolment of pilots and ATCOs creates a challenge here as this database would apply worldwide. A further discussion of VHF security options can be found in [49].

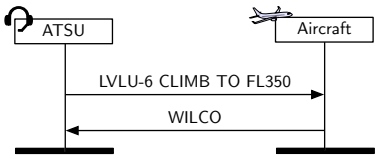

Figure 1: Standard CPDLC exchange: ATSU requests that the aircraft climb to flight level 350 (35,000 ft), aircraft responds that it will do so (i.e. with *Wilco*, or *will comply*).

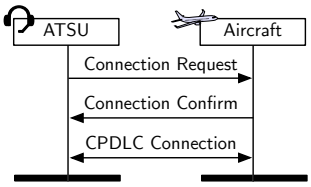

Figure 2: The standard CPDLC connection establishment handshake between an aircraft and an ATSU, based on [19].

2.2 Avionic Data Links

Given the pressing issues with analogue radio systems, namely congestion and a lack of security, other solutions are needed. While voice communications operate over analogue radio, the majority of other communications operate as applications on top of data links. These links use VHF, SATCOM, and HF technologies.

VHF (Very High Frequency). Aviation uses the 117.975 to 137.000 MHz band, over which data and voice services are provided [51]. 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, providing higher bit rates and acting as a general purpose network layer [30].

SATCOM (Satellite Communications). In some areas the range of VHF is not sufficient to reach aircraft, such as during oceanic crossings. In these areas data connection is provided through the use of geostationary satellites. These satellite links are general purpose, able to carry more than just flight data—this includes phone communications and high-speed internet connectivity [2, 42].

HF (High Frequency). HF operates at 3 to 30 MHz. Radio waves at this frequency reflect off the Earth's ionosphere, allowing a much larger operational range than VHF. There are approx. 15 HFDL (HF Data Link) ground stations, which support almost complete global coverage. However, the bit rate of HFDL is low and much of the message space is taken up with error correction mechanisms, due to the unfavourable propagation conditions. As a result, HF is used as a backup when VHF and SATCOM links are unavailable.

2.2.1 Benefits of Data Link ATC. As discussed in Sec. 2.1, the vast majority of communications between ATCs and aircraft are well-structured and use consistent phrasing. Data link ATC was introduced to reduce the load on voice-based ATC infrastructure—by replacing common voice exchanges with text-based messages, congestion on voice frequencies can be offloaded onto data link instead. We see this in our data collection (described in Sec. 4.5), observing over 400 messages per hour at peak times. This frees up voice channels significantly, allowing voice ATC to be used as an emergency fallback.

The standard phraseology employed by ATCs over voice lends itself well to a data link system, allowing voice messages to be linearly mapped to text messages using a standard library of keywords. In this way messages end up with a well-structured grammar and the system begins to resemble a communications protocol. Furthermore, this allows some aspects to be completely automated, such as the logon handshake and the control handover process.

As well as reducing congestion on voice communication channels, data link ATC has a number of other benefits, such as:

- Lower noise, reducing the need for repeated messages,
- Source and destination labels—messages are typically not encrypted, but units are configured so that only the intended recipient will display the messages,
- Lower immediacy requirements in listening and responding to ATC messages, as they directly receive relevant messages.

2.3 CPDLC Introduction

Controller-Pilot Data Link Communications is the primary method of modern data link ATC. In this section, we will explain its basic operations. Fundamentally, CPDLC messages can contain multiple elements with multiple commands. However, the processing logic for multi-element messages does not differ significantly from single-element messages—in the majority of cases, multi-element messages can be treated and processed in the same way as multiple single-element messages. As a result we will mostly be considering single-element messages in this paper.

We refer to the CPDLC unit on the ATC end as the *ATSU* or Air Traffic Services Unit.

There are two globally competing implementations of CPDLC: FANS 1/A and ATN B1. Generally, an aircraft implements one of these two, as does each ATSU. ATN B1 is used in much of continental Europe, and FANS 1/A is commonly used elsewhere, including Australia and the US. Both systems are in large parts compatible and there are ongoing efforts to converge them over time to maximize data link ATC coverage [35].

2.3.1 Standard Messages. Standard CPDLC messages broadly fall into one of two categories: *commands* and *information*. Commands are usually sent in the uplink direction (i.e. ATSU to aircraft) and information messages can be sent in either direction. Most CPDLC messages require a response. For commands, this response is either a *Wilco* (short for 'will comply') or an *Unable* downlink message, indicating whether or not the aircraft is able to comply with the request. Other types of messages may require *Affirm* or *Negative* responses, or *Roger* or *Unable*. Some messages do not require any response, though these are rare. An example of a message exchange is shown in Fig. 1.

2.3.2 Connection Establishment. In order to establish a CPDLC connection, the ATSU must correlate an aircraft's identifier with its flight plan, which is provided out of band. This is so that (as with voice-based ATC) the ATCO is aware of the intent of the aircraft and can direct it accordingly. If the aircraft already has an active CPDLC connection with a different ground station, then this information is sent ground-to-ground to the new ATSU as part of the connection handover process [21]. Otherwise, the correlation is done through

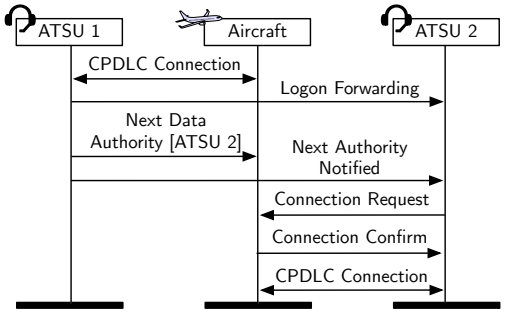

Figure 3: A standard CPDLC connection handover between ATSU 1, to which the aircraft is connected, and ATSU 2, which is the ATCO for the aircraft's next sector. ATSU 1 instructs the aircraft to connect to ATSU 2, before terminating its own connection with the aircraft. Based on [23].

a CPDLC *Logon Request* message from the aircraft, containing some of the following information [21]:

- Information on supported data link applications (including version numbers),
- Aircraft identifier (i.e. the aircraft registration or the unique Mode S 24-bit address of its transponder),
- Any other information required to correlate the logon request with the flight plan.

The ATSU then responds with a confirmation message.

Following a successful logon, the ATSU sends a CPDLC *Connection Request* message to the aircraft. If the aircraft does not have an active connection, it establishes the connection with the ATSU as its active connection, and sends a *Connection Confirm* message in response (see Fig. 2). We discuss the handover case, where an aircraft already has an active CPDLC connection, below.

2.3.3 Connection Termination. When an ATSU needs to terminate its connection with an aircraft, it sends the aircraft a *Termination Request* message. The aircraft responds with a *Termination Confirm* message, and the CPDLC connection is closed. This can only be initiated by the ATSU; in cases where the aircraft needs to terminate the connection either a *Disconnection Request* or *User Abort* message is used, depending on the CPDLC implementation [22]. These messages are only needed in case of errors; they are not used in standard operation.

2.3.4 Connection Handover. As an aircraft moves between sectors, it will need to hand over ATC communications between ATSUs. With voice, the current ATCO provides the frequency for the next sector. With CPDLC, the connection handover happens automatically and appears seamless to the flight crew [20]. If the handover occurs correctly, the crew do not need to perform another CPDLC logon, as any data sent to the ATSU during the logon is sent across during the handover. In Fig. 3, we show the standard CPDLC connection handover process, also described below:

(1) The previous data authority (ATSU 1) sends a ground-to-ground message to the new data authority (ATSU 2) containing logon forwarding information,
(2) ATSU 1 then sends a *Next Data Authority* message to the aircraft containing the identifier of the next ATSU,
(3) ATSU 1 sends a ground-to-ground message to the next ATSU informing it that the aircraft has been notified.
(4) ATSU 2 then sends a *Connection Request* message to the aircraft, which is responded to with a *Connection Confirm* (or *Connection Rejection* if the ATSU is not recognized as the next data authority, sometimes coupled with a *Not Authorized Next Data Authority* message).

Following this process, there is an inactive CPDLC connection between the aircraft and the next ATSU, ATSU 2, which becomes the active connection following the termination of the old connection as described in Sec. 2.3.3. The new CPDLC connection becomes active as soon as the aircraft processes the message, which occurs before the *Termination Confirm* message is sent.

In some scenarios, the current data authority does not send logon forwarding information to the next ATSU but instead transmits a *Contact Request* message to the aircraft, instructing it to send a *Logon Request* to the new data authority. This is followed by a *Contact Response* message, and finally a *Contact Complete* message.

The *Next Authority Notified* message is only supported in certain areas. Where it is available, the message is sent ground-to-ground between ATSUs following the *Next Data Authority* message, indicating that the new ATSU should send a *Connection Request* to the aircraft.[1] This is not essential to CPDLC's operation but it is helpful—if the aircraft receives a *Connection Request* before the *Next Data Authority* message, the connection is rejected. This message forces the new ATSU to wait until the aircraft is ready before initiating the handover.

2.4 Data Link Security

The CPDLC protocol does not have any built-in security beyond a basic message integrity checksum. Despite this, it is not trivially vulnerable to every attack—the system's human component means many basic attacks can be detected, as seen with voice-based ATC [32, 47]. We explore more realistic advanced attacks in Sec. 4.

Existing work on the security of ATC data links includes the authors of [11], who provide an overview of CPDLC and a threat model of the system, as well as suggesting possible security improvements. Similarly the authors of [3] look at data integrity threats to CPDLC and propose security measures at each network layer. In [4] the feasibility of transmitting crafted CPDLC messages is shown through experiments using decoders and encoders.

The work presented in [46] puts pilots in simulator scenarios to show that attacks on avionic systems can cause significant disruption and reduce trust in the systems in question. It is therefore of great importance that we understand the scope of attacks on CPDLC, their potential impact, and what can be done to mitigate threats.

In this work, we build on the existing research demonstrating the ease of crafting and injecting arbitrary CPDLC messages. We analyse the protocol itself in order to discover concrete vulnerabilities, which present a greater threat than the momentary disruption caused by individual injected messages. To the best of our knowledge, we are also the first to detect and measure such practical vulnerabilities in the real-world CPDLC system.

[1] The On-Line Data Interchange (OLDI) protocol for ground-to-ground communication supports this message, ATS Interfacility Data Communications (AIDC) does not [22].

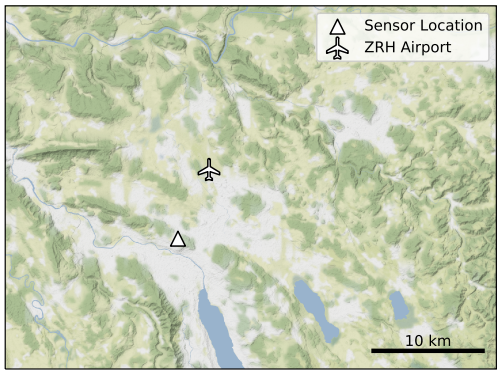

Figure 4: Overview of sensor and airport locations.

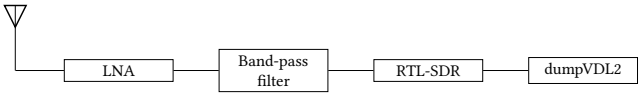

Figure 5: An overview of the software and hardware used for our data collection.

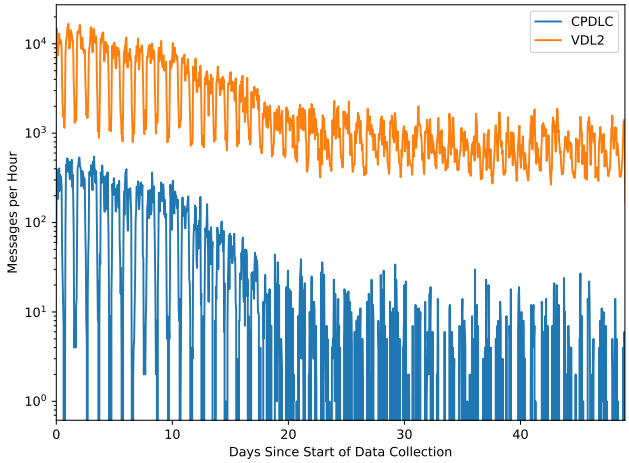

Figure 6: The number of received VDL2 messages, and VDL2 messages carrying CPDLC contents, aggregated per hour over the collection period. Plotted on a logarithmic scale.

3 ATTACKER MODEL

As CPDLC's primary use is to issue commands from ATSUs to aircraft, we assume that the attacker's main goal will be to hijack the data link and inject arbitrary messages, mostly from the ATSU to the aircraft but potentially in the other direction as well. This would allow them to issue direct commands to a chosen aircraft whilst the aircraft is in range. Such commands include instruction to change altitude, heading, or speed, activating and deactivating other data link systems, reporting the number of passengers on board, or even declaring an emergency. Such an attack could also cause the aircraft to ignore legitimate messages, which has the potential to cause delays until the problem is rectified.

The commercial-off-the-shelf equipment required to execute these attacks is straightforward to acquire, and is composed of:

- a HackRF, or other SDR able to transmit on VHF frequencies, costing around $300-500 [10],
- a VHF airband antenna suitable for reception and transmission, costing about $250 [50],
- an amplifier to increase transmission power so signals reach the aircraft, approximately $600 [1] (possibly more depending on desired transmission range).

As the acquisition of this equipment does not require a large budget, attacks can be performed by a motivated adversary, but exclude some low-resource attackers such as script-kiddies or hobbyists. On the software side, a CPDLC encoder and decoder is required to execute the attacks described in this paper. The `dumpVDL2` free open-source decoder is available [31], but although the authors of [4] demonstrated the feasibility of encoding CPDLC messages, no encoder is openly available yet. Because of this, an attacker would need to produce their own SDR-based software to carry out their attack.

In this paper, we consider attacks where the attacker is fixed at a single location. This limits the range to the radio horizon (around 400 km in radius), in turn constraining the duration of attacks to how long the aircraft remains in range. An attacker could scale up these attacks with antennae in multiple locations or by becoming mobile.

Most of the attacks discussed by us require the injection of messages as a wireless attack primitive. This is achievable with the equipment described above and a CPDLC encoder. Some of our attacks, such as those in Sec. 4.3.3, require the attacker to further be able to destructively interfere with legitimate messages. This is more difficult, requiring a well-timed burst of radio interference over the target ATSU frequency band. However, such reactive jamming has been shown to be feasible in [52] through partially decoding a transmission before initiating jamming. The CPDLC message type is at the start of the message followed by the parameters, so reactive jamming is likely to be highly effective.

Overall, we assume the attacker is able to read all CPDLC communications within the radio horizon, as well as inject, block and alter messages between aircraft and ground stations. Certain CPDLC messages are sent between ground stations, and we assume the attacker is unable to read or alter these—they are typically sent over wires and are thus harder to attack than radio communications [14].

3.1 Data Collection

Owed to CPDLC's unencrypted nature, anyone with a radio receiver can read and collect real messages sent by commercial aircraft equipped with the technology. Our data collection setup enabled us to explore this aspect of the system's threat model, and better understand the protocol in the process. Through analysis of the collected messages we were able to ensure that the concrete implementation of CPDLC used in the real-world indeed matched the official standard, thus enabling us to verify the attacks described in Sec. 4.

While the attacks described in this paper could theoretically be performed over any of the data link systems described in Sec. 2.2, we chose to collect and analyse messages transmitted specifically over the VDL2 system, in the VHF range. True to our attacker model, there already exist free and open-source tools to decode VDL2 communications, enabling a wide range of motivated adversaries. Additionally,

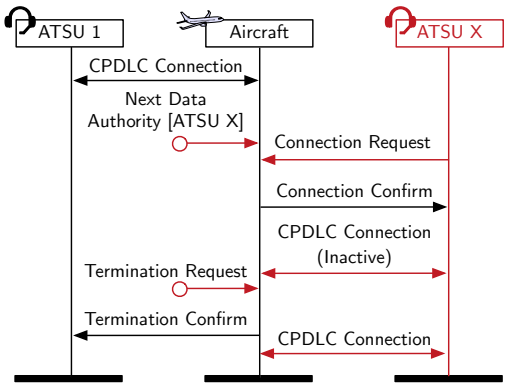

Figure 7: Design of the man-in-the-middle attack on the CPDLC handover. An attacker triggers a false handover to ATSU X, which is an identifier for a legitimate, but not in range, ATSU. The attacker injects messages appearing to be ATSU X, following protocol for connection handover.

VDL2 is in wide use already, and as such is fairly representative of CPDLC communications as a whole.

Our receiver was located at ETH Zürich's Hönggerberg campus, overlooking the airport at a distance of approximately 5 km (see Fig. 4). We used a Raspberry Pi running *dumpVDL2*, a free and open-source decoder available on GitHub [31]. The overall signal flow can be seen in Fig. 5. Our data collection ran continuously for 49 days, during which we saw 2,932,878 messages—57,372 of these contained CPDLC messages. The rate of messages over time is seen in Fig. 6. We see a clear drop in messages during the night, as well as a downwards trend over the whole collection period; this is due to our data collection occurring during the early stages of the COVID-19 pandemic, during which many flights were cancelled worldwide.

4 CONCEPT OF ATTACKS

Aircraft implicitly trust ATC—indeed, this trust is fundamental to the way in which airspace operates. If an ATCO gives an instruction to an aircraft, the aircraft is expected to comply unless it cannot, in which case the flight crew will inform the ATCO as soon as possible. Likewise, the aircraft expects that the instructions issued by the ATC are legitimate and will not endanger the aircraft.

As discussed previously, neither CPDLC nor its underlying wireless data links have dedicated security mechanisms by default. This allows an attacker to perform wireless message injection, thus interfering with exchanges between ATC and an aircraft.

In this section, we describe a man-in-the-middle attack on CPDLC which would 'capture' an aircraft's CPDLC communication, i.e. forcing it to switch to an attacker-controlled ATSU. This allows the attacker to issue arbitrary ATC commands until either the legitimate ATCOs or flight crew onboard the aircraft notice.

We begin by describing a basic attack relying solely on injection, before moving to more complex attacks involving the messages surrounding the CPDLC control handover process.

We do not consider message replay attacks; CPDLC's lack of encryption means attackers with access to an encoder can simply encode and inject messages rather than replay old messages.

4.1 Injection Attack

Due to CPDLC's lack of authentication, an attacker can craft and inject messages claiming to be the ATSU to which an aircraft is currently connected. This is a very simple attack, but it is thwarted due to the *Wilco* (i.e. will comply) message returned from the aircraft to the ATSU after each command. When this attack is attempted, the ATCO will notice an unwarranted *Wilco* and issue a follow-up message cancelling the command—likely before the flight crew begin to follow the instruction.

4.2 Man-in-the-Middle Attack

Injection attacks are easy to perform but since the humans-in-the-loop monitor both sides of the link, they are highly likely to be caught—if anything that is obviously unusual happens, the ATCO should investigate the issue. If an attacker is to have a longer-lasting effect then the CPDLC protocol itself must be attacked. One such class of attacks involves the attacker acting as a man-in-the-middle (MITM), convincing the aircraft to connect to a false ATSU controlled by the attacker, rather than the legitimate current ATSU.

In the standard CPDLC control handover (see Fig. 3), the aircraft is told to connect to the next ATSU through the *Next Data Authority* message, which does not require a response [24]. If the attacker injects a copy of this message with the identifier of an arbitrary ATSU, they will be able to trick the aircraft's CPDLC system into connecting to a false, attacker controlled ATSU. This has the effect of the aircraft rejecting legitimate messages from the real, current ATSU, and complying with spoofed commands without immediately alerting the ATCO via a standard response.

The full design of this attack can be seen in Fig. 7. Concretely, the attacker takes the following steps:

(1) Attacker injects a *Next Data Authority* message to the aircraft, instructing it to connect to ATSU X,
(2) Attacker sends a *Connection Request* message to the aircraft, and awaits a *Connection Confirm*. This establishes an inactive CPDLC connection between ATSU X and the aircraft,
(3) Attacker injects a *Termination Request* as if from ATSU 1, sent to the aircraft,
(4) Once the aircraft terminates the connection with ATSU 1, the aircraft-ATSU X CPDLC connection becomes active.

During the later steps, the aircraft will respond with a *Termination Confirm* to ATSU 1, which could alert ATSU 1 to the capture. This makes it relatively straightforward to spot the attack at this point.

Although it may be possible to detect after execution, the short-term effect of this attack is notable. Once the attacker has gained an active CPDLC connection with the aircraft, it can send arbitrary messages without a response from the aircraft reaching the legitimate ATSU. Should ATSU 1 fail to notice the termination of its connection with the aircraft, the first indication that something has gone wrong will be the aircraft starting to follow malicious commands. At this point, even if the ATCO is able to alert the flight crew that something has gone wrong, disruption is likely.

4.3 Advanced Man-in-the-Middle

As noted above, the attack can be spotted should ATSU 1 identify an unwarranted connection termination. Based on a systematic analysis of the protocol and the ATC system as a whole, we now suggest

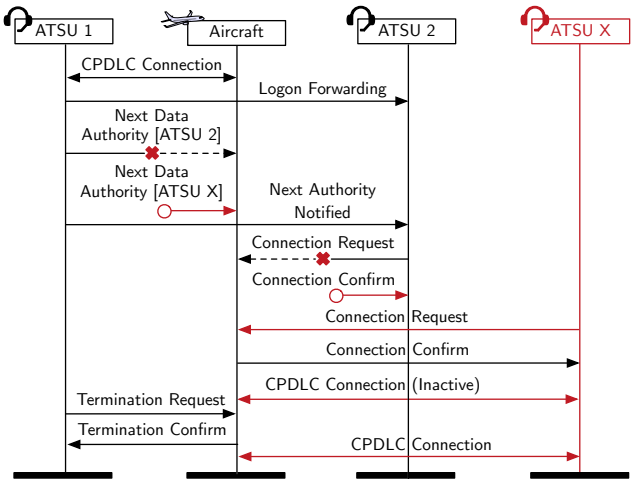

Figure 8: Design of the MITM attack on the CPDLC connection handover process, in which the attacker is able to block legitimate messages. Red arrows indicate messages involving the attacker, red crosses indicate jammed messages, and red circles are injected messages. The attacker compromises an ongoing CPDLC connection handover, causing the aircraft to connect to ATSU X instead of ATSU 2.

several techniques that make it harder for ATSU 1 to notice the attack, or to regain control of the aircraft once they do so.

4.3.1 Voice Disruption. To make it more difficult for the legitimate ATCO to regain contact with the aircraft following a capture, the attacker can attempt to disrupt voice communications alongside CPDLC. By injecting a *Monitor* CPDLC message the attacker can instruct the flight crew to switch voice frequency, thus breaking contact with the legitimate ATCO.

4.3.2 ATSU Identifier. In the spoofed *Next Data Authority* message of the basic MITM attack, the attacker specifies an ATSU identifier for the aircraft to connect to. Identifier choice should be made with care—if a nearby ATSU is chosen then the connection may be rejected due to a logon forwarding failure (as described in Sec. 2.3.4). Flight crew are informed of the identifier of the next ATSU following a successful handover [20], so it may be beneficial to choose an identifier similar to that of a nearby ATSU to avoid causing suspicion.

4.3.3 Selective Message Jamming. If the attacker is able to selectively jam legitimate messages, a much stronger set of attacks is possible. By blocking the *Termination Confirm* message in the original attack (seen in Fig. 7), the ATSU is not alerted to the attack when the aircraft disconnects. This means the first indication that something has gone wrong will be when the legitimate ATSU attempts to issue a command, and receives a *Not Current Data Authority* message in response (or, as discussed above, when the attacker issues a command and the aircraft complies, and radar data relays this to ATCOs). This gives the attacker a lot more time to act before they are discovered.

Alternatively, the attacker can perform a similar attack by taking advantage of a legitimate CPDLC handover, demonstrated in Fig. 8. By blocking the *Next Data Authority* message (and the *Connection Request* from the new ATSU) and injecting new messages with the ATSU identifier changed, the attacker once again tricks the aircraft into connecting to the incorrect ATSU. This attack has the same ramifications as the original MITM attack, with the added benefit that the *Termination Request* is legitimate and the handover happens at the expected time, so the ATCO and flight crew are significantly less likely to notice an immediate problem. If the ATSU does not support *Logon Forwarding* then a *Contact Request* message will be sent (see Sec. 2.3.4). This message also includes the address of the new ATSU, so the attacker will need to jam and spoof these messages in the same way as the other messages.

4.3.4 (Not) Current Data Authority. Following a capture, all messages from the legitimate ATSU will receive a *Not Current Data Authority* response [24], limiting the duration of the attack. If the attack is performed surrounding a legitimate handover as above, then this logic can be exploited. Since this message is sent regardless of whether the connection is inactive or simply non-existent, the legitimate next ATSU may be expecting a *Current Data Authority* message to activate the link. The ATSU will refrain from sending messages until then, making it harder to use rejected messages as a means to identify a hijacked connection.

The *Current Data Authority* message only exists under the "ATN B1" implementation of CPDLC, so this attack variant is only possible in certain areas. The longevity of this attack is also limited since the ATCO should begin to investigate if the aircraft ventures too far into the sector without an active connection [26].

4.4 Attack Impact

In each variant of this attack, the adversary can either deny ATC communications or briefly capture an aircraft's CPDLC communication and issue their own commands under the guise of a legitimate ATSU. Detecting such an attack in progress relies on either:

- ATCOs noticing unexpected or out of sequence messages, or unexpectedly no longer being the current data authority,
- ATCOs noticing no voice communications or unexpected aircraft movements through radar,
- Flight crew being familiar with the area and thus identifying false ATSU identifiers, or spotting unusually quiet ATC communications.

Each of these identification steps not only takes time but requires each party to be actively looking for an issue. It is important to note that such sophisticated wireless attacks are not in the primary focus of the processes used to debug issues by pilots and ACTOs, which concentrate on hard- and software failures first.

Should the attacker successfully carry out the attack and be able to inject arbitrary messages, the potential disruption is severe. Once fight crew identify that they have been cut off from legitimate ATC they will seek to alert the ground. This will be done either by voice (possibly declaring an emergency through use of the terms MAYDAY or PAN PAN), or by turning their squawk code—an ATC-issued identifier which is transmitted to ATC by the aircraft transponder—to 7500 to indicate radio failure [15, 18].

ATC response to the MITM attack will depend on whether they come to believe the aircraft to be subject to unlawful interference. At the very least, the aircraft will be monitored to see if it is following communication failure procedures, such as squawking the correct

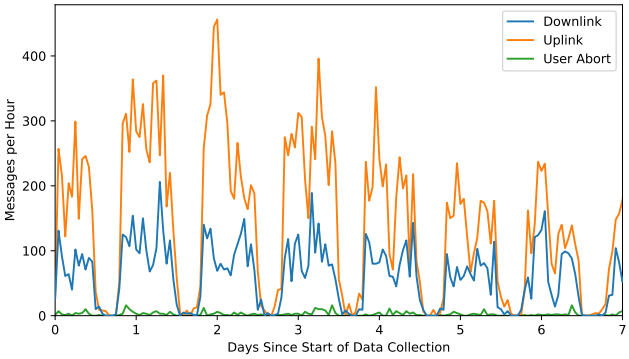

Figure 9: Hourly CPDLC message type statistics.

number and continuing on the pre-filed flight plan [16]. Should the aircraft believe it is subject to interference, it will be required to follow unlawful interference rules and attempt to land as soon as possible, causing an undue diversion [17]. If they believe the aircraft has been unlawfully interfered with and begins to deviate from flight plans, it will be treated as a 'strayed aircraft' [26]. This can result in the aircraft being intercepted by military aircraft; a Ryanair flight in 2018 saw such an interception as a result of radio failure [9].

4.5 Real-World Vulnerability Analysis

To validate and quantify the opportunities for an adversary to carry out the described attacks in the real world, we analyze the collected CPDLC messages in order to measure the handover occurrences and the messages' physical characteristics. With our equipment setup we were able to collect both uplink and downlink messages, supporting the assumption that an attacker can affect communications in both directions. The number of downlink messages was observed to be approximately half the number of uplink messages, shown in Fig. 9. This fits with our understanding of the protocol; the majority of uplink messages require a response from the aircraft, but many downlink messages do not.

In our data collection, we received VDL2 communications involving a total of 4,798 aircraft, out of which 2,307 were using CPDLC. For illustrative purposes, we extracted position reports from a subset of these messages, shown in Fig. 10. Messages were received from a distance of up to 300 km, with the majority of messages within a radius of 100 km. This presents a significant risk—provided an attacker has the necessary equipment to carry out the attack, they can do so without being nearby. While it may be possible to locate a nearby attacker, it will be very difficult to determine the precise location of an attacker within even a 100 km radius. This risk may be partially mitigated by triangulating an attacker's location from multiple antennae.

During our collection period, the ground stations within our reception range transmitted a total of 5,395 *Next Data Authority* messages. A number of these messages were re-transmits, putting the number of distinct handovers at 3,335. This translates to approximately one handover every 21 minutes. Far fewer handovers occur at night—taking this into account reveals that there is only 16 minutes between handovers during the day. Furthermore, handovers were observed to be significantly more frequent before the COVID-19

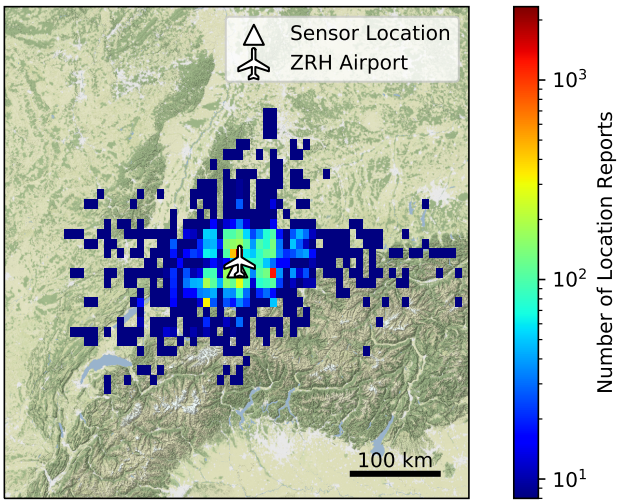

Figure 10: Density plot of received location reports via VDL2 and different sub-protocols.

pandemic, at approximately one every 6 minutes. We can assume the rate of handovers will return to this level as air travel usage returns to normal. From our sensor location above the airport, we were able to receive messages from a total of 8 ground stations located at and around the airport. We saw a total of 123 individual ground station addresses, and observed approximately two thirds of ground stations communicating using CPDLC.

Our data analysis shows that an attacker has ample opportunity to carry out the MITM attacks described above—not only are they not required to be very close in order to communicate with an aircraft or ATSU, but they can also communicate with multiple base stations simultaneously from a single location. Furthermore, the frequency of CPDLC handovers is sufficiently high that attacks can be performed continuously, with the potential for multiple attacks to be performed simultaneously. It also increases the viability of attacks involving message jamming—even if selectively jamming a message through destructive interference is not always successful, the attacker can simply try over until it succeeds.

Our data collection and analysis demonstrate that such attacks have the opportunity and the potential to have a significant effect on many flights in a typical airport airspace. All message exchanges in the described attacks follow the CPDLC protocol as we observed it in the real-world. With CPDLC message injection recently having been demonstrated in a laboratory setting [4], we can thus safely assume that the described message injection is feasible and all messages will be treated as legitimate by both aircraft and ATSU.

5 COUNTERMEASURES

In this section we propose a number of potential countermeasures to the attacks described in Sec. 4. These range from additions to the message processing logic to help catch basic attacks, through to using message signatures or encryption. We also consider how easy or difficult each would be to implement, as well as their effectiveness at mitigating attacks on the system.

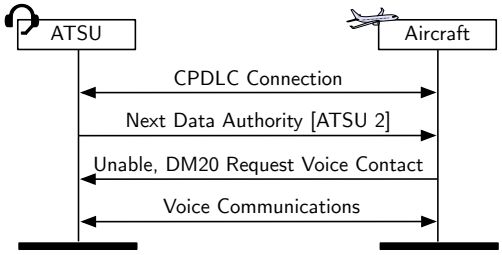

Figure 11: A failed CPDLC connection handover. The identifier of ATSU 2 has been deemed too far away by the modified CPDLC unit, so the flight crew fall back to voice contact to confirm the intention of the ATCO.

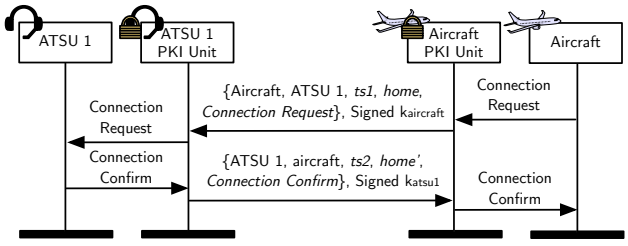

Figure 12: A standard CPDLC connection establishment with the proposed PKI system. Each message is signed before transmission, and the message signatures are verified before being forwarded to the CPDLC unit.

5.1 Geography-based

In Sec. 4.3.2 we addressed the issue of an attacker choosing which ATSU identifier to spoof, concluding that it is generally easier for the attacker to choose an identifier for an ATSU positioned beyond the aircraft's radio horizon. With this in mind we can load onto each aircraft a database of ATSU identifiers along with their locations, and upon receipt of a *Next Data Authority* message check the ATSU location against this database. If the unit is beyond the radio horizon, the aircraft can refuse the connection and revert to voice communications to resolve the problem.

A slightly more sophisticated version of this technique involves building a graph of connections between ATSUs—an edge exists between two nodes only if it is normal for aircraft to switch between those two ATSUs. CPDLC can then check if an edge exists between its current authority and the identifier in the message, and refuse the connection if none exists. This is demonstrated in Fig. 11.

Building such a database or graph is feasible—there are approximately 5,800 ATC regions in the United States [8], so conservatively assuming there are 100,000 worldwide and each entry takes 1 kB, our database will be approximately 100 MB in size. Looking up an entry is computationally very cheap, as is checking its proximity to the aircraft's current position. It may prove challenging to keep such a database up to date as new regions are introduced, but should not be impossible—such information is published every 28 or 56 days by local authorities in Aeronautical Information Publications (AIPs) [41].

There are two ways of handling voice contact; either the CPDLC unit alerts the flight crew that there has been an issue and suggests voice contact through an indicator in the cockpit or it sends an automated downlink response requesting voice contact. Either would work well but the second implementation may save time as it would not need to wait for the pilot to notice a problem before voice communications are initiated.

5.2 Interference Alerts

As it currently stands, there are a number of situations in which erroneous messages are not made known to the recipients. For instance, if an aircraft receives a message from an ATSU with which it does not have an active CPDLC connection, the message will be discarded with an automated *Not Current Data Authority* response—the flight crew are never alerted to the message.[2] Similarly, if an ATSU receives a message from an aircraft with no active CPDLC connection, the message is discarded, sometimes sending an automated free text *CPDLC Transfer Not Completed* response [25]. If the CPDLC unit warned the flight crew or ATCO when it receives these potentially suspicious messages then it would be easier for them to notice when attacks are being performed and react accordingly.

Some of the attacks described in Sec. 4 involve the use of selective jamming to block messages. If the CPDLC unit warned the flight crew and ATC when it detects such interference, it could give them advance warning about potential attacks. While reactive jamming is noted to be difficult to detect [52], some work has been done to detect such jamming which could be implemented into future systems [48].

These changes are easy to implement as they do not impact the CPDLC protocol—backwards compatibility and compliance with regulations is less of a concern. They offer the flight crew and ATCO additional useful information that they would otherwise not have, increasing the likelihood they can effectively respond to threats.

5.3 PKI

A more challenging but long lasting solution to the problems with CPDLC would be to modify the CPDLC specification to include a Public Key Infrastructure (PKI) system. It is possible to do this in a backwards-compatible way, by making the changes in the form of an intermediary box which sits between the CPDLC unit and the data link equipment in the aircraft and ATSU.

Under this new system, each ATSU and aircraft is given a private/public keypair, used for signing messages and verifying signatures respectively. We designate a small number of ATSUs as *authorities* which are responsible for distributing keys. Each aircraft/ATSU which implements this system has a list of the public keys of each authority. Each aircraft and ATSU also has one of these authorities designated as its "Home", which handles the key generation, distribution, and revocation for that unit. We avoid encrypting the messages in order to allow safe fallback options should it not be possible to verify signatures.

[2] Certain situations have been observed in which this message is not sent, but these are not typical [54].

5.3.1 Securing CPDLC Messages. In Fig. 12 we describe a standard CPDLC message exchange under this new system; our new authentication unit intercepts the plain CPDLC messages and adds the following elements:

- Source and destination identifiers, *src* and *dest*,
- Timestamp, *ts*
- "Home" ATSU, *home*
- Message, *msg*

This entire message is signed using the sender's private key. The recipient verifies the message by checking the signature is valid using the sender's public key, before forwarding the plain message onto the CPDLC unit which processes it as before. In the event that the signature does not match or the timestamp is too old, the message is still forwarded to the CPDLC unit, with an additional message element warning of integrity or authenticity issues. An automated *Invalid Signature* message is also returned to the sender.

5.3.2 Key Generation and Distribution. When a new keypair is generated, the public key must be sent to the relevant *authority* ATSU. Due to the lack of secure wireless communication links, it is preferable to instead use the ground-to-ground links already in place to transmit new keys of ATSUs. While they are unlikely to be fully secure, they at least have a much higher level of access control. Aircraft do not have direct access to this network so it would be wise to transport the key physically. Note that this key generation should not be performed by the home ATSU and sent to a device; the private key should not be transmitted over the air due to a lack of secure data links and should only be stored on the device to which it belongs.

There are two main approaches to handling key distribution. The first is to maintain on each aircraft and ATSU a database of all units' public keys. This may be difficult to implement, and would cause issues if keys expire or are revoked and the database is not updated frequently enough.

The second approach is to maintain only a partial database. This database contains up-to-date records of all *authority* ATSUs' public keys, as well as the keys of any units with which it has recently communicated. To obtain the key of a unit which does not appear in its database (or a key that has timed out), a *Key Request* message is sent to the unit's "Home" ATSU as specified in the original message. The authority responds with the key, which is stored in the database with a fixed timeout. This exchange can be seen in Fig. 13, and is a slightly modified version of the Needham-Schroeder-Lowe key distribution protocol [33]—instead of sending encrypted messages, this modified protocol uses the keys to sign messages. This does not offer confidentiality but preserves message integrity and authenticity of origin.

Of course, this only works when it is an ATSU that needs to obtain the key of an aircraft, since ground-to-ground data links can be used to communicate with the Home ATSU. In the case where an aircraft needs to obtain an ATSU's key, it will need to be sent over the air. This can be implemented by requiring the current CPDLC data authority to send the new ATSU's key alongside the *Next Data Authority* message. This can be sent as a new type of message element, which is intercepted by our new PKI unit before it reaches the CPDLC unit.

Alternatively, the aircraft's initial ATSU can be required to send all the keys it will need for the whole journey as it departs from the airport. This is slightly easier to implement, but will cause problems

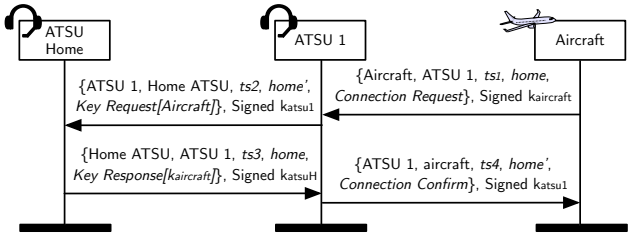

Figure 13: Key distribution under the proposed PKI system: an ATSU obtains the public key of an aircraft by communicating with its designated home ATSU.

if the aircraft deviates from its flight plan, since it will be forced to revert to unverified CPDLC until it returns to its planned route.

5.3.3 Key Revocation. We need to be able to handle key revocation in a robust manner, in case a key is leaked or an aircraft is decommissioned. Requiring requested keys to automatically expire should for the most part solve this problem, provided the timeout is sufficiently short—on the order of hours or days. If an immediate revocation is required, an *authority* ATSU can broadcast a message instructing units to remove the key in question.

5.3.4 Backwards Compatibility. Although the underlying messages are ultimately the same CPDLC messages, the structure of the new messages means they are not compatible with old systems. Unless all aircraft and ATSUs switch to the new system at once, a compatibility layer will be needed in order to allow devices running different systems to communicate with one another. Potential solutions include:

- **Manual Switch**, allowing flight crew or ATC to manually disable PKI on agreement over voice. This relies on voice communications, somewhat undermining CPDLC usage.
- **Automatic Switch**, maintaining a database of PKI-equipped ATSUs and aircraft, checked before contact begins. This relies on the database being constantly up-to-date, otherwise legitimate PKI-equipped aircraft may have messages rejected.
- **Additional CPDLC Message Element**, wherein the message signature is added as a CPDLC message element rather than an entirely new structure. This enables old units to understand signed messages without requiring additional hardware—in compatible systems the PKI unit intercepts the message and verifies the signature, but if there is no PKI unit the extra message can simply be ignored.

It is likely that an effective system would implement the additional message element, or use an automatic switch by default and fall back to manual when needed, i.e. when an aircraft and ATSU need to communicate but do not have the required keys.

5.3.5 System Robustness. Due to the use of asymmetric cryptography, the system will be secure against unauthorized transmissions, preventing the message injection and man-in-the-middle attacks covered in Sec. 4. The inclusion of the timestamp, source, and destination in the signed portion of the message also protects against message replay attacks.

The robustness of this new system depends heavily on the public-key cryptosystem used—if an insecure cryptosystem is used, then

Table 1: Comparison of the proposed countermeasures.

Countermeasure	Backwards Compatibility	Challenges	Effectiveness
Geography-Based	Yes	Up-to-date database of ATSU locations	Improves detection of attacks
Interference Alerts	Yes	Detecting reactive jamming	Improves detection of attacks
PKI	No/Partial	Key distribution, backwards compatibility	Prevents attacks

it is likely that private keys could be obtained even if the underlying infrastructure is well-designed. The specifics of what cryptosystem is used do not affect the rest of the design of this protocol, so we can simply choose a system which is widely regarded as secure, such as RSA or ECDSA, both of which are considered secure with sufficiently large keys [29, 34, 39]. Both RSA and ECDSA are already widely used in SSL certificates across the web, so using these cryptosystems to secure CPDLC should not incur a large computational overhead.

Due to the implementation of Needham-Schroeder-Lowe, it will not be possible for the attacker to inject an incorrect key during the distribution process unless they can obtain one of the legitimate private keys. Even if the attacker uses a different key in the first message of Fig. 13, they will be unable to replace the aircraft's legitimate key in the distribution exchange. As a result, the ATSU will realise the signature is incorrect once they receive the correct key.

The main risk comes from downgrade attacks, which depend on the specifics of how backwards compatibility is handled. If the new system accepts messages with no signature, then message injection attacks can still be performed, making the system no more secure than it was before. It is therefore important that unsigned messages are either ignored entirely (unless manually overridden), or the flight crew or ATCO are clearly warned about it.

Inevitably the system would be vulnerable to denial-of-service (DoS) attacks, though this is not something we can control. This should not be a major issue since the majority of CPDLC messages are acknowledged in some form, and issues with CPDLC are typically responded to by downgrading to voice communications. Furthermore, wide-scale DoS would require high-power transmissions, thereby making it easy to identify attacker locations.

6 DISCUSSION

As shown, the attacks proposed in this paper allow an attacker to masquerade as a legitimate ATCO, issuing arbitrary instructions to the aircraft. We believe this poses a risk to aircraft safety, since the attacks can be performed by a single motivated adversary. These attacks are possible for two reasons: a lack of in-built security in CPDLC, and consequently the operation of CPDLC over insecure data links.

While the risk posed by these attacks is significant, it is possible to use the countermeasures proposed in order to mitigate attacks. A high-level comparison of each of our proposed countermeasures is given in Tab. 1. Specifically, we have proposed measures which would allow existing CPDLC hardware to remain in operation. Security mechanisms would be provided through new devices working in conjunction with CPDLC or acting as a benevolent man-in-the-middle. The most expensive—though comprehensive—solution would be to use message signing through PKI. This approach would allow guarantees to be made about the sender and receiver of the aircraft, making man-in-the-middle attacks much harder. The other proposed solutions, while cheaper and easier to implement, do not offer the same level of comprehensive protection as PKI. They facilitate the detection of simpler attacks but would not deter a motivated adversary.

As with other work looking at avionics coming into wide deployment, we are seeing a system designed decades ago being deployed as a key part of future infrastructure. This highlights a key near-term challenge for aviation. Technologies need many years for development, certification and adoption. However, this means that many mature technologies underpinning airspace modernization for the next 5-10 years were designed at a time when security was not a major consideration. From this, we can see how important it is that security is a primary consideration in new systems—addressing this after the fact is extremely difficult, if even possible.

Based on this work, many avenues of future work exist. An important initial step would be to perform further security analysis on CPDLC to better understand the range of attacks that this system is vulnerable to. This would then allow analysis of how well CPDLC attacks scale, which would help to map the magnitude of the threat. Another important step would be to consider the longevity of these attacks under current system designs, especially focusing on how flight crew and ATCOs might spot attacks. This would highlight important human factors in securing the system.

7 CONCLUSION

In this paper, we identify and design a practical man-in-the-middle attack on the CPDLC system and analyze additional factors that can considerably increase the power of the attack in the deployed air traffic control system. More specifically, the described attack uses the unauthenticated nature of CPDLC-carrying data links in order to push a target aircraft into treating the attacker as a legitimate ATSU. During this time, the attacker can issue instructions as a legitimate ATCO would, without being immediately obvious to flight crew. As shown by our real-world analysis, there are regular attack opportunities from hundreds of kilometres distance — about one every 6 minutes in a typical pre-COVID-19 airspace — underlining the feasibility of our attack.

We further discussed the potential countermeasures against such attacks. Although redeploying a secure-by-design version of CPDLC is unrealistic in the short term, we proposed a range of additions to the system which would help manage attacks. In terms of lightweight measures, we identify logical checks based on realistic aircraft trajectories and indicating interference to ATC and flight crew. As a larger, more comprehensive countermeasure, we design and analyse a PKI-based message signing approach for CPDLC.

With worldwide adoption of CPDLC, its vulnerability to attack will only become more important. As such, understanding how the system can be attacked and adopting mechanisms to mitigate these attacks is becoming vital in keeping airspace safe and secure.

REFERENCES

[1] Aerodiscount. Linear Amplifier AM Booster 13W for REXON RHP-530 Aviation Radio. https://www.aerodiscount.com/en/airband-radios-accessories/553-linear-amplifier-am-booster-13w-for-rexon-rhp-530-aviation-radio.html. Accessed: 2020-12-11.

[2] AirSatOne. Viasat Ka & Ku Band High Speed Satcom Internet for Business and VIP Aviation. https://web.archive.org/web/20190425190146/https://www.airsatone.com/ka-ku-viasat-satcom-internet. Accessed: 2020-12-11.

[3] Doris Di Marco, Alessandro Manzo, Marco Ivaldi, and John Hird. Security Testing with Controller-Pilot Data Link Communications. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*, pages 526–531. IEEE, 2016.

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

[5] Eurocontrol. Controller-pilot datalink communications at our Maastricht UAC. https://www.eurocontrol.int/service/controller-pilot-datalink-communications-our-maastricht-uac. Accessed: 2020-12-11.

[6] R. Fantacci, S. Menci, L. Micciullo, and L. Pierucci. A secure radio communication system based on an efficient speech watermarking approach. *Security and Communication Networks*, 2(4):305–314, 2008.

[7] Federal Aviation Administration. Radio Communications Phraseology and Techniques. https://www.faa.gov/air_traffic/publications/atpubs/aim_html/chap4_section_2.html. Accessed: 2020-12-11.

[8] Federal Aviation Administration. Class Airspace. https://adds-faa.opendata.arcgis.com/datasets/c6a62360338e408cb1512366ad61559e_0, December 2020. Accessed: 2020-12-11.

[9] Patrick Flynn. Fighter jets intercept Ryanair flight after radio communications failure. https://www.independent.ie/irish-news/fighter-jets-intercept-ryanair-flight-after-radio-communications-failure-36614996.html, February 2018. Accessed: 2020-12-11.

[10] Great Scott Gadgets. HackRF One. https://greatscottgadgets.com/hackrf/, March 2012. Accessed: 2020-12-11.

[11] Andrei Gurtov, Tatiana Polishchuk, and Max Wernberg. Controller–Pilot Data Link Communication Security. *Sensors*, 18(5):1636, 2018.

[12] M. Hagmüller, H. Hering, A. Kröpfl, and G. Kubin. Speech watermarking for air traffic control. In *2004 12th European Signal Processing Conference*, pages 1653–1656, September 2004.

[13] H Hering, M Hagmüller, and G Kubin. Safety and Security increase for Air Traffic Management Through Unnoticeable Watermark Aircraft Identification Tag Transmitted with the VHF Coice Communication. *Digital Avionics Systems Conference, 2003. DASC '03. The 22nd*, 1:4.E.2–41–10 vol.1, 2003.

[14] International Civil Aviation Organization. *Manual of Air Traffic Services Data Link Applications*, chapter VI.1, pages VI—1–1. 1999.

[15] International Civil Aviation Organization. *Annex 10 to the Convention on International Civil Aviation. Aeronatical Telecommunications. Communication Procedures including those with PANS Status.*, volume II, chapter 5, pages 5.19–5.22. 2001.

[16] International Civil Aviation Organization. *Annex 2 to the Convention on International Civil Aviation: Rules of the Air*, chapter 3.6.5, page 3.13. 10 edition, 2005.

[17] International Civil Aviation Organization. *Annex 2 to the Convention on International Civil Aviation: Rules of the Air*, chapter 3.7, page 3.14. 10 edition, 2005.

[18] International Civil Aviation Organization. *Annex 10 to the Convention on International Civil Aviation. Aeronautical Telecommunications: Surveillance and Collision Avoidance Systems.*, volume IV, chapter 2, pages 2.3–2.4. 2007.

[19] International Civil Aviation Organization. *Global Operational Data Link (GOLD) Manual*, chapter 2.2.4, pages 2–25. 2 edition, 2013.

[20] International Civil Aviation Organization. *Global Operational Data Link (GOLD) Manual*, chapter 5.2.3, pages 5–7. 2 edition, 2013.

[21] International Civil Aviation Organization. *Global Operational Data Link (GOLD) Manual*, chapter 2.2.3, pages 2–19—2–24. 2 edition, 2016.

[22] International Civil Aviation Organization. *Global Operational Data Link (GOLD) Manual*, chapter A.2, pages A–3—A–5. 3 edition, 2016.

[23] International Civil Aviation Organization. *Global Operational Data Link (GOLD) Manual*, chapter 2.2.4.6, pages 2–18. 2 edition, 2016.

[24] International Civil Aviation Organization. *Global Operational Data Link (GOLD) Manual*, chapter A.4.13, pages A–45—A–47. 3 edition, 2016.

[25] International Civil Aviation Organization. *Global Operational Data Link (GOLD) Manual*, chapter B-EUR-2, pages B–11—B–12. 3 edition, 2016.

[26] International Civil Aviation Organization. *Annex 11 to the Convention on International Civil Aviation: Air Traffic Services*, chapter 2.25. 15 edition, 2018.

[27] International Civil Aviation Organization. The World of Air Transport in 2018. https://www.icao.int/annual-report-2018/Pages/the-world-of-air-transport-in-2018.aspx, 2018. Accessed: 2020-12-11.

[28] International Civil Aviation Organization (ICAO) European and North Atlantic Office. *EUR DOC 011. EUR Frequency Management Manual*, chapter 4. 2019.

[29] Don Johnson, Alfred Menezes, and Scott Vanstone. The Elliptic Curve Digital Signature Algorithm (ECDSA). *Int. journal of information security*, 1(1), 2001.

[30] Jun Kitaori. A performance comparison between VDL mode 2 and VHF ACARS by protocol simulator. In *2009 IEEE/AIAA 28th Digital Avionics Systems Conference*, pages 4–B. IEEE, 2009.

[31] Tomasz Lemiech. dumpvdl2. https://github.com/szpajder/dumpvdl2, 2020.

[32] Live ATC. 25-MAY-2011 FAKE ATC IN ACTION (LTBA-ISTANBUL). https://forums.liveatc.net/atcaviation-audio-clips/25-may-2011-fake-atc-in-action-(ltba-istanbul), June 2011. Accessed: 2020-12-11.

[33] Gavin Lowe. An Attack on the Needham-Schroeder Public-Key Authentication Protocol. *Information processing letters*, 56(3), 1995.

[34] National Security Agency. The Case for Elliptic Curve Cryptography. https://web.archive.org/web/20090117023500/http://www.nsa.gov/business/programs/elliptic_curve.shtml, January 2009. Accessed: 2020-12-11.

[35] ATC Data Link News. Introduction. http://members.optusnet.com.au/~cjr/introduction.htm, 2016. Accessed: 2020-12-11.

[36] Roy T. Oishi and Ann Heinke. *Digital Avionics Handbook*, chapter 2, page 2.4. CRC Press, third edition, 2015.

[37] Okuary Osechas, Mohamad Mostafa, Thomas Graupl, and Michael Meurer. Addressing vulnerabilities of the CNS infrastructure to targeted radio interference. *IEEE Aerospace and Electronic Systems Magazine*, 32(11):34–42, 2017.

[38] Bogdan Petricel. *8.33kHz Voice Channel Spacing (VCS) Implementation Handbook*, chapter 6, page 37. Eurocontrol, 2017.

[39] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[40] Kristian Silva. Sunshine Coast plane crash hoax sparks massive search. https://www.smh.com.au/national/queensland/sunshine-coast-plane-crash-hoax-sparks-massive-search-20141028-11d9xd.html, 2014. Accessed: 2020-12-11.

[41] SKYbrary. Aeronautical Information Publications (AIPs). https://www.skybrary.aero/index.php/Aeronautical_Information_Publications_(AIPs), 2017. Accessed: 2020-12-11.

[42] SKYbrary. SATCOM. https://www.skybrary.aero/index.php/SATCOM, 2017. Accessed: 2020-12-11.

[43] SKYbrary. Communication Failure: Guidance for Controllers. https://www.skybrary.aero/index.php/Communication_Failure:_Guidance_for_Controllers, 2020. Accessed: 2020-12-11.

[44] Matthew Smith, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS. In *International Conference on Financial Cryptography and Data Security 2017*. Springer, apr 2017.

[45] Matthew Smith, Daniel Moser, Martin Strohmeier, Ivan Martinovic, and Vincent Lenders. Undermining Privacy in the Aircraft Communications Addressing and Reporting System (ACARS). In *18th Privacy Enhancing Technologies Symposium (PETS 2018)*, Barcelona, July 2018.

[46] 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 *Network and Distributed Systems Security Symposium, NDSS*, 2020.

[47] T. H. Stelkens-Kobsch, A. Hasselberg, T. Mühlhausen, N. Carstengerdes, M. Finke, and C. Neeteson. Towards a more secure ATC voice communications system. In *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*, pages 4C1–1–4C1–9, September 2015.

[48] Mario Strasser, Boris Danev, and Srdjan Čapkun. Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 7(2):1–29, 2010.

[49] Martin Strohmeier, Ivan Martinovic, and Vincent Lenders. Securing the Air–Ground Link in Aviation. In *The Security of Critical Infrastructures*, pages 131–154. Springer, 2020.

[50] Two Way Accessories. VHF Airband Broadband Antenna. https://www.twowayaccessories.com/radio-accessories/radio-base-antennas-and-duplexers/vhf-airband-broadband-antenna-118-137mhz/. Accessed: 2020-12-11.

[51] U.S. Department of Commerce. United States Frequency Allocations. https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf, 2003. Accessed: 2020-12-11.

[52] 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*, 2011.

[53] Emma Younger. Melbourne Airport hoax caller Paul Sant pleads guilty to making fake flight calls, aborting Virgin landing. https://www.abc.net.au/news/2017-09-05/melbourne-airport-hoax-caller-paul-sant-pleads-guilty/8873984. Accessed: 2020-12-11.

[54] Airways New Zealand. FANS1/A Problem Reporting, Unsuccessful CPDLC transfer but no NCDA downlink. https://web.archive.org/web/20190907131530/https://www.fans-cra.com/report/de-identified/detail/c352f86491dd21907e9a7e2e0c3a833a68e55b74/. Accessed: 2020-12-11.